SISTEM INFORMASI AKUNTASI DAN BISNIS

Agus Tina
Ade Onny Siagian
Denny Rakhmad Widi Ashari
I Made Dwi Hita Darmawan
Angga Aditya Permana
Ketut Tanti Kustina
Nano Suyatna
Ika Prayanthi

GET PRESS INDONESIA

SISTEM INFORMASI AKUNTASI DAN BISNIS

Penulis :
Agus Tina
Ade Onny Siagian
Denny Rakhmad Widi Ashari
I Made Dwi Hita Darmawan
Angga Aditya Permana
Ketut Tanti Kustina
Nano Suyatna
Ika Prayanthi

ISBN :

Editor : Diana Purnama Sari,. S.E M.E
Penyunting : Tri Putri Wahyuni,S.Pd
Desain Sampul dan Tata Letak : Atyka Trianisa, S.Pd

Penerbit : GET PRESS INDONESIA
Anggota IKAPI No. 033/SBA/2022

Redaksi :
Jln. Palarik Air Pacah No 26 Kel. Air Pacah
Kec. Koto Tangah Kota Padang Sumatera Barat
Website : www. getpress.co.id
Email : adm.getpress@gmail.com

Cetakan pertama, November 2023

Hak cipta dilindungi undang-undang
Dilarang memperbanyak karya tulis ini dalam bentuk dan dengan cara apapun tanpa izin tertulis dari penerbit.

KATA PENGANTAR

Segala Puji dan syukur atas kehadirat Allah SWT dalam segala kesempatan. Sholawat beriring salam dan doa kita sampaikan kepada Nabi Muhammad SAW. Alhamdulillah atas Rahmat dan Karunia-Nya penulis telah menyelesaikan Buku Sistem Informasi Akuntasi Dan Bisnis ini.

Buku ini membahas Konsep dasar Sistem Informasi Akuntansi (SIA) dan bisnis, E-commerce dan E-Business, Manajemen data dan database, Fraud, ethics, dan pengendalian internal, Pengendalian intern dan resiko sistem IT, IT governance/ tata kelola IT, Pengauditan teknologi informas, Proses dan pengendalian atas pendapatan serta penerimaan kas.

Proses penulisan buku ini berhasil diselesaikan atas kerjasama tim penulis. Demi kualitas yang lebih baik dan kepuasan para pembaca, saran dan masukan yang membangun dari pembaca sangat kami harapkan.

Penulis ucapkan terima kasih kepada semua pihak yang telah mendukung dalam penyelesaian buku ini. Terutama pihak yang telah membantu terbitnya buku ini dan telah mempercayakan mendorong, dan menginisiasi terbitnya buku ini. Semoga buku ini dapat bermanfaat bagi masyarakat Indonesia.

Padang, November 2023

Penulis

DAFTAR ISI

DAFTAR GAMBAR

BAB 1
KONSEP DASAR SISTEM INFORMASI AKUNTANSI DAN BISNIS

Oleh Agus Tina

1.1 Pendahuluan

Ketersediaan informasi memungkinkan pengambil keputusan di perusahaan untuk memberikan saran terbaik mengenai cara kerja dan solusi apa yang dapat ditawarkan. Kehidupan pengguna pasti akan lebih mudah jika informasinya lebih menyeluruh dan mudah dipahami, serta memenuhi persyaratan kualitas informasi yang baik.

Namun, jika informasi yang dihasilkan ternyata tidak akurat, terkadang hal tersebut juga dapat menipu pengguna. Akibatnya, ketergantungan informasi harus ditentukan, dan data yang dihasilkan harus diorganisasikan. Hal ini juga berlaku untuk informasi seperti data akuntansi yang dapat digunakan untuk membuat keputusan keuangan. Sejauh ini, akuntansi telah memantapkan dirinya sebagai sistem informasi yang dapat dipercaya. Sistem informasi akuntansi adalah data yang ditampilkan dalam laporan dan ringkasan yang digunakan untuk membuat pilihan keuangan.

Jika teknologi informasi digunakan dalam proses manajemen, sistem informasi yang dikelola dapat menjadi lebih baik dan bernilai. Tentu saja, mengingat manfaatnya, akan menambah banyak nilai. Teknologi informasi yang dimiliki, misalnya melalui pengembangan proses manual menjadi otomatis. Sistem informasi manual yang sedang digunakan sebelumnya mulai menggabungkan dan mengintegrasikan dengan teknologi pendukung. Tentu saja hal ini akan berdampak signifikan terhadap standar kinerja bisnis secara keseluruhan

Sebuah sistem yang disebut sistem informasi akuntansi (SIA) diciptakan untuk mengumpulkan dan menyajikan data akuntansi

sehingga akuntan dan pemimpin bisnis dapat membuat keputusan yang tepat.

Sistem ini secara luas dianggap sebagai komponen penting kantor keuangan secara global dan dapat digunakan sebagai bagian dari solusi teknologi informasi suatu organisasi. Sistem ini sebagian besar berbasis perangkat lunak.

Di setiap industri, Sistem Informasi Akuntansi sangat penting bagi perusahaan. Konsep utamanya adalah menggabungkan protokol untuk melaporkan status keuangan organisasi secara tepat dan andal kepada semua pihak yang berkepentingan.

Teknologi informasi digunakan dalam prosedur ini untuk memajukan bisnis atau perusahaan. Mayoritas operasi bisnis akan dibuat lebih sederhana untuk bisnis yang menggunakan SIA. Biaya produksi dapat dikurangi dan dibuat lebih efektif dan efisien dengan memberikan informasi yang tepat dan akurat.

1.2 Konsep Dasar Sistem Informansi Akuntansi

Ketersediaan informasi mempengaruhi pandangan pengambil keputusan dalam suatu organisasi. Jika informasi yang diterima masyarakat berkualitas baik, maka masyarakat tidak akan kesulitan dalam mengambil keputusan. Jika suatu organisasi memiliki sistem yang baik, informasi yang berkualitas dapat diperoleh. Misalnya, dengan adanya sistem informasi akuntansi yang kompeten maka akan tercipta informasi keuangan yang baik sehingga memudahkan penggunanya dalam mengambil keputusan.

Komponen organisasi yang dikenal sebagai sistem informasi akuntansi mengumpulkan, mengatur, memproses, menganalisis, dan menyampaikan data keuangan dan pengambilan keputusan yang berkaitan dengan pihak di luar perusahaan dan pihak eksternal. Sistem Informasi Akuntansi memproses semua sumber data yang diterimanya guna menyiapkan informasi bagi manajemen. Hal ini juga berdampak pada bagaimana organisasi perusahaan berinteraksi dengan lingkungannya.

Sebagai sistem informasi akuntansi, ia harus mengumpulkan data informasi yang menjelaskan operasi bisnis, mengubahnya menjadi informasi, dan membuatnya tersedia bagi pengguna di dalam dan di luar perusahaan. Selain itu, satu-satunya sistem yang

bertugas memenuhi kebutuhan informasi di luar perusahaan adalah sistem informasi akuntansi. Data akuntansi berkaitan dengan divisi yang bertugas mengawasi arus keuangan bisnis. Karena pemasaran, produksi, dan operasi bisnis lainnya memerlukan arus kas, maka penting untuk mengelola semua arus kas untuk memastikan penggunaan dana yang tersedia secara efisien. Pihak yang berkepentingan terhadap informasi keuangan suatu Perusahaan dibagi menjadi dua yaitu pihak eksternal dan pihak internal.

1.3 Pengertian Sistem, Informasi, Akuntansi dan Sistem Informasi Akuntansi

1.3.1 Sistem

Suatu sistem terdiri dari dua atau lebih bagian yang bekerja sama dan satu sama lain untuk mencapai tujuan tertentu. Selain itu, menurutnya bisnis adalah suatu sistem yang terdiri dari banyak divisi yang bekerja sama sebagai subsistem (Romney. M.B. and Steinbart 2006). Sementara beberapa orang berpendapat bahwa sistem adalah sekelompok prosedur terhubung yang digunakan untuk menyelesaikan aktivitas tertentu atau mewujudkan tujuan tertentu. (NS 2009).

Dengan kata lain, sistem adalah kumpulan beberapa bagian yang bekerja sama untuk menyelesaikan suatu tugas. Sistem biasanya terdiri dari beberapa subsistem yang lebih kecil, yang masing-masing mendukung sistem utama dengan cara yang berbeda. Ambil contoh sistem komputer. Suatu komputer biasanya akan berfungsi jika mempunyai bagian-bagian seperti prosesor (untuk pengolahan data), memori (untuk penyimpanan), monitor (untuk tampilan layar), dan keyboard (untuk media input data). Sistem akan berhenti jika salah satu bagian ini rusak, sehingga tujuan sistem tidak tercapai.

1.3.2 Informasi

Informasi diciptakan dengan menggabungkan data dan fakta yang relevan dengan cara yang paling sesuai dengan kebutuhan konsumennya, yaitu agar mereka dapat mengambil keputusan yang tepat (NS 2009). Data dikumpulkan melalui proses pengumpulan sistem untuk menghasilkan informasi, yang kemudian diolah

sehingga tepat untuk disampaikan ke pengguna informasi (Dengen, N. and Hatta 2009).

Terdapat empat dimensi agar dapat meningkatkan nilai dari suatu informasi, yaitu Relavansi, Akurasi, Aktual dan Kelengkapan (Soenarno 2015).

Informasi yang berkualitas akan memberikan manfaat bagi penggunanya. Beberapa manfaat dari informasi adalah peningkatan pengetahuan, penurunan skeptisisme di kalangan konsumen informasi, penurunan peluang kegagalan, penurunan keragaman yang tidak perlu, dan penyediaan standar, norma, pengukuran, dan penilaian untuk menilai pencapaian tujuan dan sasaran.

1.3.3 Akuntansi

Secara umum, akuntansi adalah aktivitas jasa yang tujuannya adalah memberikan data kuantitatif tentang situasi keuangan dan kinerja operasi perusahaan yang akan membantu dalam pengambilan keputusan mengenai perekonomian. Menurut (Nasution 2004) Akuntansi adalah suatu istilah luas yang mengacu pada sejumlah teori, praduga tentang bagaimana berperilaku (*behavior*), aturan bagaimana mengambil tindakan, dan prosedur pengumpulan dan pelaporan informasi yang berguna mengenai kegiatan dan tujuan suatu organisasi. Pendapat lain mengatakan, Akuntansi adalah sistem informasi yang mengubah data menjadi laporan keuangan yang berasal dari operasional bisnis perusahaan, dan menginformasikannya kepada pengambil keputusan (Wauran 2016).

Akuntansi diperlukan dan menyangkut sejumlah prosedur, termasuk teknik pencatatan dan cara penyajian laporan keuangan, agar informasi yang disajikan dapat dipertanggungjawabkan. Karena proses pembuatan dan penyajian laporan keuangan didasarkan pada catatan hasil yang telah disimpan, maka kedua strategi ini mempunyai keterkaitan yang erat. agar terhindar dari kesalahan (Nasution 2004).

1.3.4 Sistem Informasi Akuntansi

Di antara sistem informasi yang digunakan manajemen untuk menjalankan bisnisnya adalah sistem informasi akuntansi.

Sebagai subsistem informasi manajemen, sistem ini menangani data keuangan untuk menyediakan informasi keuangan sebagai tanggapan atas permintaan baik dari pengguna internal maupun eksternal. Sistem informasi akuntansi suatu organisasi bertugas mengumpulkan informasi dari pengolahan dan pengumpulan data transaksi serta mengaturnya ke dalam format yang dapat diakses oleh semua pengguna, baik internal maupun eksternal perusahaan. Sistem informasi akuntansi juga dapat dilihat sebagai sekelompok operasi organisasi yang bertugas menyampaikan informasi keuangan dan informasi yang diperoleh dari data transaksi untuk kebutuhan pelaporan baik di dalam maupun di luar perusahaan. Sistem informasi akuntansi berdampak pada bagaimana organisasi perusahaan berinteraksi dengan lingkungannya dan menyiapkan informasi untuk manajemen dengan menerapkan operasi spesifik pada setiap sumber data yang mereka terima (Romney dan Stainbart 2006).

Secara umum Sistem Informasi Akuntansi dibagi menjadi 5 subsistem/ siklus utama, yaitu (Mulyani 2012) :

1. Sistem Informasi Pendapatan.
2. Sistem Informasi Pengeluaran.
3. Sistem Informasi Produksi.
4. Sistem Informasi Penggajian.
5. Sistem Informasi Pelaporan.

1.4 Tujuan Sistem Informasi Akuntansi

Tujuan dasar SIA adalah untuk membangun kendali. Manajemen internal yang telah terlembaga mengembangkan budaya manajemen yang positif. Selain itu, SIA juga berencana melakukan hal tersebut (Marina, Wahjono, and Suarni 2018):

1. Mengakumulasikan dan mengemas informasi tentang kegiatan keuangan dan operasional bisnis.
2. Mengubah data menjadi pengetahuan yang dapat dimanfaatkan oleh bisnis untuk mengambil keputusan..
3. Memiliki kendali penuh atas bisnis.

Karena SIA adalah sistem terbuka dan tidak dapat menjamin terhadap penipuan atau kesalahan, organisasi memerlukan

pengendalian internal yang kuat untuk menjaga terhadap aktivitas internal dan eksternal yang tidak bermoral. Pengendalian internal didefinisikan secara sempit sebagai tindakan seperti memverifikasi otoritas, menghitung berapa kali plus dan minus, dan memeriksa dokumentasi pendukung untuk setiap transaksi. Namun pengendalian internal di SIA memiliki fungsi yang lebih umum, yaitu sebagai berikut (Marina, Wahjono, and Suarni 2018) :

1. Mendapatkan data yang dapat dipercaya
   Setelah dikumpulkan dan disimpan, data tersebut pada akhirnya memperoleh kredibilitas karena dapat digunakan untuk berbagai tujuan oleh pihak eksternal dan pihak internal untuk memutuskan hal yang tepat dalam bidang penjualan, layanan, pengukuran efisiensi, dan bidang lainnya.
2. Melancarkan operasional dan efisiensi
   Sistem yang dirancang dengan baik akan memfasilitasi evaluasi diri untuk meningkatkan kinerja layanan dan menyederhanakan operasi bisnis. Sistem yang efektif dapat meningkatkan protokol, formulir, dan bahkan struktur organisasi untuk memenuhi kebutuhan lingkungan internal dan eksternal bisnis.
3. Menjaga harta perusahaan
   Mencegah upaya penipuan yang disengaja atau tidak disengaja, seperti penambahan yang salah, perkalian, kekurangan faktur, dan sejenisnya, diperlukan untuk melakukan hal ini. mengoptimalkan efisiensi dan operasi.
4. Mempermudah dalam proses pengambilan keputusan
   Akan lebih mudah untuk memberikan laporan keuangan yang memenuhi tuntutan manajemen, khususnya untuk pengambilan keputusan harian dan bahkan strategis, jika data dikumpulkan secara teratur.
5. Mendorong agar taat terhadap kebijakan manajemen
   Sistem yang efektif akan tertanam dalam kehidupan anggota staf dan tidak dianggap sebagai beban, sehingga menumbuhkan kerja sama tim yang unggul dalam mencapai tujuan, visi, dan misi organisasi. Semua personel harus mengikuti kebijakan manajemen agar organisasi berhasil.

1.5 Peran Sistem Informasi Akuntansi

Kumpulan rangkaian teknologi dan prosedur terkait yang digunakan untuk mengubah data keuangan menjadi pengetahuan keuangan yang relevan bagi pemangku kepentingan dikenal sebagai sistem informasi akuntansi.

Tentu saja, suatu Sistem Informasi Akuntansi perlu memberikan nilai tambah kepada penggunanya agar dapat eksis sebagai perangkat sistem informasi. Sistem informasi harus dilihat sebagai investasi bagi bisnis dan bukan sebagai kewajiban.

Sistem informasi akuntansi memiliki peran dalam menciptakan nilai sebagai berikut.

1. Menjadikan bisnis lebih efisien.
2. Meningkatkan ketepatan dan kekinian data perusahaan.
3. Meningkatkan standar barang dan jasa.
4. Meningkatkan standar pengendalian dan perencanaan (penyusunan anggaran).

1.6 Pihak Pemakai Sistem Informasi Akuntansi

Para pihak yang dapat menggunakan informasi yang disediakan oleh Sistem Informasi Akuntansi adalah sebagai berikut (Mulyani 2012).

1. Pihak eksternal:
   a. pelanggan;
   b. pemasok;
   c. pemegang saham;
   d. lembaga pemerintah;
   e. auditor.
2. Pihak internal, di antaranya manajemen dan karyawan.

Selain mempengaruhi bagaimana organisasi bisnis berinteraksi dengan lingkungannya, AIS melakukan operasi spesifik pada setiap sumber data yang diterimanya untuk menyiapkan informasi untuk manajemen.

Informasi Akuntansi yang dihasilkan oleh SIA terdiri dari dua, yaitu sebagai berikut :

1. Informasi akuntansi keuangan, informasi dalam bentuk laporan keuangan yang ditujukan kepada pihak luar perusashaan.
2. Informasi akuntansi manajemen, informasi yang berguna dalam pengambilan keputusan akuntansi oleh manajemen.

1.7 Karakteristik Sistem Informasi Akuntansi

Karakteristik Sistem Informasi Akuntansi antara lain sebagai berikut (Romney dan Stainbart 2006):

1. Sistem informasi akuntansi melakukan ha-hal yang diperlukan
2. Berdasarkan pada prosedur yang relatif standar
3. Menghandle data dengan jelas dan lengkap
4. Berdasarkn data yang dimiliki sebelumnya
5. Memudahkan dalam pemecahan suatu masalah

DAFTAR PUSTAKA

Dengen, N. and Hatta, H.R. 2009. "Perancangan Sistem Informasi Terpadu Pemerintah Daerah Kabupaten Paser." *Jurnal Ilmiah Ilmu Komputer* 4(1): pp.47-54.

Marina, A., S. I. Wahjono, and A. Suarni. 2018. *Sistem Informasi Akuntansi: Teori Dan Praktikal*. UMSurabaya Publishing.

Mulyani, Sri. 2012. "Konsep-Konsep Dasar Sistem Informasi Akuntansi." *Sistem Informasi Akuntansi*: 1–25. https://pustaka.ut.ac.id/lib/wp-content/uploads/pdfmk/EKSI431203-M1.pdf.

Nasution, Manahan. 2004. "Akuntansi Guna Usaha(Leasing) Menurut Pernyataan SAK No. 30." *Usu* (30): 1–16.

NS, Sri Mulyani. 2009. *Sistem Informasi Manajemen Rumah Sakit: Analisis Dan Perancangan*. Bandung: Abdi Sistematika.

Romney. M.B. and Steinbart, P.J. (. 2006. *Accounting Information Systems*. 10th Editi. New Jersey: Prentice-Hall. Inc.

Romney dan Stainbart. 2006. "Sistem Informasi Akuntansi." *Konsep-konsep Dasar Sistem Informasi Akuntansi*: 3. https://pustaka.ut.ac.id/lib/wp-content/uploads/pdfmk/EKSI431203-M1.pdf.

Soenarno, A.R.P. 2015. "Analisis Pengaruh Kualitas Informasi Dan Kredibilitas Sumber Terhadap Kegunaan Informasi Dan Dampaknya Pada Adopsi Informasi (Studi Pada Masyarakat Pengikut Akun Twitter Resmi Ikaskus) (Doctoral Dissertation, Brawijaya University)."

Wauran, Anita. 2016. "Pentingnya Sistem Akuntansi Terhadap Pertanggungjawaban Sosial Pada Suatu Perusahaan." *Jurnal Riset Ekonomi, Manajemen, Bisnis dan Akuntansi* 4(4): 1126–31.

BAB 2
E-COMMERCE DAN E-BUSINESS

Oleh Ade Onny Siagian

2.1 Pengertian E-Commerce dan E-Business

E-commerce, singkatan dari *Electronic Commerce* (Perdagangan Elektronik), adalah istilah yang digunakan untuk menggambarkan segala jenis transaksi bisnis yang dilakukan secara elektronik melalui internet atau jaringan komputer lainnya. Ini mencakup pembelian dan penjualan produk atau layanan, pertukaran informasi, dan berbagai aktivitas lainnya yang terkait dengan bisnis yang dilakukan secara online (Munoz *et al.,* 2023).

Beberapa karakteristik utama dari e-commerce meliputi:

1. Transaksi Elektronik adalah E-commerce melibatkan pertukaran uang, data, atau informasi lainnya dalam bentuk digital atau elektronik. Ini dapat melibatkan pembayaran online, pemesanan produk atau layanan, pengiriman digital, dan sebagainya.
2. Akses Global adalah E-commerce memungkinkan bisnis untuk mencapai pasar global, karena internet adalah platform yang dapat diakses oleh siapa saja di seluruh dunia. Ini memberikan peluang untuk mengembangkan basis pelanggan yang lebih besar.

3. Berbagai Model Bisnis adalah Ada berbagai model bisnis e-commerce, termasuk toko online, pasar online, penjualan langsung dari produsen ke konsumen (D2C), penjualan melalui lelang online, dan banyak lagi. Setiap model memiliki karakteristik dan keuntungan sendiri.
4. Automatisasi dan Otomatisasi adalah E-commerce sering melibatkan penggunaan teknologi otomatisasi untuk mengelola inventaris, pengiriman, pemrosesan pesanan, dan layanan pelanggan. Ini dapat menghemat waktu dan upaya.
5. Keamanan dan Privasi adalah Keamanan dan privasi sangat penting dalam e-commerce karena melibatkan pertukaran data sensitif seperti informasi pembayaran dan identitas pelanggan. Teknologi keamanan seperti enkripsi data digunakan untuk melindungi informasi tersebut.
6. Pembayaran Elektronik adalah Pembayaran online adalah bagian integral dari e-commerce. Metode pembayaran seperti kartu kredit, transfer bank, dompet digital, dan metode lainnya digunakan untuk melakukan pembelian.
7. Pelacakan dan Analisis adalah E-commerce memungkinkan bisnis untuk melacak perilaku pelanggan secara rinci, mengumpulkan data transaksi, dan menganalisis data ini untuk meningkatkan strategi pemasaran dan penjualan.

E-commerce telah mengubah cara bisnis dilakukan dan telah menjadi bagian penting dari ekonomi global. Ini memberikan pelanggan lebih banyak pilihan, kenyamanan, dan aksesibilitas dalam berbelanja, sementara juga memberikan peluang bagi bisnis untuk tumbuh dan berkembang(Fernández-Bonilla et al., 2022).

Sedangkan E-business, atau Electronic Business (Bisnis Elektronik), adalah konsep yang lebih luas daripada e-commerce. Ini mencakup semua aktivitas bisnis yang menggunakan teknologi digital, khususnya internet, untuk melakukan berbagai fungsi bisnis, seperti pembelian, penjualan, pemasaran, komunikasi, dan manajemen operasional. E-business melibatkan penggunaan teknologi informasi dan komunikasi (TIK) untuk meningkatkan efisiensi, produktivitas, dan daya saing bisnis (Tamilarasi & Elamathi, 2020).

Berikut adalah beberapa aspek kunci dari e-business:

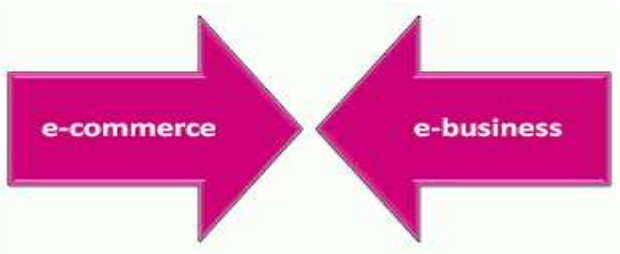
1. Pembelian dan Penjualan Online adalah Seperti yang terkait dengan e-commerce, e-business mencakup transaksi pembelian dan penjualan produk atau layanan melalui internet.
2. Pemasaran Online adalah E-business mencakup strategi pemasaran digital, termasuk iklan online, pemasaran melalui media sosial, kampanye email, dan upaya pemasaran online lainnya.
3. Manajemen Pelanggan adalah Penggunaan perangkat lunak CRM (Customer Relationship Management) dan alat-alat lainnya untuk mengelola interaksi dengan pelanggan, merespons pertanyaan, dan mempertahankan hubungan pelanggan yang baik.
4. Manajemen Operasional adalah Penggunaan teknologi untuk mengelola rantai pasokan, inventaris, produksi, dan operasi bisnis lainnya secara lebih efisien.
5. Komunikasi Bisnis adalah E-business mencakup komunikasi internal dan eksternal menggunakan alat seperti email, konferensi video, kolaborasi online, dan lain-lain.
6. Penggunaan Data dan Analitik adalah E-business melibatkan pengumpulan dan analisis data untuk mengambil keputusan bisnis yang lebih baik dan memahami perilaku pelanggan.
7. Keamanan Informasi adalah Keamanan data dan perlindungan privasi adalah bagian integral dari e-business, karena melibatkan pertukaran informasi sensitif.

8. Inovasi Teknologi adalah E-business melibatkan upaya terus-menerus untuk mengadopsi teknologi baru dan inovasi untuk meningkatkan operasi bisnis.

E-business memberikan fleksibilitas dan potensi pertumbuhan yang lebih besar daripada bisnis konvensional, karena memungkinkan akses ke pasar yang lebih luas dan kemampuan untuk beradaptasi dengan cepat dengan perubahan teknologi dan tren bisnis. Dalam konteks *e-business, e-commerce* adalah salah satu elemen yang penting, tetapi e-business mencakup lebih banyak lagi daripada sekadar transaksi online(Amit & Zott, 2001).

2.2 Gambaran E-Commerce dan E-Business dalam Sistem Informasi Akuntansi dan Bisnis

E-Commerce dan *E-Business* memiliki dampak yang signifikan dalam Sistem Informasi Akuntansi (SIA) dan Bisnis, memungkinkan perusahaan untuk mengotomatisasi berbagai proses bisnis, meningkatkan efisiensi, dan mendukung pengambilan keputusan yang lebih baik (Rehatalanit, 2021).



Berikut adalah gambaran bagaimana E-Commerce dan E-Business berinteraksi dengan SIA dan bisnis:

1. Perekaman Transaksi:
   a. E-Commerce: Dalam E-Commerce, setiap transaksi penjualan atau pembelian dicatat secara otomatis dalam sistem. Informasi ini mencakup detail pesanan, harga, informasi pelanggan, dan lainnya .
   b. E-Business: E-Business melibatkan seluruh spektrum aktivitas bisnis. SIA digunakan untuk merekam transaksi

bisnis yang melibatkan pembelian, penjualan, biaya operasional, dan lainnya. Semua data ini dapat diintegrasikan untuk memberikan gambaran yang komprehensif tentang kinerja bisnis.

2. Pengolahan Pembayaran:
   a. E-Commerce: Transaksi pembayaran online yang dilakukan melalui kartu kredit, dompet digital, atau metode pembayaran lainnya otomatis direkam dalam SIA perusahaan.
   b. E-Business: Pengolahan pembayaran dalam E-Business juga diintegrasikan dengan SIA, mencakup pemrosesan pembayaran dari pelanggan, pembayaran kepada vendor, dan pelaporan keuangan yang relevan.
3. Manajemen Persediaan:
   a. E-Commerce: Penjualan online memerlukan manajemen persediaan yang efisien. SIA digunakan untuk melacak persediaan, menginformasikan saat untuk melakukan pemesanan ulang, dan mengoptimalkan persediaan.
   b. E-Business: Dalam E-Business, SIA digunakan untuk mengelola persediaan tidak hanya untuk produk fisik tetapi juga untuk layanan dan aset digital.
4. Pengelolaan Hubungan Pelanggan:
   a. E-Commerce: Data pelanggan yang dikumpulkan dalam transaksi E-Commerce dapat digunakan untuk mengembangkan strategi pemasaran dan mempertahankan hubungan pelanggan yang kuat.
   b. E-Business: SIA digunakan untuk mengelola interaksi pelanggan di seluruh spektrum E-Business, mencakup dukungan pelanggan, penjualan, dan pemasaran.
5. Analisis Data:
   a. E-Commerce: Data transaksi E-Commerce dapat digunakan untuk menganalisis tren pembelian pelanggan, perilaku belanja, dan efektivitas kampanye pemasaran online.
   b. E-Business: SIA memungkinkan perusahaan untuk menganalisis data dari berbagai sumber, termasuk data penjualan online, data operasional, dan data keuangan, untuk mendukung pengambilan keputusan yang lebih baik.

6. Keamanan Informasi:
    a. E-Commerce dan E-Business: Keamanan informasi adalah aspek penting dalam kedua lingkungan ini. SIA digunakan untuk melindungi data pelanggan, data transaksi, dan informasi bisnis penting lainnya dari ancaman keamanan seperti peretasan dan pencurian data.

Integrasi yang baik antara *E-Commerce, E-Business*, dan SIA adalah kunci untuk mengoptimalkan efisiensi bisnis, meningkatkan pengalaman pelanggan, dan mencapai kesuksesan dalam era digital. Data yang dihasilkan dari aktivitas *E-Commerce* dan *E-Business* juga dapat digunakan untuk analisis yang mendalam dan perencanaan strategis yang lebih baik (Tumpal Manik, 2018).

2.3 Teori E-Commerce dan E-Business dalam Sistem Informasi Akuntansi dan Bisnis

Ada beberapa teori yang berkaitan dengan *E-Commerce* dan *E-Business* dalam konteks Sistem Informasi Akuntansi (SIA) dan Bisnis. Beberapa teori ini membantu memahami bagaimana teknologi informasi, *e-commerce*, dan *e-business* mempengaruhi operasi bisnis dan pengambilan keputusan(Fitriani, 2023).

Berikut adalah beberapa teori yang relevan:

1. Teori Perubahan Teknologi (*Technology Adoption Theory*): Teori ini, yang dikembangkan oleh Everett Rogers, menjelaskan bagaimana inovasi teknologi diterima dan diadopsi oleh individu atau organisasi. Dalam konteks e-commerce dan e-

business, teori ini membantu menjelaskan mengapa beberapa perusahaan mengadopsi teknologi digital dengan cepat sementara yang lain lebih lambat.

2. Teori Strukturasi (*Structuration Theory*): Teori ini, yang dikembangkan oleh Anthony Giddens, menggambarkan hubungan antara individu dan teknologi dalam konteks organisasi. Dalam konteks e-business, teori ini dapat digunakan untuk memahami bagaimana teknologi informasi mempengaruhi struktur dan tindakan organisasi.
3. Teori Penerimaan Teknologi Informasi (*Technology Acceptance Model* - TAM): Teori ini menjelaskan faktor-faktor yang memengaruhi penerimaan dan penggunaan teknologi informasi. Dalam konteks *e-commerce* dan *e-business*, TAM dapat membantu memahami mengapa pengguna (seperti pelanggan atau karyawan) menerima atau menolak teknologi digital.
4. Teori Transaksi (*Transaction Cost Theory*): Teori ini dikemukakan oleh Oliver Williamson dan menjelaskan bagaimana organisasi memilih antara transaksi internal dan eksternal berdasarkan biaya transaksi. Dalam e-commerce, perusahaan menggunakan teori ini untuk mengambil keputusan tentang apa yang harus diproduksi sendiri dan apa yang harus dibeli atau outsourced dari pihak ketiga.
5. Teori Keagenan (*Agency Theory*): Teori ini menjelaskan hubungan antara pemilik (prinsipal) dan agen (manajemen) dalam organisasi. Dalam konteks e-commerce, teori ini membantu menjelaskan masalah agen dalam hal manajemen bisnis online dan bagaimana insentif dapat digunakan untuk mengatasi masalah ini.
6. Teori Pertukaran Sosial (*Social Exchange Theory*): Teori ini berkaitan dengan pertukaran dalam hubungan sosial dan bisnis. Dalam e-commerce, teori ini dapat digunakan untuk memahami bagaimana interaksi sosial antara pelanggan dan perusahaan memengaruhi keputusan pembelian dan kesetiaan pelanggan.
7. Teori Bisnis Elektronik (*Electronic Business Theory*): Ini adalah teori yang secara khusus berkaitan dengan konsep E-Business,

mencakup berbagai aspek seperti manajemen, strategi, dan dampak teknologi informasi dalam bisnis elektronik.

8. Teori Ekonomi Informasi (*Information Economics Theory*): Teori ini mengkaji bagaimana informasi dan data memiliki nilai ekonomi. Dalam konteks e-commerce dan e-business, ini membantu memahami bagaimana perusahaan dapat mengelola dan memanfaatkan data dengan cara yang menguntungkan.

Semua teori ini membantu menyediakan kerangka kerja konseptual untuk memahami bagaimana teknologi informasi dan praktik bisnis digital mempengaruhi organisasi, keputusan bisnis, dan hasil keuangan. Penerapan teori-teori ini dapat membantu perusahaan merencanakan dan mengelola implementasi E-Commerce dan E-Business dengan lebih baik.

2.4 Siklus E-Commerce dan E-Business dalam Sistem Informasi Akuntansi dan Bisnis

Siklus *E-Commerce* dan *E-Business* dalam Sistem Informasi Akuntansi (SIA) dan Bisnis menggambarkan serangkaian langkah atau tahapan yang mencakup proses bisnis elektronik dari awal hingga akhir, termasuk transaksi, pelacakan, dan pelaporan(Gusti et al., 2010).

Berikut adalah beberapa tahapan dalam siklus E-Commerce dan E-Business:

1. Identifikasi Peluang Bisnis yaitu Tahap pertama dalam siklus E-Commerce dan E-Business adalah mengidentifikasi peluang bisnis yang dapat dimanfaatkan dengan menggunakan

teknologi digital. Hal ini mungkin melibatkan analisis pasar, studi kompetitor, dan perencanaan strategis.

2. Pembuatan Situs Web atau Platform E-Commerce yaitu Setelah peluang bisnis diidentifikasi, langkah berikutnya adalah membuat situs web atau platform E-Commerce yang sesuai dengan kebutuhan bisnis. Ini melibatkan desain situs, pengembangan, dan integrasi dengan SIA.
3. Pemasaran Online yaitu Pemasaran online adalah tahap penting dalam siklus ini. Ini mencakup promosi situs web atau platform E-Commerce melalui iklan online, media sosial, email marketing, dan strategi pemasaran digital lainnya.
4. Penerimaan Pesanan dan Transaksi yaitu Pelanggan mulai melakukan transaksi, memilih produk atau layanan, dan melakukan pembayaran melalui platform E-Commerce. SIA mencatat setiap transaksi ini secara otomatis.
5. Pengolahan Pesanan dan Pembayaran yaitu Setelah transaksi diterima, SIA digunakan untuk memproses pesanan, memeriksa ketersediaan barang, menghitung total harga, dan mengelola proses pembayaran. Ini mencakup integrasi dengan sistem pembayaran online.
6. Manajemen Persediaan yaitu SIA digunakan untuk mengelola persediaan produk atau layanan yang ditawarkan oleh perusahaan. Ini mencakup pemantauan stok, pengadaan, dan manajemen rantai pasokan.
7. Pengiriman dan Pengiriman Barang yaitu Jika bisnis melibatkan pengiriman barang fisik, SIA dapat digunakan untuk melacak pengiriman dan menyediakan informasi pelacakan kepada pelanggan.
8. Manajemen Hubungan Pelanggan yaitu SIA digunakan untuk memelihara hubungan pelanggan. Ini mencakup manajemen basis data pelanggan, dukungan pelanggan, dan analisis perilaku pelanggan.
9. Pengolahan Keuangan dan Akuntansi yaitu SIA berperan penting dalam mengelola aspek keuangan bisnis elektronik, termasuk pencatatan pendapatan, biaya operasional, pembayaran vendor, dan penyusunan laporan keuangan.

10. Analisis Data dan Pelaporan yaitu Data yang dihasilkan dari semua transaksi dan aktivitas bisnis online digunakan untuk analisis. SIA dapat menghasilkan laporan yang memberikan wawasan tentang kinerja bisnis, tren penjualan, dan lainnya.
11. Perbaikan Berkelanjutan (*Continuous Improvement*) yaitu Setelah semua data dikumpulkan dan dianalisis, perusahaan dapat mengambil tindakan perbaikan berkelanjutan untuk meningkatkan proses bisnis dan hasil.
12. Kepatuhan Hukum dan Keamanan Data yaitu Siklus ini juga mencakup kepatuhan hukum dan perlindungan data pelanggan. Perusahaan harus memastikan bahwa mereka mematuhi semua regulasi dan menjaga keamanan data pelanggan.

Siklus E-Commerce dan E-Business dalam SIA dan Bisnis adalah proses berkelanjutan yang mencakup berbagai aspek bisnis, termasuk penjualan, pemasaran, operasional, keuangan, dan manajemen pelanggan. SIA memainkan peran kunci dalam menyediakan data real-time dan analisis yang diperlukan untuk mengelola dan mengoptimalkan bisnis dalam lingkungan digital.

2.5 Konsep E-Commerce dan E-Business dalam Sistem Informasi Akuntansi (SIA) dan Bisnis.

Konsep E-Commerce dan E-Business dalam Sistem Informasi Akuntansi (SIA) dan Bisnis merujuk pada penerapan teknologi informasi dan komunikasi (TIK) dalam berbagai aspek bisnis, termasuk proses transaksi, manajemen operasional, pemasaran, dan analisis data. Berikut adalah gambaran lebih lanjut tentang kedua konsep ini dalam konteks SIA dan Bisnis yang pertama yaitu E-Commerce (Perdagangan Elektronik) adalah bagian dari E-Business yang terkait khusus dengan transaksi pembelian dan penjualan barang atau layanan melalui internet atau platform digital lainnya. dan Sistem Informasi Akuntansi (SIA) dalam E-Commerce mencakup pencatatan transaksi penjualan dan pembelian secara elektronik. Ini mencakup pemantauan inventaris, perhitungan pajak, pengelolaan akun pelanggan, dan penyusunan laporan keuangan yang relevan. sedangkan Bisnis yaitu E-Commerce memungkinkan bisnis untuk mencapai pasar global, meningkatkan

efisiensi dalam proses penjualan, dan memungkinkan pelanggan untuk berbelanja online. Ini melibatkan aktivitas seperti pembuatan toko online, pemrosesan pesanan online, dan integrasi sistem pembayaran. yang Kedua E-Business (Bisnis Elektronik) adalah konsep yang lebih luas daripada E-Commerce. Ini mencakup semua aktivitas bisnis yang menggunakan teknologi digital, termasuk E-Commerce, serta proses manajemen operasional, pemasaran, hubungan pelanggan, dan banyak lagi. dan Sistem Informasi Akuntansi (SIA) dalam E-Business mencakup lebih dari hanya pencatatan transaksi penjualan. Ini mencakup pengelolaan rantai pasokan, manajemen persediaan, manajemen pelanggan, analisis data, dan banyak aspek lainnya yang terkait dengan operasi bisnis yang lebih luas. serta Bisnis yaitu E-Business mengubah cara bisnis dijalankan. Ini memungkinkan perusahaan untuk meningkatkan efisiensi dalam manajemen operasional, memperbaiki interaksi dengan pelanggan, dan mengoptimalkan strategi bisnis secara keseluruhan.

Beberapa poin penting dalam hubungan antara E-Commerce, E-Business, SIA, dan Bisnis meliputi sebagai berikut

1. Integrasi Sistem: Untuk mencapai efektivitas maksimal, perusahaan perlu mengintegrasikan sistem informasi akuntansi dengan sistem E-Commerce dan E-Business mereka. Ini memungkinkan aliran data yang mulus dan akses yang lebih baik terhadap informasi bisnis yang penting.
2. Manajemen Data: SIA dalam konteks E-Commerce dan E-Business membantu perusahaan mengelola data transaksi, data pelanggan, dan data operasional lainnya. Data ini menjadi berharga untuk analisis bisnis dan pengambilan keputusan.
3. Keamanan dan Kepatuhan: Keamanan data dan kepatuhan terhadap regulasi adalah aspek penting dalam kedua konsep ini. Perusahaan perlu memastikan bahwa data pelanggan dan transaksi mereka aman dan bahwa mereka mematuhi semua aturan hukum yang berlaku.
4. Analisis Bisnis: E-Commerce dan E-Business menghasilkan banyak data yang dapat digunakan untuk analisis bisnis. SIA membantu perusahaan menganalisis data ini untuk memahami

tren, memprediksi permintaan pelanggan, dan meningkatkan strategi bisnis mereka.

Dalam era digital saat ini, E-Commerce dan E-Business telah menjadi elemen penting dari hampir setiap industri. Memahami bagaimana mereka berinteraksi dengan SIA dan bisnis adalah kunci untuk berhasil dalam lingkungan bisnis yang semakin terkoneksi secara digital (Bolek et al., 2023).

2.6 Manfaat dan Resiko Penggunaan E Commerce dan E Business dalan ekonomi di perusahaan

1. Manfaat Penggunaan E-Commerce dan E-Business antara lain

   Akses ke Pasar Global misal Perusahaan dapat mencapai pasar global dengan lebih mudah melalui platform E-Commerce, yang dapat meningkatkan pangsa pasar dan peluang pertumbuhan, Efisiensi Operasional seperti Proses bisnis dapat diotomatisasi dan disederhanakan dengan menggunakan E-Business, mengurangi biaya operasional dan meningkatkan produktivitas, Kenyamanan Pelanggan misalnya Pelanggan dapat berbelanja atau menggunakan layanan perusahaan secara online, memberikan kenyamanan dan fleksibilitas yang lebih besar, Pengumpulan Data yang Lebih Baik seperti E-Commerce dan E-Business menghasilkan banyak data, yang dapat digunakan untuk menganalisis perilaku pelanggan, mengidentifikasi tren pasar, dan membuat keputusan bisnis yang lebih baik, Kemampuan Personalisasi misalnya Berkat data pelanggan yang dikumpulkan, perusahaan dapat memberikan pengalaman yang lebih personal kepada pelanggan, termasuk rekomendasi produk yang relevan, Pengurangan Biaya Logistik seperti Dalam beberapa kasus, E-Commerce dapat membantu mengurangi biaya pengiriman dan logistik dengan mengintegrasikan sistem dan memungkinkan pemantauan persediaan secara real-time, Peningkatan Layanan Pelanggan misalnya E-Business memungkinkan perusahaan untuk memberikan dukungan pelanggan yang lebih baik melalui platform online, termasuk obrolan langsung dan layanan pelanggan (Octavia et al., 2020)

2. Bahaya Penggunaan E-Commerce dan E-Business antara lain

Keamanan Data misal Salah satu bahaya terbesar adalah risiko keamanan data. Pelanggaran keamanan data dapat mengakibatkan pencurian informasi pelanggan atau data bisnis yang sensitive, Kepatuhan Hukum misal Perusahaan harus mematuhi regulasi yang berkaitan dengan E-Commerce dan E-Business, termasuk privasi data, pajak, dan hukum perdagangan elektronik. Pelanggaran dapat mengakibatkan konsekuensi hukum dan denda, Persaingan yang Lebih Sengit seperti Dengan memasuki dunia online, perusahaan mungkin menghadapi persaingan yang lebih sengit dengan pesaing lokal dan global, Ketergantungan pada Teknologi misalnya Ketergantungan pada teknologi informasi membuat perusahaan rentan terhadap gangguan teknis, serangan siber, atau pemadaman sistem yang dapat berdampak besar pada operasi bisnis, Biaya Implementasi dan Perawatan seperti Implementasi dan pemeliharaan sistem E-Commerce dan E-Business dapat memakan biaya yang signifikan, terutama bagi bisnis kecil dan menengah, dan Kualitas Layanan misal Terkadang, interaksi dengan pelanggan secara online dapat mengurangi kualitas layanan personal dibandingkan dengan interaksi langsung serta Penipuan dan Penyalahgunaan seperti halnya ada potensi untuk penipuan pelanggan, penggunaan kartu kredit palsu, atau penyalahgunaan platform E-Commerce. dan Masalah Logistik seperti Pengiriman dan manajemen persediaan yang buruk dalam E-Commerce dapat mengakibatkan keterlambatan pengiriman dan pengalaman pelanggan yang buruk (Andonov et al., 2021) .

Dalam mengadopsi E-Commerce dan E-Business, perusahaan perlu mempertimbangkan manfaat dan risikonya dengan cermat (Siagian, 2021). Ini melibatkan perencanaan strategis yang matang, investasi dalam keamanan dan kepatuhan, serta pemantauan dan perbaikan berkelanjutan terhadap operasi bisnis digital mereka. Dengan perhatian yang tepat, banyak perusahaan dapat memanfaatkan potensi pertumbuhan dan efisiensi yang ditawarkan oleh E-Commerce dan E-Business(Saputri, 2017).

2.7 Metode Penggunaan E commerce dan E Business

Penggunaan E-Commerce (Perdagangan Elektronik) dan E-Business (Bisnis Elektronik) melibatkan berbagai metode dan strategi untuk mengimplementasikannya dengan sukses dalam konteks bisnis. Berikut adalah beberapa metode umum yang digunakan untuk memanfaatkan E-Commerce dan E-Business antara lain

1. Pembuatan dan Operasi Situs Web E-Commerce Salah satu metode paling dasar adalah menciptakan situs web E-Commerce yang memungkinkan perusahaan untuk menampilkan produk atau layanan mereka secara online. Ini dapat mencakup toko online dengan daftar produk, harga, dan informasi relevan,
2. Penggunaan Platform E-Commerce Banyak perusahaan menggunakan platform E-Commerce yang sudah ada, seperti Shopify, WooCommerce (untuk WordPress), Magento, atau BigCommerce. Platform-platform ini memiliki berbagai fitur dan alat yang mempermudah pengelolaan bisnis online.
3. Penggunaan Aplikasi Mobile Membangun aplikasi mobile khusus dapat menjadi metode yang efektif untuk memungkinkan pelanggan mengakses produk atau layanan perusahaan dengan mudah dari perangkat seluler mereka.
4. Penggunaan Marketplace Online yaitu Banyak perusahaan memanfaatkan marketplace online yang ada, seperti Amazon, eBay, atau Alibaba, untuk mencapai audiens yang lebih besar. Ini dapat menjadi metode cepat untuk memulai E-Commerce.
5. Pemasaran Digital yaitu Metode pemasaran digital, termasuk iklan online, kampanye iklan sosial media, SEO (Search Engine Optimization), dan pemasaran konten, digunakan untuk menjangkau dan menarik pelanggan potensial.
6. Integrasi sistem adalah kunci untuk menghubungkan berbagai komponen bisnis seperti Sistem Informasi Akuntansi (SIA), manajemen inventaris, dan manajemen pelanggan dengan platform E-Commerce atau E-Business. Hal ini memungkinkan aliran data yang efisien dan analisis yang lebih baik.

7. Manajemen Rantai Pasokan Terhubung seperti Integrasi dengan pemasok dan mitra bisnis dalam rantai pasokan juga penting dalam E-Business. Metode ini memungkinkan perusahaan untuk memantau dan mengelola persediaan dan produksi dengan lebih efisien.
8. Analisis Data Pengumpulan dan analisis data adalah metode penting untuk memahami perilaku pelanggan, mengidentifikasi tren, dan mengambil keputusan bisnis yang lebih baik.
9. Penggunaan Keamanan Data Implementasi protokol keamanan yang kuat dan pemantauan aktif keamanan data adalah metode yang penting untuk melindungi informasi pelanggan dan data bisnis dari ancaman siber.
10. Pengembangan Layanan Pelanggan Online Dalam E-Business, pengembangan layanan pelanggan online seperti chatbot, dukungan pelanggan, dan penanganan keluhan melalui platform digital dapat meningkatkan pengalaman pelanggan.
11. Personalisasi Konten dan Rekomendasi Penggunaan teknik personalisasi konten dan rekomendasi produk berdasarkan data pelanggan dapat meningkatkan retensi pelanggan dan penjualan lintas produk.

Setiap perusahaan harus memilih metode yang sesuai dengan tujuan bisnis mereka, target pasar, dan sumber daya yang tersedia. Penting untuk mengembangkan strategi yang komprehensif yang mencakup semua aspek penggunaan E-Commerce dan E-Business, dari pembuatan situs web hingga pemasaran, manajemen operasional, dan keamanan.

2.8 Penutup

Dalam konteks bisnis dan ekonomi, E-Commerce (Perdagangan Elektronik) dan E-Business (Bisnis Elektronik) telah menjadi faktor yang sangat signifikan dalam mengubah cara perusahaan beroperasi dan berinteraksi dengan pelanggan (Siagian & Wijoyo, 2021). Kesimpulan utama yang dapat diambil dari diskusi di atas adalah sebagai berikut Penggunaan Teknologi Digital, E-Commerce dan E-Business mengandalkan teknologi digital dan internet untuk mengotomatisasi proses bisnis, memungkinkan

akses ke pasar global, dan memberikan layanan yang lebih baik kepada pelanggan(Siagian et al., 2020), manfaat Bisnis seperti Implementasi E-Commerce dan E-Business dapat membawa banyak manfaat, termasuk peningkatan efisiensi operasional, peningkatan akses pasar, personalisasi layanan pelanggan, dan pengumpulan data yang lebih baik untuk analisis bisnis, tantangan dan risiko meskipun ada banyak manfaat, penggunaan E-Commerce dan E-Business juga membawa tantangan dan risiko, termasuk risiko keamanan data, kepatuhan hukum, persaingan yang lebih sengit, biaya implementasi, dan masalah logistic, Integrasi Sistem seperti Integrasi sistem informasi akuntansi (SIA) dengan E-Commerce dan E-Business penting untuk memastikan aliran data yang mulus dan akses yang lebih baik terhadap informasi bisnis dan Keamanan dan Kepatuhan karena Keamanan data dan kepatuhan terhadap regulasi adalah aspek yang harus diperhatikan dengan serius, untuk melindungi informasi sensitif dan menjaga reputasi perusahaan (Givan et al., 2020), selanjutnya pengambilan keputusan yang Lebih Baik sebab data yang dihasilkan dari aktivitas E-Commerce dan E-Business dapat digunakan untuk analisis bisnis yang mendalam, membantu perusahaan membuat keputusan yang lebih baik dalam strategi dan operasi mereka. Dalam era digital yang terus berkembang, penggunaan E-Commerce dan E-Business menjadi semakin penting bagi perusahaan untuk tetap kompetitif dan relevan dalam pasar yang terus berubah. Namun, perusahaan harus mengelola tantangan dan risiko ini dengan bijak melalui perencanaan yang matang dan investasi dalam keamanan serta pengembangan teknologi informasi yang efisien.

DAFTAR PUSTAKA

Amit, R., & Zott, C. 2001. Value creation in e-business. *Strategic Management Journal*. https://doi.org/10.1002/smj.187

Andonov, A., Dimitrov, G. P., & Totev, V. 2021. Impact of E-commerce on Business Performance. *TEM Journal*. https://doi.org/10.18421/TEM104-09

Bolek, V., Romanová, A., & Korček, F. 2023. The Information Security Management Systems in E-Business. *Journal of Global Information Management*. https://doi.org/10.4018/JGIM.316833

Fernández-Bonilla, F., Gijón, C., & De la Vega, B. 2022. E-commerce in Spain: Determining factors and the importance of the e-trust. *Telecommunications Policy*. https://doi.org/10.1016/j.telpol.2021.102280

Fitriani, D. 2023. Peranan Sistem Informasi Manajemen Terhadap Perkembangan E-Commerce Dalam Pengambilan Keputusan Bagi Usaha UMKM. *Jkpim : Jurnal Kajian Dan Penalaran Ilmu Manajemen*.

Givan, B., Indrawan, H. E., & Siagian, A. O. 2020. Pelatihan Membuat Business Plan Bagi Pemuda Karang Taruna RW 01 Pinangsia Taman Sari Jakarta. *Jurnal Karya Untuk Masyarakat (JKuM)*. https://doi.org/10.36914/jkum.v1i2.396

Gusti, I., Karmawan, M., Kom, S., Sundjaja, A. M., Luhukay, D., & Akuntansi, J. K. 2010. ANALISIS DAN PERANCANGAN E-COMMERCE PD. GARUDA JAYA. *Seminar Nasional Aplikasi Teknologi Informasi*.

Munoz, F., Holsapple, C. W., & Sasidharan, S. 2023. E-commerce. In *Springer Handbooks*. https://doi.org/10.1007/978-3-030-96729-1_67

Octavia, A., Indrawijaya, S., Sriayudha, Y., Heriberta, Hasbullah, H., & Asrini. 2020. Impact on e-commerce adoption on entrepreneurial orientation and market orientation in business performance of smes. *Asian Economic and Financial Review*. https://doi.org/10.18488/journal.aefr.2020.105.516.525

Rehatalanit, Y. L. . 2021. Peran E-Commerce Dalam Pengembangan Bisnis. *Jurnal Teknologi Industri*.

Saputri, A. 2017. E-Commerce Dan E-Business. *Jurnal Ekonomi & Bisnis*.

Siagian, A. O. 2021. *Lembaga-lembaga Keuangan dan Perbankan Pengertian, Tujuan, dan Fungsinya - Ade Onny Siagian - Google Buku*. 4 Mar Et.

Siagian, A. O., Martiwi, R., & Indra, N. 2020. Manajemen Pemasaran. *Jurnal Pemasaran Kompetitif*.

Siagian, A. O., & Wijoyo, H. 2021. kepuasaan pelanggan. *Insight Management Journal*.

Tamilarasi, R., & Elamathi, N. 2020. E-COMMERCE- BUSINESS-TECHNOLOGY- SOCIETY. *International Journal of Engineering Technologies and Management Research*. https://doi.org/10.29121/ijetmr.v4.i10.2017.103

Tumpal Manik. 2018. Analysis of the Role of Accounting Information Systems in E-Commerces Against Online Business Control. *Jurnal Ilmiah Akuntansi Dan Finansial Indonesia*.

BAB 3
MANAJEMEN DATA DAN DATABASE

Oleh Denny Rakhmad Widi Ashari

3.1 Pendahuluan

Kita akan menjelajahi pentingnya manajemen data dan database dalam konteks Sistem Informasi Akuntansi dan Bisnis (SIAB) serta bagaimana aspek-aspek ini membantu perusahaan untuk mencapai kesuksesan dalam dunia bisnis yang berubah dengan cepat. Salah satunya manajemen data dan database dapat membantu perusahaan dalam mengumpulkan dan mengelola data dengan akurat dan transparan, sehingga memungkinkan perusahaan untuk mengambil keputusan yang lebih baik dan efisien (Sabatini and Sudana, 2019). Juga, manajemen data dan database dapat membantu perusahaan dalam mengumpulkan dan menganalisis data karakteristik perusahaan dan kinerja perusahaan untuk mendukung pengambilan keputusan terkait manajemen laba (Tang and Fiorentina, 2021). Terakhir, manajemen data dan database dapat membantu perusahaan dalam membuat strategi pemasaran (Ashari, 2023) dan menganalisis data terkait aktivitas riil perusahaan (Sari and Pinasthika, 2021). Dalam keseluruhan, manajemen data dan database memainkan peran kunci dalam Sistem Informasi Akuntansi dan Bisnis (SIAB). Dengan mengoptimalkan penggunaan data melalui manajemen data yang baik, perusahaan dapat mendukung pengambilan keputusan yang lebih baik dan efisien. Referensi yang telah disebutkan memberikan pemahaman yang lebih mendalam tentang pentingnya manajemen data dan database dalam konteks Sistem Informasi Akuntansi dan Bisnis, serta bagaimana aspek-aspek ini membantu manajemen untuk mencapai kesuksesan dalam dunia bisnis di era distrupsi (Al Haris, Ashari and Rifa'i, 2023).

3.2 Pengertian Manajemen Data dan Database

Manajemen data adalah proses pengumpulan, penyimpanan, pengolahan, dan penggunaan data secara efektif untuk mendukung pengambilan keputusan dan operasi bisnis (LaBonte, 2016), dengan tujuan untuk mengelola informasi dengan efisien, meningkatkan keamanan data, meningkatkan efisiensi operasional, mendukung pengembangan aplikasi dan sistem, serta memastikan kepatuhan perusahaan terhadap peraturan dan standar yang berlaku (LaBonte, 2016) (Frerichs, 2016).

Menurut Andaru, Basis data atau *database* adalah sekumpulan data yang tersimpan dalam komputer dengan tatacara tertentu, memungkinkan penggunaan program komputer untuk mengambil informasi dari basis data tersebut (Andaru, 2018).

Database menurut Wijoyo adalah sistem berkas komputer yang menggunakan pengaturan khusus dengan tujuan untuk meningkatkan pembaruan setiap rekaman serta pembaruan bersama pada rekaman terkait. Selain itu, ini bertujuan untuk mempermudah dan mempercepat akses ke semua rekaman melalui program aplikasi, serta akses yang cepat ke data yang disimpan yang diperlukan untuk dibaca bersama-sama guna penyusunan laporan rutin atau laporan khusus (Wijoyo *et al.*, 2021).

Jadi *database* adalah kumpulan data yang terstruktur di dalam komputer dengan pengaturan tertentu agar pengguna dapat menggunakan program komputer untuk mengambil informasi dari basis data tersebut yang berbentuk sistem berkas komputer didesain dengan konfigurasi khusus, bertujuan untuk memfasilitasi pembaruan dan akses yang cepat terhadap rekaman, terutama untuk menyusun laporan rutin dan khusus.

3.3 Tujuan Manajemen Data

Adapun tujuan utama dari manajemen data secara detail dapat disebutkan sebagai berikut (LaBonte, 2016) :

1. Menyediakan aksesibilitas dan keandalan data. Dengan menggunakan database yang baik, perusahaan dapat mengelola data dengan lebih efisien dan menghindari kehilangan atau kerusakan data.

2. Memungkinkan perusahaan untuk mengintegrasikan data dari berbagai sumber yang berbeda, sehingga memungkinkan analisis yang lebih komprehensif dan pengambilan keputusan yang lebih baik.
3. Keamanan data juga menjadi tujuan penting dalam manajemen data. Dengan menggunakan sistem manajemen data yang baik, perusahaan dapat menerapkan kontrol akses yang ketat untuk melindungi data sensitif dan menghindari kebocoran data, database juga dapat dilengkapi dengan fitur keamanan seperti enkripsi data dan pencatatan aktivitas pengguna, yang membantu dalam mendeteksi dan mencegah ancaman keamanan.
4. Efisiensi operasional juga menjadi tujuan yang penting dalam manajemen data. Dengan menggunakan database yang terstruktur, perusahaan dapat mengelola data dengan lebih efisien dan menghindari duplikasi data yang tidak perlu, database juga memungkinkan perusahaan untuk melakukan analisis data yang lebih cepat dan akurat, sehingga memungkinkan pengambilan keputusan yang lebih baik dan respons yang lebih cepat terhadap perubahan pasar.
5. Mendukung pengembangan aplikasi dan sistem perusahaan. Dengan menggunakan database yang baik, perusahaan dapat mengintegrasikan data dengan aplikasi dan sistem yang ada, sehingga memungkinkan pengembangan dan pemeliharaan sistem yang lebih efisien dan juga manajemen data juga memungkinkan perusahaan untuk melakukan analisis data yang lebih mendalam dan menghasilkan wawasan yang berharga untuk pengembangan produk dan strategi bisnis.
6. Berperan dalam memastikan kepatuhan perusahaan terhadap peraturan dan standar yang berlaku. Dengan menggunakan database yang baik, perusahaan dapat dengan mudah mengelola dan melacak data yang diperlukan untuk memenuhi persyaratan peraturan seperti perlindungan data pribadi dan pelaporan keuangan.

7. Membantu perusahaan menjaga konsistensi dan integritas data, yang penting dalam memastikan kepatuhan terhadap standar dan prosedur yang ditetapkan.

3.4 Peran Manajemen Data dan Database Dalam Perusahaan

Peran manajemen data dan database dalam perusahaan sangat penting dalam mengelola informasi dan memastikan efisiensi operasional. Manajemen data melibatkan pengumpulan, penyimpanan, pengolahan, dan penggunaan data secara efektif untuk mendukung pengambilan keputusan dan operasi bisnis (Tahmidi, Oktaroza and Hartanto, 2022). Dalam konteks ini, database berperan sebagai tempat penyimpanan data yang terstruktur dan terorganisir, yang memungkinkan akses dan manipulasi data dengan mudah (Budianto, Fauzi and Santosa, 2022).

Salah satu peran utama manajemen data dan database adalah menyediakan aksesibilitas dan keandalan data. Dengan menggunakan database yang baik, perusahaan dapat mengelola data dengan lebih efisien dan menghindari kehilangan atau kerusakan data (Budianto, Fauzi and Santosa, 2022). Selain itu, manajemen data dan database juga memungkinkan perusahaan untuk mengintegrasikan data dari berbagai sumber yang berbeda, sehingga memungkinkan analisis yang lebih komprehensif dan pengambilan keputusan yang lebih baik (Tahmidi, Oktaroza and Hartanto, 2022).

Selain itu, manajemen data dan database juga berperan dalam menjaga keamanan data perusahaan. Dengan menggunakan sistem manajemen data yang baik, perusahaan dapat menerapkan kontrol akses yang ketat untuk melindungi data sensitif dan menghindari kebocoran data. Selain itu, database juga dapat dilengkapi dengan fitur keamanan seperti enkripsi data dan pencatatan aktivitas pengguna, yang membantu dalam mendeteksi dan mencegah ancaman keamanan (Budianto, Fauzi and Santosa, 2022).

Manajemen data dan database juga berperan dalam meningkatkan efisiensi operasional perusahaan. Dengan

menggunakan database yang terstruktur, perusahaan dapat mengelola data dengan lebih efisien dan menghindari duplikasi data yang tidak perlu (Budianto, Fauzi and Santosa, 2022). Selain itu, database juga memungkinkan perusahaan untuk melakukan analisis data yang lebih cepat dan akurat, sehingga memungkinkan pengambilan keputusan yang lebih baik dan respons yang lebih cepat terhadap perubahan pasar (Tahmidi, Oktaroza and Hartanto, 2022).

Selain itu, manajemen data dan database juga berperan dalam mendukung pengembangan aplikasi dan sistem perusahaan. Dengan menggunakan database yang baik, perusahaan dapat mengintegrasikan data dengan aplikasi dan sistem yang ada, sehingga memungkinkan pengembangan dan pemeliharaan sistem yang lebih efisien (Budianto, Fauzi and Santosa, 2022). Selain itu, manajemen data dan database juga memungkinkan perusahaan untuk melakukan analisis data yang lebih mendalam dan menghasilkan wawasan yang berharga untuk pengembangan produk dan strategi bisnis (Tahmidi, Oktaroza and Hartanto, 2022).

Dalam konteks perusahaan, manajemen data dan database juga berperan dalam mendukung kepatuhan perusahaan terhadap peraturan dan standar yang berlaku. Dengan menggunakan database yang baik, perusahaan dapat dengan mudah mengelola dan melacak data yang diperlukan untuk memenuhi persyaratan peraturan seperti perlindungan data pribadi dan pelaporan keuangan (Budianto, Fauzi and Santosa, 2022). Selain itu, manajemen data dan database juga memungkinkan perusahaan untuk menjaga konsistensi dan integritas data, yang penting dalam memastikan kepatuhan terhadap standar dan prosedur yang ditetapkan (Tahmidi, Oktaroza and Hartanto, 2022).

3.5 Kegiatan Manajemen Data

Kegiatan manajemen data merupakan proses yang penting dalam pengelolaan informasi dan pengambilan keputusan di berbagai bidang, termasuk bisnis, pendidikan, dan pemerintahan. Dalam era digital saat ini, penggunaan sistem informasi manajemen telah menjadi hal yang umum dan penting dalam mengelola data dengan efisien dan efektif. Adapun kegiatan manajemen data adalah

sebagai berikut seperti perancangan, implementasi, dan pengelolaan kegiatan manajemen data berdasarkan referensi yang relevan dan berkualitas.

3.5.1 Pengumpulan Data

Dalam pengumpulan data, dokumen sumber berperan sebagai formulir yang digunakan untuk mencatat data yang diperlukan. Dokumen sumber ini berfungsi sebagai input bagi sistem yang akan mengelola data tersebut. Dokumen sumber adalah formulir yang digunakan untuk mengumpulkan dan mencatat data yang diperlukan. Dokumen sumber ini berperan sebagai input bagi sistem yang akan mengelola data tersebut. Dalam konteks pengumpulan data, dokumen sumber sangat penting karena merupakan sumber informasi yang digunakan untuk mengumpulkan data yang diperlukan dalam suatu perusahaan atau organisasi (Han, Kamber and Pei, 2012).

Dalam konteks perusahaan, pengumpulan data yang baik dan efektif sangat penting untuk mendukung pengambilan keputusan yang tepat dan operasi bisnis yang efisien. Data yang dikumpulkan melalui dokumen sumber dan metode pengumpulan data yang tepat dapat digunakan untuk menganalisis kinerja perusahaan, mengidentifikasi tren pasar, dan mengembangkan strategi bisnis yang efektif (Agustia, 2013) (Devi, Budiasih and Badera, 2017).

Dalam pengumpulan data, juga penting untuk memperhatikan kepatuhan terhadap peraturan dan standar yang berlaku. Pengungkapan informasi nonfinansial dalam laporan keuangan merupakan salah satu aspek penting dalam pengumpulan data. Pengungkapan ini dapat membantu perusahaan memenuhi persyaratan peraturan dan memberikan informasi yang relevan kepada pemangku kepentingan perusahaan (Swarte *et al.*, 2020).

3.5.2 Integritas dan pengujian

Dalam dunia bisnis yang terus berkembang, data adalah aset berharga. Data yang akurat dan konsisten adalah pondasi bagi pengambilan keputusan yang baik, pengembangan strategi bisnis, dan pelaporan keuangan yang sah. Oleh karena itu, penting untuk

memahami integritas data dan peran pengujian data dalam memastikan bahwa data yang digunakan dalam perusahaan adalah benar dan andal. Integritas dan pengujian data merupakan aspek penting dalam manajemen data. Integritas data mengacu pada keutuhan dan konsistensi data, sedangkan pengujian data dilakukan untuk memastikan konsistensi dan akurasi data berdasarkan peraturan dan kendala yang telah ditentukan sebelumnya (Septian, Fachrudin and Nugroho, 2019) (Hastari and Bimantoro, 2018).

Integritas data adalah kualitas keandalan dalam menyajikan informasi yang akurat, lengkap, dan dapat dipercaya (Milda Putri and Yanti, 2022). Dalam konteks laporan keuangan, integritas laporan keuangan mengacu pada sejauh mana informasi yang disajikan dalam laporan keuangan dapat diandalkan dalam pengambilan keputusan (Wulan and Suzan, 2022). Integritas laporan keuangan juga mencakup kualitas keandalan, seperti verifiability (memiliki pendapat yang sama) dan representational faithfulness (kesesuaian dengan realitas) (Milda Putri and Yanti, 2022). Dengan kata lain integritas data adalah konsep yang berkaitan dengan kualitas dan keandalan data dalam sebuah sistem. Ini mengacu pada sejauh mana data adalah akurat, konsisten, dan sesuai dengan peraturan serta kendala yang telah ditentukan sebelumnya. Integritas data merupakan faktor kunci dalam memastikan bahwa informasi yang dihasilkan dari data tersebut dapat diandalkan.

Pengujian data adalah proses yang dirancang untuk memeriksa data yang tersimpan dalam basis data perusahaan. Tujuan utama pengujian data adalah memastikan bahwa data tersebut memenuhi kriteria integritas yang telah ditetapkan. Inilah bagaimana data diperiksa untuk meyakinkan konsistensi dan akurasinya berdasarkan peraturan dan kendala yang telah ditentukan sebelumnya. Pengujian integritas data juga dapat dilakukan dalam konteks pengelolaan basis data (Rahma *et al.*, 2021).

Integritas dan pengujian data merupakan aspek penting dalam manajemen data. Integritas data memastikan keutuhan dan konsistensi data, sedangkan pengujian data dilakukan untuk memastikan konsistensi dan akurasi data berdasarkan peraturan

dan kendala yang telah ditentukan sebelumnya. Pengujian data dapat dilakukan dalam berbagai konteks, seperti pengujian akurasi aplikasi atau sistem, pengujian kepatuhan terhadap peraturan, dan pengujian intensitas ancaman keamanan. Dengan melakukan integritas dan pengujian data yang baik, perusahaan dapat memastikan bahwa data yang digunakan dalam pengambilan keputusan dan operasi bisnis adalah akurat dan konsisten.

3.5.3 Penyimpanan

Penyimpanan data adalah salah satu elemen paling krusial dalam dunia teknologi informasi. Saat kita berbicara tentang penyimpanan data, kita merujuk pada tempat di mana segala informasi berharga disimpan dan dengan mudah diakses saat diperlukan. Penyimpanan data merupakan proses dimana data disimpan pada suatu medium, seperti pita magnetik atau piringan magnetik. Medium penyimpanan ini digunakan untuk menyimpan data dalam bentuk fisik agar dapat diakses dan digunakan kembali di kemudian hari (Irawati and Fitriyani, 2022). Dalam perkembangan teknologi, format penyimpanan data telah mengalami perubahan dengan adanya penyimpanan data dalam bentuk digital, seperti dalam basis data berbasis web (Seto *et al.*, 2022).

Pemanfaatan teknologi dalam penyimpanan data juga memberikan keuntungan dalam mengontrol duplikasi data. Dalam format penyimpanan data berbasis web, duplikasi data dapat dihindari dengan lebih mudah (Seto *et al.*, 2022). Selain itu, teknologi cloud computing juga telah digunakan sebagai media penyimpanan data. Penelitian menunjukkan bahwa pemanfaatan teknologi cloud computing dapat mempermudah pengguna dalam mengakses data di mana pun melalui internet (Todingbua and Setiyawati, 2022).

Pentingnya penyimpanan data juga terlihat dalam berbagai sektor, seperti bisnis dan pemerintahan. Dalam bisnis, penyimpanan data yang efektif dapat meningkatkan kepuasan pelanggan dan mempengaruhi niat pelanggan untuk melakukan pembelian ulang (Wiradarma and Respati, 2020). Dalam konteks keuangan, penyimpanan data juga memiliki peran penting. Peningkatan literasi

keuangan digital pada pelaku usaha mikro, kecil, dan menengah (UMKM) melalui sosialisasi gerakan nasional non-tunai dapat membantu meningkatkan efisiensi dalam penyimpanan dan pengelolaan data keuangan (Lestari, Santoso and Indarto, 2021) (Al Haris and Ashari, 2023). Selain itu, dalam laporan keuangan organisasi perangkat daerah, kualitas laporan keuangan juga dipengaruhi oleh faktor-faktor yang berkaitan dengan penyimpanan data (Khoirunisa and Ahmad, 2022).

Dalam kesimpulannya, penyimpanan data merupakan proses penting dalam berbagai bidang, seperti bisnis, pemerintahan, pendidikan, keuangan, dan teknologi. Pemanfaatan teknologi dalam penyimpanan data, seperti basis data berbasis web dan teknologi cloud computing, memberikan kemudahan dalam mengontrol duplikasi data dan meningkatkan aksesibilitas data. Selain itu, penyimpanan data juga memiliki peran penting dalam meningkatkan kepuasan pelanggan, efisiensi pengelolaan data keuangan, dan pengembangan sistem teknologi.

3.5.4 Pemeliharaan

Pemeliharaan data merupakan suatu proses yang penting dalam menjaga keberlanjutan dan mutakhirnya sumberdaya data atau berkas. Proses pemeliharaan data meliputi penambahan data baru, perubahan data yang sudah ada, dan penghapusan data yang tidak lagi diperlukan. Tujuan dari pemeliharaan data adalah untuk memastikan bahwa data yang tersedia tetap relevan, akurat, dan up-to-date.

Dalam era di mana volume data terus meningkat, penambahan data baru adalah langkah yang penting. Data baru dapat berasal dari berbagai sumber, termasuk transaksi bisnis, interaksi pelanggan, survei, dan banyak lagi. Setiap kali data baru ditambahkan, potensi peningkatan pengetahuan dan pemahaman organisasi semakin berkembang. Penting untuk memastikan bahwa data baru yang ditambahkan diintegrasikan dengan baik ke dalam sistem yang ada dan bahwa formatnya sesuai dengan standar yang telah ditetapkan. Ini akan memungkinkan data baru ini bergabung dengan informasi yang ada, memperkaya pengetahuan, dan memastikan konsistensi data (Prabowo *et al.*, 2022).

Pemeliharaan data adalah bagian integral dari manajemen data yang sukses. Ini melibatkan penambahan data baru untuk memperkaya pengetahuan, perubahan data yang ada untuk menjaga akurasi, dan penghapusan data yang tidak lagi diperlukan untuk menghindari kepadatan yang tidak perlu. Dengan pemeliharaan data yang baik, organisasi dapat memastikan bahwa data mereka tetap relevan, andal, dan berguna dalam mengambil keputusan dan mencapai tujuan bisnis.

3.5.5 Keamanan

Keamanan data merupakan hal yang sangat penting dalam era digital saat ini. Data harus dijaga dengan baik untuk mencegah penghancuran, kerusakan, atau penyalahgunaan. Salah satu aspek penting dalam keamanan IT adalah melindungi sumber daya yang diakses oleh beberapa pengguna (Pamuji, 2022). Hal ini menunjukkan bahwa keamanan data tidak hanya melibatkan perlindungan terhadap data itu sendiri, tetapi juga perlindungan terhadap akses dan penggunaan data oleh pihak yang tidak berwenang. Dalam sistem informasi, keamanan data menjadi masalah yang terus dikembangkan, seperti mengembangkan metode dan teknik yang dapat menjaga keamanan data dalam sistem (Handoko and Abdussalam, 2022).

Kepercayaan dan persepsi risiko terhadap keamanan konsumen memiliki implikasi terhadap minat beli, sehingga perlu melakukan pengontrolan dan penjagaan keamanan atas transaksi data untuk membangun kepercayaan konsumen (Wahyuni and Dahmiri, 2021). Dalam dunia bisnis, keamanan data juga menjadi faktor penting dalam pembentukan kepercayaan konsumen. Jaminan keamanan berperan penting dalam pembentukan kepercayaan dengan mengurangi perhatian konsumen tentang penyalahgunaan data pribadi dan transaksi data yang mudah rusak (Kusuma, 2019). Oleh karena itu, perusahaan perlu menjaga keamanan data konsumen untuk membangun kepercayaan dan loyalitas konsumen.

Keamanan data adalah langkah yang sangat penting dalam dunia yang semakin terhubung secara digital ini. Data adalah aset berharga yang harus dijaga dengan baik dari segala potensi

ancaman. Dengan tindakan yang tepat, seperti pemulihan bencana, perlindungan dari kerusakan, dan pencegahan penyalahgunaan data, individu dan organisasi dapat memastikan bahwa data mereka tetap aman, andal, dan sesuai dengan peraturan yang berlaku. Keamanan data adalah langkah pertama dalam menjaga nilai dan integritas informasi dalam era digital ini.

3.5.6 Organisasi Data

Organisasi data adalah langkah penting dalam manajemen informasi yang efektif. Ini memungkinkan organisasi untuk memanfaatkan data dengan lebih baik, mendukung pengambilan keputusan, dan menjaga kualitas data. Dengan pemahaman yang baik tentang organisasi data, organisasi dapat memaksimalkan nilai dari aset data mereka dan memenuhi kebutuhan informasi pemakai dengan lebih baik, organisasi perlu mengelola data dengan baik untuk memenuhi kebutuhan informasi pemakai. Data yang disusun dengan baik akan memudahkan pemakai dalam mengakses informasi yang mereka butuhkan.

Organisasi data adalah proses pengaturan dan penyusunan data sedemikian rupa sehingga dapat diakses dan dimanfaatkan dengan efisien. Dalam organisasi data, data disusun dalam struktur yang teratur dan terorganisir agar dapat dengan mudah ditemukan dan digunakan. Struktur data yang umum digunakan dalam organisasi data adalah struktur hierarkis, struktur jaringan, dan struktur relasional (Mutaufiq, 2021).

Dapat disimpulkan bahwa organisasi perlu mengelola data dengan baik untuk memenuhi kebutuhan informasi pemakai. Sistem informasi eksekutif dan teknologi informasi dapat digunakan untuk memudahkan pemakai dalam mengakses dan menganalisis data. Dengan memenuhi kebutuhan informasi pemakai, organisasi dapat berfungsi dengan baik dan mencapai tujuan yang telah ditetapkan.

3.5.7 Pengambilan data

Pengambilan data adalah elemen penting dalam dunia yang semakin terhubung secara digital ini. Akses ke informasi adalah kunci untuk pengambilan keputusan yang baik, perkembangan bisnis, dan kemajuan teknologi. Dengan sistem yang baik dan

teknologi yang tepat, data tersedia bagi pemakai, memberikan manfaat yang besar dalam berbagai aspek kehidupan dan bisnis. Hal ini memungkinkan pengguna untuk menjalani hidup yang lebih efisien dan terinformasi, serta membantu organisasi untuk mencapai kesuksesan yang lebih besar dalam dunia yang terus berubah dengan cepat ini.

3.6 Kesimpulan

Manajemen data dan database memegang peran penting dalam pengelolaan informasi di berbagai bidang, khususnya dalam konteks perusahaan dan organisasi. Mereka memberikan landasan untuk pengumpulan, penyimpanan, pengolahan, dan penggunaan data secara efektif, yang mendukung pengambilan keputusan yang cerdas dan operasi bisnis yang lancar. Dalam kesimpulan, manajemen data dan database adalah fondasi penting dalam pengelolaan informasi di berbagai sektor. Mereka memberikan alat yang diperlukan untuk mengoptimalkan penggunaan data, memastikan keamanan, meningkatkan efisiensi, mendukung pengembangan, dan memenuhi persyaratan peraturan. Dengan pendekatan yang tepat terhadap manajemen data, perusahaan dapat memanfaatkan aset berharga ini untuk meraih keberhasilan dan kompetitivitas yang lebih besar di dunia bisnis yang terus berkembang.

DAFTAR PUSTAKA

Agustia, D. 2013. 'Pengaruh Faktor Good Corporate Governance, Free Cash Flow, dan Leverage Terhadap Manajemen Laba', *Jurnal Akuntansi dan Keuangan*, 15(1). Available at: https://doi.org/10.9744/jak.15.1.27-42.

Andaru, A. 2018. 'Pengertian database secara umum', *OSF Prepr*, 2.

Ashari, D.R.W. 2023. '9.3 Strategi Pemasaran Produk Konsumen di Pasar Global', *STRATEGI PEMASARAN*, p. 184.

Budianto, F.A., Fauzi, R. and Santosa, I. 2022. 'Perancangan Enterprise Architecture Dengan TOGAF ADM 9.2 Pada Fungsi Business Planning and Performance Pada PT XYZ', *Jurnal Ilmiah Teknologi Informasi Asia*, 16(2), p. 75. Available at: https://doi.org/10.32815/jitika.v16i2.757.

Devi, S., Budiasih, I.G.N. and Badera, I.D.N. 2017. 'PENGARUH PENGUNGKAPAN ENTERPRISE RISK MANAGEMENT DAN PENGUNGKAPAN INTELLECTUAL CAPITAL TERHADAP NILAI PERUSAHAAN', *Jurnal Akuntansi dan Keuangan Indonesia*, 14(1), pp. 20–45. Available at: https://doi.org/10.21002/jaki.2017.02.

Han, J., Kamber, M. and Pei, J. 2012. 'Data Mining: Concepts and Techniques', *Choice Reviews Online* [Preprint]. Available at: https://doi.org/10.5860/choice.49-3305.

Handoko, L.B. and Abdussalam, A. 2022. 'Text Security Using Vigenere Cipher and Hill Cipher', *Bit (Fakultas Teknologi Informasi Universitas Budi Luhur)*, 19(1), p. 37. Available at: https://doi.org/10.36080/bit.v19i1.1790.

Al Haris, M.B. and Ashari, D.R.W. (2023) 'DAMPAK KEBIJAKAN OJK RESTRUKTURISASI TERHADAP LEMBAGA JASA KEUANGAN KEDIRI RAYA DI MASA PANDEMI COVID-19', *ESPAS: Jurnal Ekonomi dan Perbankan*, 1(1), pp. 16–29.

Al Haris, M.B., Ashari, D.R.W. and Rifa'i, A. (2023) 'Strategi Manajemen Pemasaran Syariah pada BPR Arsindo Kediri di Era Disrupsi', *SINDA: Comprehensive Journal of Islamic Social Studies*, 3(2), pp. 59–68. Available at: https://doi.org/10.28926/SINDA.V3I2.1086.

Hastari, D. and Bimantoro, F. (2018) 'Sistem Pakar Diagnosa Gangguan Mental pada Anak dengan Metode Dempster Shafer', *Journal of Computer Science and Informatics Engineering (J-Cosine)*, 2(2), pp. 71–79. Available at: https://doi.org/10.29303/jcosine.v2i2.106.

Irawati, N. and Fitriyani, E.N. (2022) 'Faktor-Faktor yang Memengaruhi Minat Sedekah Non Tunai', *Journal of Islamic Economics and Finance Studies*, 3(2), p. 179. Available at: https://doi.org/10.47700/jiefes.v3i2.4779.

Khoirunisa, N. and Ahmad, A. (2022) 'Faktor-Faktor Yang Mempengaruhi Kualitas Laporan Keuangan Pada Organisasi Perangkat Daerah Kabupaten Jember', *Jurnal Akuntansi Terapan dan Bisnis*, 2(1), pp. 82–91. Available at: https://doi.org/10.25047/asersi.v2i1.3189.

Kusuma, A. (2019) 'Analisis Faktor-Faktor Yang Berpengaruh Terhadap Keputusan Pembelian Secara Online di Website Tokopedia (Studi Kasus pada Mahasiswa di Universitas Islam Indonesia)', *Journal Competency of Business*, 3(1), pp. 65–79. Available at: https://doi.org/10.47200/jcob.v3i1.670.

LaBonte, K. (2016) 'Data Management for Researchers: Organize, Maintain and Share Your Data for Research Success.', *Issues in Science and Technology Librarianship* [Preprint], (84). Available at: https://doi.org/10.29173/istl1683.

Lestari, R.I., Santoso, D. and Indarto, I. (2021) 'Meningkatkan literasi keuangan digital pada pelaku UMKM melalui sosialisasi gerakan nasional non-tunai', *Jurnal Inovasi Hasil Pengabdian Masyarakat (JIPEMAS)*, 4(3), p. 378. Available at: https://doi.org/10.33474/jipemas.v4i3.10947.

Milda Putri, T. and Yanti, H.B. (2022) 'PENGARUH CORPORATE GOVERNANCE PERCEPTION INDEX, UKURAN PERUSAHAAN DAN KUALITAS AUDIT TERHADAP INTEGRITAS LAPORAN KEUANGAN', *Jurnal Ekonomi Trisakti*, 2(2), pp. 1165–1176. Available at: https://doi.org/10.25105/jet.v2i2.14516.

Mutaufiq, A. (2021) 'Pengaruh Struktur Organisasi Terhadap Kualitas Sistem Informasi Akuntansi Manajemen', *Jurnal Ekonomi Utama*, 1(2), pp. 81–88. Available at: https://doi.org/10.55903/astina.v1i1.5.

Pamuji, A. (2022) 'Prediksi Otorisasi Pengguna Sistem Berkas pada Algoritma Klasifikasi dengan Teknik Naïve Bayes', *Infomatek*, 24(1), pp. 35–44. Available at: https://doi.org/10.23969/infomatek.v24i1.4604.

Prabowo, A.P. *et al.* (2022) 'Factors Affecting the Adoption of record keeping in Koperasi Cianjur Utara', *JURNAL EKONOMI DAN KEBIJAKAN PEMBANGUNAN*, 11(2), pp. 146–160. Available at: https://doi.org/10.29244/jekp.11.2.2022.146-160.

Rahma, F.I. *et al.* (2021) 'Implementasi Constraint CHECK Pada Basis Data Aplikasi LaundryPOS Dalam Aspek Kebenaran Data', *Creative Information Technology Journal* [Preprint]. Available at: https://doi.org/10.24076/citec.2020v7i2.259.

Sabatini, K. and Sudana, I.P. (2019) 'Pengaruh Pengungkapan Corporate Social Responsibility Pada Nilai Perusahaan Dengan Manajemen Laba Sebagai Variabel Moderasi', *Jurnal Ilmiah Akuntansi dan Bisnis* [Preprint]. Available at: https://doi.org/10.24843/JIAB.2019.v14.i01.p06.

Sari, M.R. and Pinasthika, B.T. (2021) 'Apakah Manajemen Laba dilakukan untuk Tax Planning atau untuk Menjadikan Laba Lebih Persisten?', *Journal of Management and Business Review*, 18(2), pp. 65–82. Available at: https://doi.org/10.34149/jmbr.v18i2.272.

Septian, J.A., Fachrudin, T.M. and Nugroho, A. (2019) 'Analisis Sentimen Pengguna Twitter Terhadap Polemik Persepakbolaan Indonesia Menggunakan Pembobotan TF-IDF dan K-Nearest Neighbor', *Journal of Intelligent System and Computation*, 1(1), pp. 43–49. Available at: https://doi.org/10.52985/insyst.v1i1.36.

Seto, S.B. *et al.* (2022) 'Perancangan Sistem Informasi Data Kependudukan Berbasis Web pada Kelurahan Lokoboko Kecamatan Ndona', *Mitra Mahajana: Jurnal Pengabdian Masyarakat*, 3(1), pp. 34–40. Available at: https://doi.org/10.37478/mahajana.v3i1.1488.

Swarte, W. *et al.* (2020) 'PENGARUH STRUKTUR KEPEMILIKAN DAN TATA KELOLA PERUSAHAAN TERHADAP PENGUNGKAPAN MANAJEMEN RISIKO', *EKUITAS (Jurnal Ekonomi dan Keuangan)*, 3(4), pp. 505–523. Available at: https://doi.org/10.24034/j25485024.y2019.v3.i4.4205.

Tahmidi, F.B., Oktaroza, M.L. and Hartanto, R. (2022) 'Pengaruh Kualitas Audit dan Komite Audit terhadap Manajemen Laba', *Bandung Conference Series: Accountancy*, 2(2). Available at: https://doi.org/10.29313/bcsa.v2i2.3236.

Tang, S. and Fiorentina, F. (2021) 'PENGARUH KARAKTERISTIK PERUSAHAAN, KINERJA PERUSAHAAN, DAN MANAGEMENT ENTRENCHMENT TERHADAP MANAJEMEN LABA', *Jurnal Ekonomi Bisnis dan Kewirausahaan*, 10(2), p. 121. Available at: https://doi.org/10.26418/jebik.v10i2.47461.

Todingbua, D. and Setiyawati, N. (2022) 'Pengintegrasian Penyimpanan Google Drive Pada Pembangunan Aplikasi Monitoring Project Menggunakan pyDrive', *JURIKOM (Jurnal Riset Komputer)*, 9(4), p. 800. Available at: https://doi.org/10.30865/jurikom.v9i4.4452.

Wahyuni, A.D. and Dahmiri, D. (2021) 'KEPERCAYAAN DAN PERSEPSI RISIKO TERHADAP KEAMANAN KONSUMEN DAN IMPLIKASINYA TERHADAP MINAT BELI KONSUMEN DI MARKETPLACE SHOPEE KOTA JAMBI', *Jurnal Manajemen Terapan dan Keuangan*, 10(01), pp. 29–41. Available at: https://doi.org/10.22437/jmk.v10i01.12384.

Wijoyo, H. *et al.* (2021) 'Sistem Informasi Manajemen'. Insan Cendekia Mandiri.

Wiradarma, I.W.A. and Respati, N.N.R. (2020) 'PERAN CUSTOMER SATISFACTION MEMEDIASI PENGARUH SERVICE QUALITY TERHADAP REPURCHASE INTENTION PADA PENGGUNA LAZADA DI DENPASAR', *E-Jurnal Manajemen Universitas Udayana*, 9(2), p. 637. Available at: https://doi.org/10.24843/EJMUNUD.2020.v09.i02.p12.

Wulan, D. and Suzan, L. (2022) 'Pengaruh Leverage, Kepemilikan Manajerial, Dan Ukuran Perusahaan Terhadap Integritas Laporan Keuangan', *Jurnal Analisa Akuntansi dan Perpajakan*, 6(2), pp. 127–139. Available at: https://doi.org/10.25139/jaap.v6i2.5124.

BAB 4
FRAUD, ETHICS & INTERNAL CONTROL

Oleh I Made Dwi Hita Darmawan

4.1 Fraud dan Dilematis Psikologis

Fraud adalah tindakan yang disengaja dan menipu dengan tujuan merugikan perusahaan atau individu. Ini mencakup manipulasi data, kebijakan palsu, atau tindakan penipuan lainnya. Untuk memahami fraud, penting untuk membedakan antara kesalahan biasa dan tindakan penipuan yang disengaja (Nalukenge et al., 2018; Nawawi and Salin, 2018; Nwanyanwu, 2018). Fraud melibatkan unsur kesempatan, tekanan, dan rasionalisasi. Kesempatan adalah situasi di mana seseorang dapat melakukan fraud, tekanan adalah alasan yang mendorong seseorang untuk melakukan fraud, dan rasionalisasi adalah cara seseorang membenarkan tindakan tersebut.

Terdapat berbagai jenis fraud, termasuk:

1. Penipuan Keuangan: Manipulasi laporan keuangan untuk mendapatkan keuntungan pribadi atau memberikan gambaran yang salah kepada pemegang saham.
2. Korupsi: Penyalahgunaan kekuasaan atau posisi untuk mendapatkan keuntungan pribadi, seperti suap atau nepotisme.
3. Penggelapan Aset: Pencurian atau penggelapan aset perusahaan, seperti uang tunai, inventaris, atau kekayaan intelektual.
4. Penipuan oleh Karyawan: Tindakan penipuan yang dilakukan oleh karyawan terhadap perusahaan mereka.
5. Penipuan oleh Pihak Ketiga: Tindakan penipuan yang melibatkan pihak eksternal yang berinteraksi dengan perusahaan.

Faktor-faktor pemicu ini misalnya ekonomi, seperti tekanan keuangan atau keinginan untuk memperkaya diri sendiri (Bachtiar and Elliyana, 2020; Chowdhury and Shil, 2019; Putra et al., 2019; Setiawan, 2018). Faktor sosial, seperti norma kelompok atau budaya organisasi yang kurang etis. Faktor psikologis, seperti kebutuhan akan pengakuan atau kekuasaan. Pencegahan fraud melibatkan pengembangan pengendalian internal yang kuat, pelatihan karyawan, dan penggunaan teknologi yang tepat. Strategi deteksi meliputi analisis data, pengawasan, dan pelaporan keuangan yang teliti. Penting untuk memiliki kebijakan dan prosedur yang jelas untuk mendeteksi tanda-tanda fraud.

Sistem informasi akuntansi dapat membantu dalam pencegahan dan deteksi fraud melalui otomatisasi, audit jejak, dan pengawasan yang lebih ketat. Perangkat lunak yang canggih dapat mengidentifikasi pola-pola yang mencurigakan dalam data keuangan. Memahami hukum yang berlaku terkait dengan fraud adalah penting. Ini termasuk peraturan akuntansi dan undang-undang anti-penipuan (Fernandhytia and Muslichah, 2020; Herawaty and Hernando, 2021). Etika juga penting, karena melibatkan pertimbangan moral dalam menghadapi situasi yang mencurigakan.

Perusahaan harus memiliki prosedur pelaporan yang jelas untuk memungkinkan karyawan atau pihak luar melaporkan tindakan fraud. Proses investigasi harus dilakukan dengan cermat dan sesuai dengan hukum. Manajemen risiko yang efektif adalah kunci dalam mencegah fraud. Ini melibatkan identifikasi, evaluasi, dan mitigasi risiko fraud dalam seluruh organisasi. Profesional akuntansi memiliki tanggung jawab penting dalam mendeteksi dan melaporkan fraud. Mereka harus mematuhi kode etik profesi dan hukum yang berlaku.

4.2 Ethics: Konflik Kepentingan dan Merosotnya Akal Sehat

Etika dalam bisnis merujuk pada prinsip-prinsip moral dan nilai-nilai yang memandu perilaku organisasi dan individu dalam konteks bisnis. Pentingnya etika dalam bisnis adalah menciptakan budaya organisasi yang berfokus pada integritas, transparansi, dan

tanggung jawab sosial. Pengambilan keputusan berdasarkan etika melibatkan pertimbangan nilai-nilai dan norma moral dalam proses pengambilan keputusan (Handoyo and Bayunitri, 2021; Rashid et al., 2022; Sudirman et al., 2021). Ini dapat mencakup penilaian konsekuensi jangka panjang, dampak sosial, dan kepatuhan terhadap hukum dan peraturan.

Kode etik adalah panduan yang mengatur perilaku para profesional. Misalnya, Kode Etik Akuntan Profesional menetapkan standar etika bagi akuntan. Kode etik membantu memelihara kepercayaan publik dan menjaga profesionalisme. Konflik etika dapat muncul dalam berbagai situasi, seperti konflik kepentingan, manipulasi laporan keuangan, atau tekanan untuk melanggar etika. Mempelajari kasus-kasus konflik etika membantu profesional dalam menghadapi situasi serupa.

CSR mengacu pada kewajiban perusahaan untuk berkontribusi pada masyarakat dan lingkungan. Implementasi CSR memerlukan transparansi dalam pelaporan keuangan dan pengukuran dampak sosial. Keamanan dan privasi data adalah bagian penting dari etika dalam bisnis digital. Organisasi harus melindungi data pelanggan dan pihak ketiga serta mengikuti regulasi privasi yang berlaku, seperti GDPR (Darmawan and Ratmayanti, 2023).

Etika dalam teknologi mencakup pertimbangan tentang dampak teknologi baru, penggunaan kecerdasan buatan, etika hacking, dan perlindungan hak kekayaan intelektual. Bisnis harus mempertimbangkan konsekuensi etika dari inovasi mereka (Maulidi and Ansell, 2022; Ratmayanti et al., 2023). Pengawasan etika adalah proses pemantauan dan menilai praktik bisnis untuk memastikan kepatuhan terhadap etika. Audit etika dapat membantu mengidentifikasi pelanggaran etika dan mengusulkan perbaikan.

Bisnis global menghadapi tantangan etika yang berbeda, seperti perbedaan budaya, kebijakan korupsi, dan lingkungan kerja. Bisnis harus mengintegrasikan norma etika lokal dan global (Darmawan and Tresna, 2023; Naim et al., 2021). Pelatihan etika adalah upaya untuk meningkatkan kesadaran dan pemahaman etika di seluruh organisasi. Ini mencakup pendidikan tentang kode etik, kasus-kasus etika, dan situasi dunia nyata.

4.3 Internal Control: Tiang Pertahanan Terakhir

Pengendalian internal adalah serangkaian prosedur, kebijakan, dan praktik yang diterapkan dalam sebuah organisasi untuk memastikan integritas, akurasi, dan keamanan informasi keuangan. Ini mencakup semua langkah yang diambil untuk melindungi aset organisasi, mencegah penipuan, dan memastikan kepatuhan terhadap peraturan (Darmawan, 2023). Pengendalian internal bertujuan untuk mencapai beberapa hal, termasuk:

1. Mencegah Penipuan: Pengendalian membantu mencegah tindakan penipuan dan kecurangan dalam organisasi.
2. Meningkatkan Efisiensi Operasional: Pengendalian membantu dalam optimalisasi operasional dan penggunaan sumber daya.
3. Memastikan Kepatuhan: Mereka memastikan bahwa organisasi mematuhi peraturan dan kebijakan yang berlaku.

Komponen pengendalian internal meliputi:

1. Lingkungan Pengendalian: Ini mencakup budaya organisasi, etika, dan nilai-nilai yang mendukung pengendalian internal.
2. Evaluasi Risiko: Organisasi harus mengidentifikasi dan mengevaluasi risiko-risiko yang dapat mempengaruhi pencapaian tujuan bisnis.
3. Aktivitas Pengendalian: Aktivitas-aktivitas yang dijalankan untuk mengelola dan mengendalikan risiko-risiko yang telah diidentifikasi.
4. Informasi dan Komunikasi: Mengenai penyebaran informasi yang relevan dan komunikasi yang efektif tentang pengendalian internal.
5. Pemantauan: Proses pemantauan berkelanjutan untuk memastikan pengendalian internal tetap efektif.

COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) telah mengembangkan prinsip-prinsip yang dikenal sebagai Kerangka Acuan Pengendalian Internal. Prinsip-prinsip ini mencakup penilaian risiko, lingkungan pengendalian, aktivitas pengendalian, informasi dan komunikasi, serta

pemantauan (Darmawan, 2023). Proses penilaian risiko melibatkan mengidentifikasi potensi risiko yang dapat mempengaruhi organisasi, mengevaluasi probabilitas dan dampaknya, dan mengembangkan strategi pengendalian untuk mengelola risiko tersebut. Pengendalian internal dapat dibagi menjadi tiga kategori utama:

1. Pengendalian Pencegahan: Langkah-langkah yang diambil untuk mencegah terjadinya risiko.
2. Pengendalian Pendeteksian: Prosedur-prosedur yang digunakan untuk mendeteksi risiko jika terjadi.
3. Pengendalian Korektif: Tindakan yang diambil jika risiko telah terjadi untuk meminimalkan dampaknya.

Audit internal adalah proses pemeriksaan independen dan objektif yang dilakukan oleh auditor internal untuk menilai efektivitas pengendalian internal. Audit eksternal, di sisi lain, dilakukan oleh auditor independen dari luar organisasi. Keamanan informasi adalah komponen penting dari pengendalian internal. Ini melibatkan perlindungan data dan informasi bisnis dari akses yang tidak sah atau potensi ancaman siber (Darmawan, 2023b).

Teknologi informasi dan sistem informasi dapat memperkuat pengendalian internal dengan otomatisasi proses bisnis, pelaporan real-time, dan deteksi ancaman siber. Melibatkan karyawan dalam pemahaman dan penerapan pengendalian internal melalui pelatihan, komunikasi yang efektif, dan peningkatan kesadaran akan pentingnya pengendalian. Tantangan modern melibatkan perubahan regulasi, perubahan teknologi, dan tuntutan bisnis yang berkembang. Organisasi harus terus mengadaptasi pengendalian internal mereka (Darmawan, 2023). Manfaat dari pengendalian internal yang efektif termasuk meningkatnya kepercayaan pemangku kepentingan, pengurangan risiko kerugian, dan keberlanjutan bisnis jangka panjang.

4.4 Skandal Enron 2001: Kejahatan Akuntansi Terbesar Sepanjang Sejarah

Salah satu perusahaan terbesar di Amerika Serikat (AS) pernah menarik perhatian internasional karena memanipulasi laporan keuangannya untuk memikat para investor. Enron terlibat dalam kontroversi penipuan investor pada saat perusahaan ini dikenal sebagai perusahaan terbesar ketujuh di Amerika Serikat. Melalui laporan keuangannya yang mengesankan, Enron mampu menarik investor baru dan meningkatkan modal lebih lanjut (Liputan 6, 2014).

Namun, banyak penipuan manajerial pada akhirnya menyebabkan pencapaian perusahaan energi besar ini runtuh. Para investor tidak diberitahu tentang utang Enron selain pendapatannya. Enron diduga mendapat dukungan dari Gedung Putih sebagai tambahannya. Masuk akal jika Enron menginvestasikan sejumlah besar uang dalam kampanye mantan Presiden AS George W. Bush

4.4.1 Pernah Menjadi Salah Satu Bisnis Terbesar di AS

Lahir di Missouri, Amerika Serikat, Kenneth Lay mendirikan Enron, sebuah perusahaan energi. Perusahaan yang berkantor pusat di Houston, Texas ini telah berkembang dengan cepat, dengan hanya sedikit orang yang mengetahui bagaimana perusahaan ini dimulai. Enron mampu menjadi perusahaan AS terbesar ketujuh hanya dalam waktu 15 tahun.

Lebih dari 40 negara menjadi rumah bagi 21.000 karyawan perusahaan ini. Enron bernilai US$ 68 miliar, atau Rp 768,5 triliun (kurs: Rp 11.301/US$), berkat upaya Lay dan dua rekannya. Seiring dengan semakin banyaknya investor yang membeli saham, harga setiap lembar saham meningkat menjadi US$ 90.

4.4.2 Skandal Enron Mulai Muncul ke Permukaan, Menyebabkan Kerugian Sebesar US$74 Miliar

Enron membeli saham di JEDI, sebuah perusahaan energi yang berbeda, pada bulan November 1997. Setelah itu, Enron menjual sahamnya kepada Chewco, sebuah bisnis yang didirikannya. Kepemimpinan Chewco kemudian memulai banyak

kesepakatan rumit yang memungkinkan Enron menyembunyikan kewajibannya. Majalah Fortune yang terkenal di seluruh dunia mengungkapkan bahwa Enron adalah perusahaan yang memiliki banyak utang pada 20 Februari 2001. Pada saat itu, para investor mulai menarik diri dari Enron, membuat sahamnya turun menjadi US$ 75,09.

Terungkap bahwa Lay telah melebih-lebihkan pendapatan dalam laporan keuangan bisnisnya. Selain itu, dia juga mahir memanipulasi dokumen keuangan untuk menyembunyikan kewajibannya. Kurang dari setahun kemudian, pada akhir tahun 2001, saham Enron jatuh hingga 26 sen dolar AS. Ketika semua kecurangannya terbongkar, Lay dilaporkan kehilangan hingga US$ 76 miliar dari para investor.

4.4.3 Investor Menginginkan Penjelasan dari Perusahaan yang Bangkrut

Pada tanggal 2 Desember 2001, Enron mengumumkan kebangkrutannya. CEO Andersen Joseph Berardino menyatakan bahwa organisasinya menemukan potensi aktivitas kriminal yang dilakukan oleh Enron. Departemen Kehakiman AS kemudian mengirimkan tim investigasi pada tanggal 9 Januari 2002, untuk menguatkan tuduhan kriminal tersebut. Setelah dua belas tahun menikmati kemakmuran, kejatuhan Enron disambut dengan tuntutan penjelasan dari para investor, anggota staf, pemegang saham, dan politisi.

Akhirnya, ditemukan bahwa penipuan dan pencucian uang mungkin terjadi. Michael Kopper, seorang karyawan, kemudian terseret ke dalam kasus ini. Penipuan Enron yang lengkap kemudian dipublikasikan olehnya. Akhirnya, tiga dalang dari penipuan investasi tersebut diidentifikasi: mantan ketua audit keuangan Enron David Duncan, mantan ketua dan CEO Kenneth Lay, dan mantan manajer keuangan Andrew Fastow.

4.4.5 Lay Meninggal Dunia Ketika Sedang Menunggu Keputusan Pengadilan

Lay menyatakan bahwa ia akan mematuhi prosedur hukum yang berlaku, namun ia menolak untuk berbicara lebih lanjut mengenai masalah ini. Sementara itu, Fastow sedang menjalani masa hukumannya ketika ditemukan bahwa, ketika menangani administrasi keuangan perusahaan, ia terlibat dalam perilaku tidak jujur. Duncan, kepala audit Enron, juga dituduh menyembunyikan banyak penemuan penting dari penyelidikan.

Jeffrey Skilling, salah satu pemimpin Enron lainnya yang turut mendirikan bisnis tersebut, membantah memiliki pengetahuan tentang aktivitas ilegal tersebut. Setelah itu, Lay dilayani dengan sebelas tuntutan hukum yang berkaitan dengan penipuan dan kejahatan terkait lainnya. Sayangnya, Lay meninggal dunia pada tahun 2006 ketika sedang berlibur sambil menunggu masa hukumannya.

4.4.6 Konsekuensi dari Skandal Enron terhadap Politik

Mengingat Enron memiliki jaringan luas dengan kontak-kontak yang berpengaruh di Gedung Putih, skandal ini juga masuk ke dalam politik AS. Lay telah menghubungi banyak politisi negara bagian untuk meminta bantuan, bahkan ketika harga sahamnya mulai menurun. Enron juga diketahui menyumbang jutaan dolar untuk kampanye presiden George W. Bush pada tahun 2000.

Pada akhirnya diketahui bahwa Bush dan Lay adalah teman baik. Bush pada saat itu langsung mundur dan tidak tertarik untuk bergabung dalam pertarungan hukum perusahaan tersebut. Lay akhirnya menyampaikan berita bahwa Enron telah mengajukan kebangkrutan setelah menghubungi dua anggota kabinet AS.

4.5 Kesimpulan

Dalam buku ini, penulis telah membahas tiga topik utama yang sangat relevan dalam konteks sistem informasi akuntansi dan bisnis, yaitu Fraud, Ethics, dan Internal Control. Kesimpulan yang dapat diambil secara komprehensif dari pembahasan ini adalah sebagai berikut:

1. Fraud merupakan ancaman serius dalam dunia bisnis dan akuntansi. Dalam buku ini, kami menyoroti bahwa kecurangan dapat terjadi dalam berbagai bentuk, mulai dari manipulasi laporan keuangan hingga penyalahgunaan informasi. Pentingnya deteksi dini dan pencegahan fraud tidak dapat diabaikan. Sistem informasi akuntansi harus dirancang dengan ketat untuk meminimalkan celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Monitoring yang efektif, penggunaan teknologi canggih, dan pelibatan manajemen dalam pengawasan merupakan langkah-langkah kunci dalam melawan kecurangan.
2. Etika dalam bisnis dan akuntansi memiliki peran krusial dalam memastikan keberlanjutan dan reputasi perusahaan. Dalam buku ini, kami menegaskan bahwa setiap pemangku kepentingan harus beroperasi dengan integritas dan kejujuran. Standar etika yang tinggi harus diterapkan dalam setiap tahapan proses bisnis, termasuk pelaporan keuangan. Pemahaman terhadap tanggung jawab sosial perusahaan juga menjadi aspek penting etika dalam bisnis. Penegakan nilai-nilai etika akan menciptakan lingkungan yang sehat dan berkelanjutan.
3. Kontrol internal memiliki peran sentral dalam memitigasi risiko dan melindungi aset perusahaan. Dalam buku ini, kami menyoroti bahwa perancangan kontrol internal yang efektif mencakup pemisahan tugas, validasi independen, serta penggunaan teknologi untuk memantau dan mengendalikan proses bisnis. Pentingnya penilaian risiko secara berkala dan penyesuaian kontrol internal sesuai dengan perubahan lingkungan bisnis tidak boleh diabaikan. Sistem informasi akuntansi yang kuat juga menjadi komponen utama dalam mendukung efektivitas kontrol internal.

   Dengan mengintegrasikan pemahaman mendalam tentang fraud, ethics, dan internal control, pembaca diharapkan dapat mengembangkan wawasan yang holistik dan praktis terkait bagaimana sistem informasi akuntansi dan bisnis dapat

dirancang dan dikelola untuk mencapai tujuan keuangan sambil menjaga keberlanjutan dan integritas perusahaan.

4.6 Rekomendasi Masa Depan

Berdasarkan analisis mendalam terhadap Fraud, Ethics, dan Internal Control, terdapat beberapa rekomendasi strategis yang dapat diimplementasikan untuk menghadapi tantangan masa depan dalam konteks sistem informasi akuntansi dan bisnis:

1. Implementasi Teknologi Canggih, perusahaan perlu mempertimbangkan penggunaan teknologi canggih seperti kecerdasan buatan (AI) dan analisis data untuk mendeteksi potensi kecurangan dengan lebih akurat dan efisien. Integrasi teknologi ini dalam sistem informasi akuntansi dapat memberikan tingkat otomatisasi yang tinggi dalam pemantauan dan deteksi anomali.
2. Penguatan Pelatihan Etika, perusahaan harus meningkatkan inisiatif pelatihan etika bagi karyawan di semua tingkatan. Pemahaman yang lebih baik tentang konsekuensi dari tindakan tidak etis dan pentingnya integritas dapat membentuk budaya perusahaan yang didasarkan pada nilai-nilai moral. Program pelatihan reguler dan studi kasus etika dapat membantu membangun kesadaran dan komitmen terhadap praktik bisnis yang etis.
3. Pengembangan Sistem Pengawasan Berbasis Risiko, melihat perkembangan cepat dalam lingkungan bisnis, perusahaan harus merancang sistem pengawasan berbasis risiko yang adaptif. Penilaian risiko yang terus-menerus dan penyesuaian kontrol internal akan memastikan bahwa perusahaan dapat mengidentifikasi dan mengatasi risiko baru yang muncul seiring waktu.
4. Keterlibatan Pemangku Kepentingan, meningkatkan keterlibatan pemangku kepentingan, terutama manajemen puncak, dalam pengawasan dan pengendalian internal menjadi kunci. Manajemen harus memimpin dengan contoh dan menunjukkan komitmen mereka terhadap praktik bisnis yang etis dan penguatan kontrol internal.

5. Audit Internal yang Kuat, memperkuat fungsi audit internal akan memberikan keuntungan tambahan dalam memastikan efektivitas sistem informasi akuntansi dan kontrol internal. Audit internal yang proaktif dan mendalam dapat mengidentifikasi celah atau masalah potensial sebelum mereka menjadi ancaman serius bagi perusahaan.
6. Adopsi Standar Keuangan dan Etika Global, dalam konteks bisnis global, perusahaan perlu mengadopsi standar keuangan dan etika yang berlaku secara internasional. Hal ini dapat mempermudah perbandingan dan membangun kepercayaan dari pemangku kepentingan global.

Dengan mengimplementasikan rekomendasi ini, perusahaan dapat membangun fondasi yang kuat untuk melindungi aset mereka, meminimalkan risiko fraud, dan membentuk budaya bisnis yang didasarkan pada integritas dan etika. Masa depan sistem informasi akuntansi dan bisnis membutuhkan pendekatan yang proaktif dan adaptif untuk mengatasi perubahan lingkungan bisnis yang dinamis.

DAFTAR PUSTAKA

Bachtiar, I.H., Elliyana, E., 2020. Determinan upaya pencegahan fraud pemerintah desa. Imanensi: Jurnal Ekonomi, Manajemen.

Chowdhury, A., Shil, N.C., 2019. Influence of new public management philosophy on risk management, fraud and corruption control and internal audit: evidence from an Australian public sector. Accounting and Management Information.

Darmawan, I Made Dwi Hita, 2023a. MEMBEDAH PRINSIP PELAPORAN KONSERVATISME AKUNTANSI: PRO KONTRA, KEGUNAAN DAN PERTIMBANGAN UNTUK PEMANGKU KEPENTINGAN. JURNAL MANEKSI 12, 410–416.

Darmawan, I. M. D. H., 2023. Analisis Kinerja Keuangan Pemerintah Provinsi DKI Jakarta (Studi Kasus Pada Tahun Politik 2018). Monex: Journal of Accounting Research 12, 309–323.

Darmawan, I Made Dwi Hita, 2023b. Information Technology Training Towards Digital MSMEs (Collaboration with the Bangli District Cooperative and MSMEs office). Journal of Social Sciences and Technology for Community Service 4.

Darmawan, I.M.D.H., Ratmayanti, N.G.S., 2023. The Impact of Education Budget Politics on Discontinuation of Scholarship: A Case Study of SMAN Bali Mandara. Bestuurskunde: Journal of Governmental Studies 3, 143–155.

Darmawan, I.M.D.H., Tresna, I.G.N.A.P., 2023. ACCOUNTING, CULTURE, AND HINDUISM: A NARRATIVE REVIEW. Vidyottama Sanatana: International Journal of Hindu Science and Religious Studies 7, 235–243.

Fernandhytia, F., Muslichah, M., 2020. The effect of internal control, individual morality, and ethical value on accounting fraud tendency. Media Ekonomi Dan

Handoyo, B.R.M., Bayunitri, B.I., 2021. The influence of internal audit and internal control toward fraud prevention. International Journal of Financial.

Herawaty, N., Hernando, R., 2021. Analysis of Internal Control of Good Corporate Governance and Fraud Prevention (Study at the Regional Government of Jambi City). Sriwijaya International Journal of Audit.

Liputan 6, 2014. Enron, Skandal Besar Perusahaan Energi yang Cekik Investor. Liputan 6.

Maulidi, A., Ansell, J., 2022. Corruption as distinct crime: the need to reconceptualise internal control on controlling bureaucratic occupational fraud. J Financ Crime.

Naim, A., Darmawan, I.M.D.H., Wulandari, N., 2021. HERDING BEHAVIOR: MENGEKSPLORASI SISI ANALISIS BROKER SUMMARY. Media Riset Akuntansi, Auditing & Informasi 21, 207–226.

Nalukenge, I., Nkundabanyanga, S.K., ..., 2018. Corporate governance, ethics, internal controls, and compliance with IFRS. Journal of Financial.

Nawawi, A., Salin, A., 2018. Internal control and employees' occupational fraud on expenditure claims. J Financ Crime.

Nwanyanwu, L.A., 2018. Accountants' ethics and fraud control in Nigeria: the emergence of a fraud control model. um.edu.mt.

Putra, I.G.C., Saitri, P.W. 2019. Accounting fraud tendency on village credit institution of accounting.

Rashid, M.A., Al-Mamun, A., Roudaki, H. 2022. An overview of corporate fraud and its prevention approach. Business and Finance.

Ratmayanti, N.G.S., Nugroho, A.H.L., Darmawan, I.M.D.H., Wiratama, A.B., 2023. Chakras in the Boardroom: Integrating Ancient Wisdom with Modern Business Practices for Enhanced Emotional and Spiritual Intelligence. Religious: Jurnal Studi Agama-Agama dan Lintas Budaya 7, 153–164.

Setiawan, S., 2018. The effect of internal control and individual morality on the tendency of accounting fraud. Asia Pacific Fraud Journal.

Sudirman, S., Sasmita, H., Krisnanto, B. 2021. Effectiveness of Internal Audit in Supporting Internal Control and Prevention of Fraud. Bongaya Journal of Accounting.

BAB 5
PENGENDALIAN INTERNAL DAN RISIKO SISTEM IT

Oleh Angga Aditya Permana

5.1 Pendahuluan

Gambar 5.1. Risk Management
Sumber : https://www.fao.org/

Pengendalian internal dan manajemen risiko sistem IT merupakan aspek penting dalam menjaga keamanan, keandalan, dan efisiensi sistem informasi dalam sebuah perusahaan. Pengendalian internal merujuk pada langkah-langkah yang diambil oleh perusahaan untuk memastikan kepatuhan, melindungi aset, dan mencegah kecurangan dalam operasionalnya. Di sisi lain, manajemen risiko sistem IT berkaitan dengan upaya mengidentifikasi, mengevaluasi, dan mengatasi potensi risiko yang terkait dengan teknologi informasi yang digunakan dalam operasi bisnis. (Leitch 2016)

Pentingnya pengendalian internal dan manajemen risiko sistem IT tidak hanya terbatas pada pemeliharaan keamanan data,

tetapi juga berhubungan dengan menjaga kelancaran proses bisnis secara keseluruhan. Langkah-langkah pengendalian intern meliputi pengelolaan akses terhadap informasi, penetapan kebijakan dan prosedur yang jelas, serta audit internal yang teratur. Hal ini bertujuan untuk mencegah kebocoran data, penyalahgunaan informasi, dan kerentanan sistem.

Manajemen risiko sistem IT mengharuskan perusahaan untuk mengidentifikasi potensi ancaman terhadap keamanan sistem, seperti serangan siber, kehilangan data, atau gangguan operasional. Selanjutnya, perusahaan perlu mengevaluasi dampak dari ancaman tersebut serta mengembangkan strategi untuk mengurangi risiko, termasuk penggunaan teknologi keamanan yang tepat, backup data, dan rencana pemulihan bencana.

Dengan mengintegrasikan pengendalian intern yang kuat dan manajemen risiko sistem IT yang efektif, perusahaan dapat meminimalkan risiko kerugian, meningkatkan keandalan sistem informasi, dan memberikan perlindungan yang lebih baik terhadap aset data. Upaya ini membantu perusahaan dalam menjaga kepercayaan dari pelanggan, karyawan, serta pihak-pihak yang terkait dengan perusahaan, sambil menjaga kelangsungan operasional yang stabil dan aman.

Dalam konteks pengendalian intern, aspek penting lainnya adalah pemisahan tugas (segregation of duties) yang mengharuskan tugas-tugas yang kritis dipisahkan di antara beberapa orang atau departemen. Hal ini mencegah terjadinya penyalahgunaan kekuasaan atau kesalahan yang tidak disengaja. Selain itu, peningkatan transparansi melalui dokumentasi yang baik mengenai kebijakan, prosedur operasional, serta laporan keuangan juga menjadi bagian integral dari pengendalian intern. Dokumentasi ini membantu memastikan bahwa operasi berjalan sesuai dengan aturan yang ditetapkan.

Di sisi manajemen risiko sistem IT, penting untuk melakukan evaluasi risiko secara terus-menerus dan mengidentifikasi ancaman baru yang mungkin muncul seiring dengan perkembangan teknologi. Pendekatan yang proaktif dalam mengelola risiko sistem IT melibatkan penerapan kontrol keamanan yang canggih, termasuk

pemantauan dan deteksi dini terhadap ancaman keamanan yang baru.

Selain itu, penilaian secara teratur terhadap efektivitas pengendalian intern dan manajemen risiko sistem IT diperlukan untuk mengevaluasi kinerja serta menyesuaikan strategi yang digunakan sesuai dengan perubahan lingkungan bisnis dan teknologi. Langkah-langkah ini membantu organisasi untuk tetap adaptif dan responsif terhadap tantangan baru yang mungkin timbul.

Keseluruhan, pengendalian intern dan manajemen risiko sistem IT merupakan fondasi yang krusial dalam mendukung keberhasilan dan keamanan sistem informasi akuntansi dan bisnis. Dengan memprioritaskan langkah-langkah ini, perusahaan dapat meningkatkan ketahanan, efisiensi, dan keandalan sistem mereka, yang pada gilirannya akan mendukung pertumbuhan yang berkelanjutan serta menjaga kepercayaan dari berbagai pihak yang terlibat.

5.2 Apa saja yang perlu dikendalikan?

Gambar 5.2. Internal Control
Sumber : https://annualreport2019.umicore.com/

Dalam pengendalian internal dan manajemen risiko sistem IT pada sistem informasi akuntansi dan bisnis, ada beberapa hal yang perlu diperhatikan dan dikendalikan: (Leitch 2016; Nurmalitasari 2016)

1. **Akses dan Keamanan Data:**
   Pengelolaan hak akses ke sistem informasi untuk memastikan bahwa hanya pengguna yang berwenang yang memiliki akses ke data yang relevan.

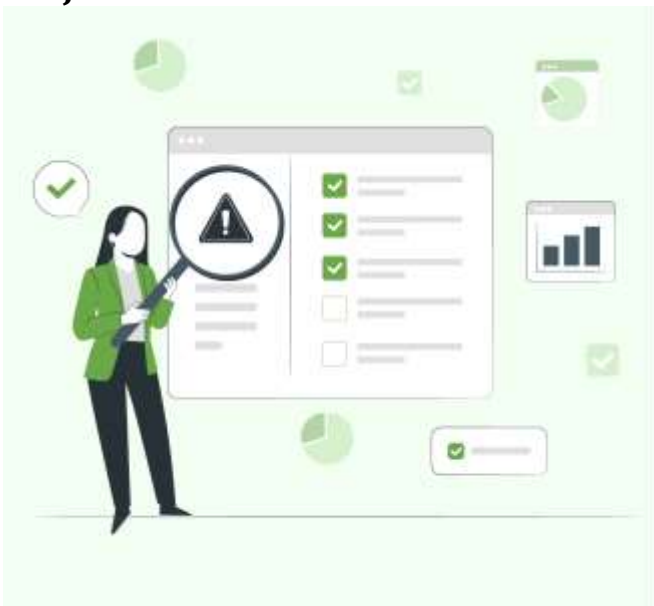
Perlindungan data sensitif dengan menggunakan enkripsi dan teknologi keamanan lainnya untuk mencegah akses tidak sah.

2. **Integritas Data:**
   Memastikan bahwa data yang dimasukkan ke dalam sistem adalah akurat, lengkap, dan tidak terpengaruh oleh kesalahan manusia atau kegiatan yang tidak sah.
   Menggunakan kontrol validasi data untuk memverifikasi integritas data yang dimasukkan.
3. **Pemantauan dan Audit:**
   Melakukan pemantauan terhadap aktivitas sistem secara rutin untuk mendeteksi aktivitas yang mencurigakan atau potensi ancaman keamanan.
   Melakukan audit internal secara berkala untuk mengevaluasi kepatuhan terhadap kebijakan, menganalisis potensi risiko, dan memperbaiki kelemahan yang teridentifikasi.
4. **Backup dan Pemulihan Data:**
   Melakukan pencadangan data secara teratur dan menyimpannya di lokasi yang aman untuk memastikan bahwa data dapat dipulihkan dalam kasus kehilangan atau kerusakan data.
5. **Pemisahan Tugas (*Segregation of Duties*):**
   Memastikan bahwa tugas-tugas kritis terpisah di antara beberapa orang atau departemen untuk mencegah penyalahgunaan kekuasaan atau kesalahan yang tidak disengaja.
6. **Kebijakan dan Prosedur:**
   Menetapkan kebijakan dan prosedur yang jelas terkait dengan penggunaan sistem informasi, keamanan data, akses, dan pengelolaan risiko.
7. **Kepatuhan Regulasi:**
   Memastikan bahwa sistem informasi dan kebijakan yang diterapkan memenuhi persyaratan dari berbagai peraturan dan standar yang berlaku.
8. **Pengelolaan Risiko IT:**
   Mengidentifikasi, mengevaluasi, dan mengelola risiko-risiko terkait dengan keamanan sistem IT, seperti serangan siber, kehilangan data, atau kerentanan sistem lainnya.

9. **Pendidikan dan Kesadaran Pengguna:**
   Memberikan pelatihan kepada karyawan tentang praktik keamanan informasi serta meningkatkan kesadaran akan ancaman keamanan yang mungkin terjadi.

Mengendalikan aspek-aspek ini membantu dalam menjaga keamanan, integritas, dan ketersediaan sistem informasi akuntansi dan bisnis, serta mendukung operasi yang lancar dan keberhasilan bisnis jangka panjang.

5.3 Apa saja risiko sistem IT?



Gambar 5.3. Risiko Sistem IT
Sumber : https://www.v-comply.com/

Ada beberapa risiko yang terkait dengan sistem IT dalam konteks sistem informasi akuntansi dan bisnis. Berikut adalah beberapa risiko umum yang perlu diperhatikan: (Leitch 2016; Sarwoko 2020)

1. **Ancaman Keamanan Cyber:**
   Serangan Malware: Infeksi perangkat lunak dengan program jahat yang dapat merusak, menghapus, atau mencuri data.

Serangan Phishing: Upaya untuk memperoleh informasi sensitif dengan menyamar sebagai entitas tepercaya melalui komunikasi elektronik.

Serangan *Denial-of-Service* (DoS): Memblokir akses ke sistem atau layanan dengan melimpahkan permintaan yang berlebihan.

2. **Kehilangan atau Kerusakan Data:**

   Kehilangan Data: Kehilangan informasi penting akibat kegagalan sistem, kesalahan manusia, atau serangan siber.

   Kerusakan Data: Kerusakan atau perubahan yang tidak sah terhadap integritas data yang dapat menyebabkan ketidakakuratan atau kehilangan informasi.

3. **Kesalahan Manusia:**

   Kesalahan Input Data: Kesalahan manusia dalam memasukkan atau memanipulasi data yang dapat mengakibatkan ketidakakuratan informasi atau laporan.

   Kesalahan Konfigurasi: Kesalahan dalam konfigurasi sistem atau perangkat lunak yang dapat menyebabkan kerentanan keamanan atau ketidakstabilan sistem.

4. **Ketergantungan pada Infrastruktur Teknologi:**

   Gangguan Operasional: Gangguan pada perangkat keras, jaringan, atau layanan hosting yang dapat mengganggu operasi bisnis.

   Ketergantungan pada Penyedia Layanan: Risiko terkait dengan keandalan penyedia layanan atau infrastruktur cloud yang digunakan.

5. **Kepatuhan dan Hukum:**

   Pelanggaran Regulasi: Tidak mematuhi persyaratan hukum, regulasi, atau standar keamanan yang berlaku, yang dapat mengakibatkan sanksi atau denda.

6. **Risiko Manajemen Proyek IT:**

   Keterlambatan atau Kegagalan Proyek: Keterlambatan dalam pengembangan sistem atau proyek IT yang melebihi anggaran biaya atau tidak mencapai tujuan yang diinginkan.

7. **Ketergantungan pada Karyawan atau SDM:**

   Risiko SDM: Ketergantungan terlalu besar pada satu atau beberapa individu kunci dalam pengelolaan sistem yang dapat

mengakibatkan risiko jika mereka meninggalkan perusahaan atau tidak tersedia.

Memahami dan mengelola risiko-risiko ini penting dalam menjaga keamanan, integritas, dan ketersediaan sistem informasi akuntansi dan bisnis. Perusahaan harus mengidentifikasi, mengevaluasi, dan mengurangi risiko-risiko ini sebisa mungkin untuk melindungi data dan memastikan kelancaran operasi bisnis.

5.4 Bagaimana Mengendalikan Internal dan Risiko Sistem IT?

Gambar 5.4. Pengendalian Internal
Sumber : https://www.otpcapital.com.ua/

Untuk mengendalikan internal dan risiko sistem IT dalam sistem informasi akuntansi dan bisnis, perusahaan perlu menerapkan serangkaian langkah-langkah yang dapat memastikan keamanan, integritas, dan ketersediaan informasi. Berikut adalah beberapa cara untuk mengendalikan internal dan risiko sistem IT pada sistem informasi akuntansi dan bisnis: (Leitch 2016)

1. **Kebijakan dan Prosedur:**
   Membuat kebijakan dan prosedur yang jelas terkait penggunaan sistem informasi, akses data, dan keamanan informasi.

Melakukan pelatihan kepada karyawan agar memahami dan mematuhi kebijakan dan prosedur tersebut.

2. **Manajemen Akses:**
   Menerapkan kontrol akses yang ketat terhadap sistem informasi dengan memberikan hak akses yang tepat sesuai dengan peran dan tanggung jawab masing-masing pengguna.
   Menggunakan otentikasi dua faktor atau metode keamanan lainnya untuk memperkuat keamanan akses.
3. **Pemantauan dan Audit:**
   Melakukan pemantauan secara teratur terhadap aktivitas sistem untuk mendeteksi aktivitas yang mencurigakan atau potensi ancaman keamanan.
   Melakukan audit internal secara berkala untuk mengevaluasi kepatuhan terhadap kebijakan dan prosedur serta mengidentifikasi potensi risiko.
4. **Pengelolaan Risiko:**
   Mengidentifikasi risiko-risiko yang terkait dengan sistem informasi akuntansi dan bisnis, lalu membuat strategi pengelolaan risiko yang tepat seperti penggunaan sistem keamanan yang kuat, backup data, dan rencana pemulihan bencana.
   Menetapkan langkah-langkah mitigasi risiko untuk mengurangi dampak potensial dari ancaman tersebut.
5. **Pembaruan dan Pemeliharaan Sistem:**
   Memastikan sistem informasi selalu diperbarui dengan versi terbaru dan menjalankan pemeliharaan rutin untuk mengatasi kerentanan keamanan yang mungkin ada.
   Menggunakan perangkat lunak antivirus dan firewall yang terkini untuk melindungi sistem dari serangan malware dan serangan siber lainnya.
6. **Pendekatan Terpadu terhadap Keamanan:**
   Menerapkan pendekatan yang komprehensif terhadap keamanan informasi dengan mengintegrasikan aspek-aspek teknologi, kebijakan, pelatihan, dan pemantauan keamanan secara bersama-sama.

7. **Kerjasama dengan Ahli Keamanan IT:**
   Melibatkan ahli keamanan IT atau konsultan keamanan untuk mengidentifikasi potensi risiko dan memberikan saran terkait perbaikan keamanan yang diperlukan.
8. **Enkripsi dan Pengamanan Data:**
   Menggunakan teknologi enkripsi untuk melindungi data sensitif yang disimpan dan dipertukarkan antara sistem internal dan eksternal.
   Menggunakan teknik pengamanan data yang tepat seperti pengacakan (*hashing*) dan enkripsi untuk melindungi integritas data.
9. **Backup dan Pemulihan Data:**
   Melakukan pencadangan data secara rutin dan menyimpan cadangan tersebut di lokasi yang aman, sehingga data dapat dipulihkan dengan cepat jika terjadi kehilangan atau kerusakan data.
   Mengembangkan rencana pemulihan bencana yang mencakup langkah-langkah untuk mengembalikan sistem dan data dalam situasi kegagalan atau bencana.
10. **Pemantauan Terhadap Ancaman Keamanan Terbaru:**
    Mengikuti perkembangan terkini dalam keamanan IT dan mengidentifikasi ancaman baru yang mungkin muncul, serta mengambil tindakan pencegahan yang sesuai.
11. **Kepatuhan Regulasi:**
    Memastikan bahwa sistem informasi akuntansi dan bisnis mematuhi semua peraturan, standar, dan regulasi yang relevan, seperti peraturan privasi data (GDPR, CCPA, dll.) dan standar keamanan industri yang berlaku.
12. **Sosialisasi Kultur Keamanan:**
    Mendorong budaya keamanan informasi di seluruh perusahaan dengan menyelenggarakan pelatihan reguler tentang keamanan informasi, membentuk kesadaran keamanan bagi semua karyawan.
13. **Penggunaan Teknologi Terbaru dengan Bijak:**
    Memilih dan mengimplementasikan teknologi terbaru dengan hati-hati, mempertimbangkan aspek keamanan serta potensi dampaknya terhadap sistem secara keseluruhan.

14. **Respon Terhadap Insiden:**
    Mempersiapkan rencana respons terhadap insiden keamanan, yang mencakup langkah-langkah untuk menangani serangan atau kebocoran data dengan cepat dan efektif.

Mengendalikan internal dan mengelola risiko sistem IT pada sistem informasi akuntansi dan bisnis merupakan upaya berkelanjutan yang memerlukan komitmen dari seluruh organisasi. Dengan mengintegrasikan praktik terbaik keamanan informasi ke dalam operasi sehari-hari, perusahaan dapat menjaga keamanan, integritas, dan ketersediaan data yang sangat penting bagi bisnis mereka.

5.5 Tahapan Pengendalian dan Risiko Sistem IT

Gambar 5.5. Tahapan Risk Management
Sumber : https://www.bstdb.org/

Tahapan dalam pengendalian internal dan manajemen risiko sistem IT pada sistem informasi akuntansi dan bisnis melibatkan serangkaian langkah-langkah yang diperlukan untuk mengidentifikasi, mengevaluasi, dan mengelola risiko-risiko yang terkait dengan teknologi informasi. Berikut adalah tahapan umum dalam pengendalian internal dan manajemen risiko sistem IT: (Leitch 2016)

1. **Identifikasi Risiko:**
   Langkah pertama adalah mengidentifikasi berbagai risiko yang mungkin timbul dari sistem informasi dan teknologi yang digunakan. Ini melibatkan analisis menyeluruh terhadap ancaman, kerentanan, dan potensi dampak terhadap operasi bisnis.

2. **Evaluasi Risiko:**
   Setelah risiko-risiko diidentifikasi, langkah selanjutnya adalah mengevaluasi risiko-risiko tersebut berdasarkan probabilitas terjadinya dan dampaknya terhadap perusahaan. Ini membantu dalam menentukan prioritas dan fokus untuk mengelola risiko.
3. **Pengembangan Strategi Pengelolaan Risiko:**
   Tahap ini melibatkan pengembangan strategi untuk mengurangi, mentransfer, atau mengelola risiko-risiko yang telah diidentifikasi. Ini dapat mencakup penggunaan kontrol keamanan tambahan, asuransi, atau mitigasi risiko lainnya.
4. **Implementasi Kontrol dan Langkah Pengendalian:**
   Setelah strategi pengelolaan risiko diputuskan, langkah selanjutnya adalah menerapkan kontrol dan langkah-langkah pengendalian yang sesuai. Ini bisa termasuk pembaruan perangkat lunak keamanan, pengaturan hak akses yang tepat, atau penerapan kebijakan dan prosedur yang lebih ketat.
5. **Pemantauan dan Pengujian:**
   Proses pengendalian dan manajemen risiko sistem IT harus secara teratur dipantau dan dievaluasi. Pengujian terhadap efektivitas kontrol dan prosedur pengendalian juga diperlukan untuk memastikan bahwa sistem berfungsi sesuai dengan yang diharapkan.
6. **Pengaturan Kembali dan Perbaikan Berkelanjutan:**
   Berdasarkan hasil pemantauan dan pengujian, diperlukan langkah-langkah pengaturan kembali atau perbaikan yang diperlukan. Ini bisa berupa perbaikan terhadap kelemahan yang teridentifikasi, penyesuaian strategi pengelolaan risiko, atau perubahan dalam kebijakan dan prosedur.
7. **Pendidikan dan Kesadaran Pengguna:**
   Selain langkah-langkah teknis, penting juga untuk memberikan pendidikan dan pelatihan kepada pengguna sistem mengenai praktik keamanan informasi dan kesadaran akan risiko yang ada.
8. **Komunikasi dan Pelaporan:**
   Komunikasi yang efektif tentang risiko-risiko yang diidentifikasi dan langkah-langkah pengendalian yang diimplementasikan sangat penting. Perusahaan perlu memiliki saluran komunikasi

yang jelas untuk melaporkan risiko dan masalah terkait keamanan kepada pihak yang berwenang.

9. **Kepatuhan dan Audit:**
   Menjaga tingkat kepatuhan terhadap kebijakan, peraturan, dan standar keamanan merupakan bagian penting dari pengendalian internal. Audit teratur dari sistem informasi dan keamanan IT diperlukan untuk memastikan bahwa pengendalian yang diimplementasikan efektif dan memenuhi persyaratan yang berlaku.
10. **Pengelolaan Perubahan:**
    Dalam lingkungan teknologi yang terus berkembang, perubahan adalah konstan. Pengelolaan perubahan yang baik termasuk dalam tahap-tahap pengendalian untuk memastikan bahwa setiap perubahan dalam sistem informasi atau teknologi diimplementasikan dengan benar dan tidak mengorbankan keamanan atau keandalan sistem.
11. **Revisi dan Penyesuaian:**
    Setelah suatu periode, penting untuk melakukan evaluasi kembali atas seluruh sistem pengendalian internal dan manajemen risiko. Penyesuaian dan perbaikan terus-menerus diperlukan agar sistem tetap adaptif terhadap perubahan lingkungan bisnis dan teknologi.
12. **Pengembangan Rencana Darurat dan Pemulihan:**
    Membuat rencana darurat dan pemulihan yang komprehensif dalam menghadapi insiden keamanan atau bencana yang mungkin terjadi. Rencana ini harus melibatkan langkah-langkah untuk mengidentifikasi, menangani, dan memulihkan sistem dari situasi yang kritis.

Tahapan ini memberikan kerangka kerja yang komprehensif untuk mengelola risiko sistem IT dan mengimplementasikan pengendalian internal yang efektif. Dengan menjalankan tahapan ini secara terus-menerus, perusahaan dapat meningkatkan kemampuan mereka dalam mengatasi ancaman dan risiko yang mungkin timbul terkait dengan teknologi informasi, serta menjaga keamanan dan keandalan sistem informasi akuntansi dan bisnis mereka.

5.6 Contoh Kasus dalam Bidang Ritel

Gambar 5.6. Bidang Ritel
Sumber : https://www.ikonmarket.com/

Sebagai contoh, pertimbangkan sebuah perusahaan ritel besar yang mengelola sistem informasi akuntansi dan bisnis untuk rantai toko mereka. Perusahaan ini telah mengidentifikasi beberapa risiko dalam pengendalian internal dan manajemen risiko sistem IT mereka: (Leitch 2016)

1. **Ancaman Serangan Siber:**
   a. Risiko: Potensi serangan malware atau serangan phishing yang dapat mengancam keamanan data pelanggan dan informasi keuangan perusahaan.
   b. Langkah Pengendalian: Implementasi firewall yang kuat, antivirus terbaru, dan pelatihan keamanan untuk karyawan guna mengidentifikasi dan mencegah serangan tersebut.
2. **Kegagalan Infrastruktur Teknologi:**
   a. Risiko: Kemungkinan gangguan pada sistem POS (*Point of Sale*) atau sistem pembayaran yang dapat mengganggu operasi harian toko.
   b. Langkah Pengendalian: Pencadangan rutin sistem, pemantauan kesehatan infrastruktur IT, dan rencana pemulihan bencana yang mengatur langkah-langkah pemulihan dalam kasus kegagalan sistem.

3. **Kesalahan Manusia dalam Input Data:**
    a. Risiko: Kesalahan dalam menginput harga produk atau data transaksi yang dapat mengakibatkan ketidakakuratan laporan keuangan.
    b. Langkah Pengendalian: Validasi data otomatis, pelatihan karyawan tentang pentingnya keakuratan data, dan penggunaan sistem yang dapat mendeteksi dan mengoreksi kesalahan input.
4. **Ketergantungan pada Penyedia Layanan:**
    a. Risiko: Risiko kerentanan terhadap gangguan atau kegagalan layanan hosting yang digunakan untuk menyimpan data penting.
    b. Langkah Pengendalian: Evaluasi menyeluruh terhadap penyedia layanan, penggunaan layanan hosting dengan reputasi baik dan dukungan teknis yang handal, serta pencadangan data secara teratur.
5. **Kepatuhan Regulasi:**
    a. Risiko: Pelanggaran aturan privasi data pelanggan yang dapat mengakibatkan sanksi hukum atau kerugian reputasi.
    b. Langkah Pengendalian: Memastikan kepatuhan terhadap regulasi privasi data seperti GDPR atau CCPA melalui kebijakan dan prosedur yang ketat, serta pelaporan rutin kepada pihak yang berwenang.

Melalui identifikasi risiko dan langkah-langkah pengendalian internal yang sesuai, perusahaan ini dapat meminimalkan dampak negatif dari risiko-risiko tersebut, menjaga keamanan data, serta menjalankan operasi bisnis mereka dengan lebih aman dan efisien.

5.7 Contoh Kasus dalam Bidang Perbankan

Gambar 5.7. Bidang Perbankan
Sumber : https://vir.com.vn/

Dalam industri perbankan, pengendalian internal dan manajemen risiko sistem IT sangat penting untuk menjaga keamanan informasi sensitif, kinerja operasional yang lancar, serta kepatuhan terhadap peraturan yang berlaku. Berikut adalah contoh kasus di bidang perbankan terkait pengendalian internal dan manajemen risiko sistem IT: (Leitch 2016)

1. **Ancaman Serangan Siber:**
   a. Risiko: Potensi serangan siber seperti peretasan (hacking), malware, atau serangan phishing yang dapat mengakibatkan pencurian data pribadi nasabah atau pencurian dana.
   b. Langkah Pengendalian: Penerapan lapisan keamanan yang kuat seperti firewall, enkripsi data sensitif, pemantauan sistem keamanan, serta pelatihan karyawan untuk mengenali dan mencegah serangan siber.
2. **Kesalahan dalam Transaksi atau Pengolahan Data:**
   a. Risiko: Kesalahan manusia dalam pengolahan data keuangan atau transaksi yang dapat mengakibatkan ketidakakuratan informasi akuntansi atau kerugian finansial.
   b. Langkah Pengendalian: Implementasi sistem validasi transaksi otomatis, peninjauan dan verifikasi data secara

berkala, serta pelatihan karyawan tentang pentingnya keakuratan data dalam transaksi perbankan.

3. **Kegagalan Sistem atau Infrastruktur Teknologi:**
   a. Risiko: Kemungkinan terjadi kegagalan pada sistem perbankan utama yang dapat mengganggu layanan perbankan atau transaksi nasabah.
   b. Langkah Pengendalian: Pencadangan rutin sistem, rencana pemulihan bencana yang terstruktur, uji coba keandalan sistem secara berkala, serta pemantauan terus-menerus terhadap kesehatan infrastruktur IT.
4. **Kepatuhan Terhadap Regulasi dan Standar Keamanan:**
   a. Risiko: Pelanggaran terhadap peraturan perbankan, standar keamanan informasi, atau privasi data nasabah yang dapat mengakibatkan sanksi hukum atau penurunan kepercayaan nasabah.
   b. Langkah Pengendalian: Penerapan prosedur kepatuhan yang ketat terhadap regulasi seperti Basel III, PCI DSS, atau regulasi privasi data yang berlaku, serta audit rutin untuk memastikan kepatuhan perusahaan terhadap standar tersebut.
5. **Manajemen Ketergantungan pada Pihak Ketiga:**
   a. Risiko: Ketergantungan terlalu besar pada pihak ketiga seperti penyedia layanan keuangan atau vendor teknologi yang rentan terhadap risiko kegagalan layanan atau kerentanan keamanan.
   b. Langkah Pengendalian: Evaluasi risiko vendor yang ketat sebelum bekerja sama, pembuatan kontrak yang mengatur ketersediaan layanan dan keamanan, serta melakukan pemantauan terhadap performa pihak ketiga secara teratur.

Dalam sektor perbankan, manajemen risiko dan pengendalian internal sistem IT menjadi krusial dalam menjaga kepercayaan nasabah, melindungi data keuangan yang sensitif, serta menjaga kepatuhan terhadap regulasi yang ketat. Dengan langkah-langkah pengendalian yang efektif, perbankan dapat mengurangi

risiko-risiko tersebut dan memastikan operasional yang aman dan andal.

5.8 Contoh Kasus dalam Bidang Kesehatan

Gambar 5.8. Bidang Kesehatan
Sumber : https://www.opendei.eu/

Dalam bidang kesehatan, pengendalian internal dan manajemen risiko sistem IT memiliki peran penting untuk melindungi informasi medis sensitif, menjaga keandalan sistem, serta memastikan kepatuhan terhadap regulasi privasi data kesehatan. Berikut adalah contoh kasus terkait pengendalian internal dan manajemen risiko sistem IT dalam industri kesehatan: (Leitch 2016)

1. **Kerahasiaan dan Keamanan Informasi Pasien:**
    a. Risiko: Ancaman terhadap kerahasiaan informasi medis pasien seperti pencurian identitas, akses ilegal terhadap catatan medis, atau serangan siber terhadap sistem kesehatan.
    b. Langkah Pengendalian: Enkripsi data medis sensitif, penggunaan otorisasi akses yang ketat, pelatihan karyawan tentang keamanan informasi, serta implementasi firewall dan perangkat lunak keamanan yang canggih.

2. **Kegagalan Sistem Elektronik Rekam Medis (EHR):**
    a. Risiko: Kemungkinan terjadinya gangguan atau kegagalan sistem EHR yang dapat menghambat akses terhadap informasi medis pasien atau mengganggu layanan kesehatan.
    b. Langkah Pengendalian: Pemantauan dan pemeliharaan rutin pada sistem EHR, perencanaan pemulihan bencana yang terstruktur, serta kebijakan backup data secara berkala untuk memastikan ketersediaan informasi medis dalam situasi darurat.
3. **Pelanggaran Kepatuhan Terhadap HIPAA (Health Insurance Portability and Accountability Act):**
    a. Risiko: Pelanggaran aturan privasi data kesehatan yang ditetapkan oleh HIPAA dapat mengakibatkan sanksi hukum yang serius dan kerugian reputasi bagi penyedia layanan kesehatan.
    b. Langkah Pengendalian: Penerapan prosedur kepatuhan HIPAA yang ketat, pelatihan staf tentang privasi data kesehatan, serta audit rutin untuk memastikan kepatuhan terhadap regulasi tersebut.
4. **Ketergantungan pada Teknologi Medis:**
    a. Risiko: Ketergantungan terhadap peralatan medis yang menggunakan teknologi informasi rentan terhadap gangguan operasional atau kerentanan keamanan.
    b. Langkah Pengendalian: Pemeliharaan rutin peralatan medis, pemantauan keamanan jaringan yang terhubung dengan peralatan medis, serta penggunaan perangkat lunak yang terupdate secara berkala.
5. **Manajemen Risiko terkait Pemrosesan Data Kesehatan Besar:**
    a. Risiko: Risiko besar terkait dengan pemrosesan dan penyimpanan data kesehatan yang besar, seperti risiko kehilangan atau korupsi data.
    b. Langkah Pengendalian: Sistem pencadangan data yang andal, enkripsi data yang disimpan, serta kebijakan dan prosedur yang ketat dalam pengelolaan dan pemrosesan

data besar untuk memastikan keamanan dan integritas data.

Pengendalian internal yang kuat dan manajemen risiko sistem IT yang efektif dalam industri kesehatan sangat penting untuk melindungi informasi sensitif pasien, menjaga ketersediaan layanan kesehatan yang andal, dan mematuhi peraturan privasi data kesehatan yang ketat. Dengan demikian, memberikan perlindungan bagi pasien dan meningkatkan kepercayaan terhadap penyedia layanan kesehatan.

5.9 Contoh Kasus dalam Bidang Komunikasi

Gambar 5.9. Bidang Komunikasi
Sumber : https://www.zdnet.com/

Dalam industri telekomunikasi, pengendalian internal dan manajemen risiko sistem IT sangat vital untuk menjaga jaringan yang andal, melindungi data pelanggan, serta memastikan kehandalan layanan. Berikut adalah contoh kasus terkait pengendalian internal dan manajemen risiko sistem IT dalam industri telekomunikasi: (Leitch 2016)

1. **Keamanan Jaringan dan Data Pelanggan:**
   a. Risiko: Ancaman terhadap keamanan jaringan seperti serangan DDoS (*Distributed Denial of Service*) yang dapat mengganggu layanan atau pencurian data pribadi pelanggan.
   b. Langkah Pengendalian: Implementasi firewall yang kuat, pemantauan keamanan jaringan secara terus-menerus, enkripsi data pelanggan, serta pelatihan karyawan tentang deteksi dan respons terhadap serangan siber.
2. **Kegagalan atau Gangguan Layanan Telekomunikasi:**
   a. Risiko: Kegagalan dalam layanan jaringan atau gangguan teknis yang dapat mengganggu konektivitas atau kualitas layanan bagi pelanggan.
   b. Langkah Pengendalian: Pemantauan jaringan secara terus-menerus, rencana pemulihan bencana yang terstruktur, serta pengujian dan pemeliharaan rutin pada infrastruktur jaringan.
3. **Pelanggaran Privasi Pelanggan dan Kepatuhan Regulasi:**
   a. Risiko: Pelanggaran terhadap privasi pelanggan atau aturan regulasi telekomunikasi yang dapat mengakibatkan sanksi hukum dan penurunan kepercayaan pelanggan.
   b. Langkah Pengendalian: Implementasi kebijakan privasi yang ketat sesuai dengan regulasi seperti GDPR atau FCC, audit kepatuhan secara berkala, serta pelatihan karyawan tentang pentingnya privasi data pelanggan.
4. **Manajemen Kinerja Infrastruktur Telekomunikasi:**
   a. Risiko: Risiko kinerja rendah pada infrastruktur telekomunikasi yang dapat mengakibatkan lambatnya layanan atau ketidakstabilan jaringan.
   b. Langkah Pengendalian: Pemantauan dan analisis kinerja infrastruktur secara berkala, pemeliharaan rutin pada perangkat keras jaringan, serta penggunaan teknologi yang memungkinkan skalabilitas dan efisiensi jaringan.
5. **Ketergantungan pada Pihak Ketiga atau Vendor:**
   a. Risiko: Ketergantungan terlalu besar pada pihak ketiga atau vendor yang dapat menghadapi risiko kegagalan layanan atau masalah keamanan.

b. Langkah Pengendalian: Evaluasi risiko vendor yang ketat sebelum kerja sama, pengawasan dan penilaian performa vendor secara teratur, serta perencanaan alternatif jika terjadi kegagalan dari pihak ketiga.

Pengendalian internal dan manajemen risiko sistem IT yang efektif dalam industri telekomunikasi sangat penting untuk menjaga kualitas layanan, keamanan data, dan kepercayaan pelanggan. Dengan langkah-langkah pengendalian yang tepat, perusahaan telekomunikasi dapat mengurangi dampak negatif dari risiko-risiko tersebut dan memastikan layanan yang handal bagi pelanggan.

5.10 Contoh Kasus dalam Bidang Teknologi Informasi

Gambar 5.10. Bidang Teknologi Informasi
Sumber : https://visaenvoy.com/

Dalam bidang komputer dan teknologi informasi, pengendalian internal dan manajemen risiko sistem IT sangat penting untuk menjaga keamanan, ketersediaan, dan integritas data, serta untuk memastikan operasional yang lancar. Berikut adalah contoh kasus terkait pengendalian internal dan manajemen risiko sistem IT dalam bidang komputer: (Leitch 2016)

1. **Keamanan Informasi dan Serangan Siber:**
   a. Risiko: Ancaman serangan siber seperti malware, ransomware, atau serangan phishing yang dapat mengancam keamanan sistem komputer, data sensitif, atau kehilangan akses terhadap sistem.

b. Langkah Pengendalian: Implementasi firewall, antivirus yang terupdate, pemantauan keamanan sistem secara terus-menerus, pelatihan karyawan tentang praktik keamanan cyber, serta backup data yang teratur.

2. **Kegagalan Perangkat Keras atau Perangkat Lunak:**
   a. Risiko: Kemungkinan terjadi kegagalan pada perangkat keras (seperti hard drive, RAM) atau perangkat lunak yang dapat mengakibatkan kehilangan data atau gangguan operasional.
   b. Langkah Pengendalian: Pemeliharaan rutin pada perangkat keras, backup data secara berkala, penerapan update perangkat lunak yang teratur, serta rencana pemulihan bencana yang terstruktur.
3. **Pelanggaran Privasi Data Pengguna:**
   a. Risiko: Risiko pelanggaran privasi data pengguna seperti kebocoran informasi pribadi atau sensitif yang dapat menyebabkan kerugian finansial atau hilangnya kepercayaan pelanggan.
   b. Langkah Pengendalian: Enkripsi data, pengaturan akses yang ketat, kepatuhan pada regulasi privasi data (seperti GDPR), serta pelatihan karyawan tentang perlunya menjaga kerahasiaan data pengguna.
4. **Ketergantungan pada Layanan Cloud atau Pihak Ketiga:**
   a. Risiko: Ketergantungan pada layanan cloud atau vendor pihak ketiga yang dapat menyebabkan risiko kegagalan layanan atau kerentanan keamanan.
   b. Langkah Pengendalian: Evaluasi keamanan layanan cloud atau vendor sebelum penggunaan, perjanjian kontrak yang memperhatikan keamanan dan keandalan layanan, serta pemantauan performa vendor secara teratur.
5. **Kesalahan Manusia dan Pengelolaan Akses:**
   a. Risiko: Kesalahan manusia dalam manajemen akses atau dalam pengoperasian sistem yang dapat menyebabkan kebocoran data atau ketidakakuratan informasi.
   b. Langkah Pengendalian: Implementasi pengelolaan hak akses yang tepat, pelatihan karyawan tentang tata kelola

akses yang baik, serta audit dan pemantauan atas aktivitas pengguna.

Pengendalian internal dan manajemen risiko sistem IT yang efektif dalam bidang komputer adalah kunci dalam menjaga keamanan sistem, melindungi data sensitif, serta memastikan keandalan dan ketersediaan layanan. Dengan strategi pengendalian yang baik, perusahaan dapat mengurangi dampak negatif dari risiko-risiko tersebut dan menjaga kinerja yang optimal dari sistem komputer dan teknologi informasi.

DAFTAR PUSTAKA

Leitch M. 2016. *Intelligent Internal Control and Risk Management*. Routledge.

Nurmalitasari D. 2016. Sistem Pengendalian Intern Manajemen Risiko (Studi Di Pt. Bank Dki Unit Usaha Syariah Cabang Pondok Indah Jakarta). *J. Ilm. Mhs. FEB*.

Sarwoko H. 2020. Model Penilaian Efektifitas Satuan Pengawas Intern (Spi). :1–117.

BAB 6
IT GOVERNANCE

Oleh Ketut Tanti Kustina

6.1 Tata Kelola IT atau *IT Governance*

Dokumen teknologi informasi (TI) sangat penting dalam mengatur transaksi, memproses, dan menyebarkan informasi. Bagi beberapa organisasi TI, menjadi sangat penting untuk mendukung, mendukung, mengubah, dan mengembangkan bisnis (Ravichandran, 2018). Saat ini, setiap lembaga atau perusahaan harus mengembangkan TI. Karena investasi yang diperlukan dalam teknologi informasi, pengelolaan TI sangat penting (Dadoukis, Fiaschetti and Fusi, 2021). Pengelolaan TI yang baik memungkinkan proses TI saat ini berjalan secara sistematis, terkendali, efektif, dan efisien, sehingga dapat mengurangi biaya operasional dan meningkatkan daya saing.

Selama beberapa dekade terakhir, banyak organisasi telah menggunakan TI, dan intensitasnya telah meningkat. Tata kelola TI yang baik tidak hanya bertindak sebagai pendukung atau dukungan, tetapi juga menjadi bagian atau penentu keberhasilan organisasi (Vugec, Spremić and Bach, 2017); mereka juga memainkan peran penting dalam mendukung operasi organisasi. Ini diperlukan untuk memastikan bahwa penggunaan TI benar-benar mendukung tujuan penyelenggaraan pemerintahan, dengan memperhatikan efektivitas penggunaan sumber daya dan pengelolaan risiko yang terkait.

"*The board of directors and executive management are responsible for IT Governance*." *Information Technology* (IT) *is a crucial component of corporate governance. It encompasses the leadership, organizational structures, and processes that guarantee the organization's IT systems support and enhance its strategy and objectives*"(Helwig, Hong and Hsiao-wecksler, 2015)

Dimungkinkan bahwa eksekutif manajemen dan pimpinan puncak perusahaan bertanggung jawab atas tata kelola TI. Tata kelola TI adalah bagian dari tata kelola perusahaan, yang terdiri dari

lima kepemimpinan, struktur organisasi, dan proses untuk memastikan keberlanjutan organisasi TI dan pengembangan strategi dan tujuan organisasi. Tata kelola TI adalah bagian penting dari tata kelola perusahaan yang baik atau *good corporate governance* (Matta, Cavusoglu and Benbasat, 2018).

Di era digitalisasi saat ini, teknologi informasi (TI) sangat penting untuk kesuksesan banyak bisnis, terutama dalam manajemen finansial. Akibatnya, tata kelola perusahaan (*governance* perusahaan) dan tata kelola TI (**governance** TI) tidak dapat lagi dianggap sebagai satu entitas. Konsep tata kelola teknologi informasi, juga dikenal sebagai tata kelola IT, berkaitan dengan pengelolaan dan pengawasan sistem informasi dan teknologi informasi suatu organisasi. Konsep ini bertujuan untuk memastikan bahwa penggunaan teknologi informasi dalam organisasi dilakukan dengan cara yang efektif, efisien, dan sesuai dengan tujuan bisnis. organisasi. Tata kelola perusahaan yang baik berfokus pada individu dan kelompok profesional yang bekerja secara produktif, yang dapat diawasi dan diukur kinerjanya, dan memberikan jaminan bahwa masalah penting dapat segera ditangani. Sebaliknya, selama bertahun-tahun, TI telah dianggap membantu strategi perusahaan dan merupakan bagian penting dari strategi itu sendiri.

Tata kelola IT meliputi berbagai aspek, seperti strategi penggunaan teknologi informasi, manajemen risiko, kepatuhan terhadap peraturan dan standar, pengelolaan sumber daya IT, dan pengukuran kinerja IT. Dalam konteks bisnis, tata kelola IT sangat penting karena teknologi informasi telah menjadi bagian integral dari operasi bisnis modern. Dalam era digital, hampir semua aspek bisnis dilakukan dengan bantuan teknologi informasi, mulai dari pemasaran, penjualan, hingga pengelolaan keuangan dan sumber daya manusia.

Tata kelola TI juga mengintegrasikan dan mengoptimalisasikan metode untuk merencanakan, mengorganisasikan, melaksanakan akuisisi dan implementasi, penyediaan dan dukungan, serta monitoring dan evaluasi kinerja TI. Tata kelola TI juga memberikan dasar struktur yang mengaitkan dan menyelaraskan proses-proses TI, sumber daya TI, dan informasi

yang dibutuhkan perusahaan untuk menerapkan strateginya untuk mencapai tujuan yang telah ditetapkan.

Selain itu, dalam era digital, organisasi harus menghadapi banyak risiko, seperti keamanan data, kegagalan sistem, dan kepatuhan terhadap peraturan dan standar. Tata kelola IT dapat membantu organisasi mengidentifikasi, mengevaluasi, dan mengelola risiko yang terkait dengan penggunaan teknologi informasi.

6.2 Alasan Mengapa It Governance Penting Dilakukan

Tata kelola IT atau IT governance adalah suatu konsep yang berkaitan dengan pengelolaan dan pengawasan sistem informasi dan teknologi informasi dalam suatu organisasi. Konsep ini sangat penting untuk perusahaan karena teknologi informasi telah menjadi bagian integral dari operasi bisnis modern. Berikut adalah beberapa alasan mengapa tata kelola TI penting untuk perusahaan:

1. Meningkatkan efisiensi operasional.
   Dengan menerapkan tata kelola IT yang baik, perusahaan dapat meningkatkan efisiensi operasionalnya. Hal ini dapat dicapai dengan mengoptimalkan penggunaan teknologi informasi dalam berbagai aspek bisnis, seperti pemasaran, penjualan, pengelolaan keuangan, dan sumber daya manusia.
2. Mengelola risiko.
   Dalam era digital, perusahaan harus menghadapi berbagai risiko terkait dengan penggunaan teknologi informasi, seperti keamanan data, kegagalan sistem, dan kepatuhan terhadap peraturan dan standar. Dengan menerapkan tata kelola IT yang baik, perusahaan dapat mengidentifikasi, mengevaluasi, dan mengelola risiko yang terkait dengan penggunaan teknologi informasi.
3. Memastikan kepatuhan terhadap peraturan dan standar.
   Dalam era digital, perusahaan harus mematuhi berbagai peraturan dan standar terkait dengan penggunaan teknologi informasi, seperti GDPR, HIPAA, dan PCI DSS. Dengan menerapkan tata kelola IT yang baik, perusahaan dapat

memastikan bahwa penggunaan teknologi informasi dilakukan sesuai dengan peraturan dan standar yang berlaku.

4. Meningkatkan kualitas produk atau layanan
   Dengan menerapkan tata kelola IT yang baik, perusahaan dapat meningkatkan kualitas produk atau layanan yang dihasilkan. Hal ini dapat dicapai dengan mengoptimalkan penggunaan teknologi informasi dalam berbagai aspek bisnis, seperti pengembangan produk, manajemen rantai pasok, dan layanan pelanggan.
5. Meningkatkan kepuasan pelanggan
   Dengan menerapkan tata kelola IT yang baik, perusahaan dapat meningkatkan kepuasan pelanggan. Hal ini dapat dicapai dengan mengoptimalkan penggunaan teknologi informasi dalam berbagai aspek bisnis, seperti pelayanan pelanggan, pengiriman produk, dan manajemen retur.

Dalam keseluruhan, tata kelola IT sangat penting untuk perusahaan karena teknologi informasi telah menjadi bagian integral dari operasi bisnis modern. Dengan menerapkan tata kelola IT yang baik, perusahaan dapat meningkatkan efisiensi operasional, mengelola risiko, memastikan kepatuhan terhadap peraturan dan standar, meningkatkan kualitas produk atau layanan, dan meningkatkan kepuasan pelanggan.

COBIT (*Control Objective for Information and Related Technology*) adalah sekumpulan pedoman dan panduan untuk menerapkan governance IT yang membantu auditor, manajemen, dan pengguna menjembatani perbedaan antara resiko dan bisnis, kebutuhan kontrol, dan masalah teknis. COBIT dikembangkan oleh IT *Governance Institute* (ITGI). IT *Governance Institute* (ITGI), yang merupakan anggota *dari Association of Information System Audit and Control* (ISACA), bertanggung jawab untuk mengembangkan COBIT.

6.3 Pedoman Pelaksanaan IT Governance di Indonesia

IT governance di Indonesia mengacu pada prinsip-prinsip tata kelola teknologi informasi yang diterapkan dalam organisasi di Indonesia. Prinsip-prinsip ini mencakup pengelolaan teknologi informasi secara efektif, efisien, dan sesuai dengan tujuan bisnis

organisasi. Beberapa pedoman dan standar yang digunakan dalam IT governance di Indonesia antara lain:

1. Pedoman Tata Kelola Perusahaan Terbuka.
   Surat Edaran Otoritas Jasa Keuangan Nomor 32/SEOJK.04/2015 tentang Pedoman Tata Kelola Perusahaan Terbuka mengatur tata kelola perusahaan terbuka di Indonesia. Pedoman ini mencakup prinsip-prinsip tata kelola perusahaan yang baik, termasuk tata kelola teknologi informasi. Standar ISO 27001.
   Standar ISO 27001 adalah standar internasional untuk keamanan informasi. Standar ini mencakup berbagai aspek keamanan informasi, termasuk manajemen risiko, keamanan jaringan, dan keamanan data. Standar ini dapat digunakan sebagai pedoman dalam menerapkan tata kelola teknologi informasi yang baik di Indonesia.
2. Framework COBIT 5
   COBIT 5 adalah kerangka kerja tata kelola TI yang dapat digunakan untuk mengukur kemampuan manajemen TI. Ini juga dapat digunakan sebagai pedoman untuk mengukur tingkat risiko dan perumusan mitigasi risiko. Framework ini dapat digunakan sebagai pedoman untuk menerapkan tata kelola TI yang baik di Indonesia.
3. Pedoman Tata Kelola Perbankan.
   Pedoman Tata Kelola Perbankan di Indonesia diatur dalam peraturan bank sentral mengenai penerapan tata kelola perusahaan yang baik bagi bank umum. Pedoman ini mencakup prinsip-prinsip tata kelola perusahaan yang baik, termasuk tata kelola teknologi informasi.

Dalam keseluruhan, IT governance di Indonesia mencakup prinsip-prinsip tata kelola teknologi informasi yang diterapkan dalam organisasi di Indonesia. Beberapa pedoman dan standar yang digunakan dalam IT governance di Indonesia antara lain Pedoman Tata Kelola Perusahaan Terbuka, Standar ISO 27001, Framework COBIT 5, dan Pedoman Tata Kelola Perbankan. Pedoman dan standar ini dapat digunakan sebagai pedoman dalam menerapkan tata kelola teknologi informasi yang baik di Indonesia.

6.4 Tahapan Pelaksanaan IT Governance

Sebuah perusahaan dapat menerapkan tata kelola teknologi informasi (IT *governance*) dengan mengikuti serangkaian langkah-langkah dan praktik terbaik yang dirancang untuk memastikan bahwa teknologi informasi (TI) mendukung tujuan bisnis, dikelola dengan baik, dan keamanannya terjaga. Berikut adalah langkah-langkah umum yang dapat diikuti oleh perusahaan dalam melakukan IT governance:

1. **Penetapan Visi dan Strategi IT,** meliputi :Identifikasi visi dan tujuan jangka panjang untuk pengelolaan TI dalam organisasi kemudian kembangkan strategi TI yang sejalan dengan tujuan bisnis perusahaan.
2. **Penetapan Struktur Organisasi** meliputi ; menentukan struktur organisasi TI yang jelas dengan peran dan tanggung jawab yang ditetapkan dan pastikan keterlibatan tingkat eksekutif dan dewan direksi dalam pengambilan keputusan TI.
3. **Identifikasi Stakeholder** meliputi ; melakukan Identifikasi pemangku kepentingan (stakeholder) yang terlibat dalam pengelolaan TI, termasuk eksekutif, pengguna akhir, mitra bisnis, dan auditor.
4. **Pembentukan Komite IT Governance** yaitu ; Bentuk komite IT governance yang akan memantau dan mengarahkan inisiatif TI dan kepatuhan. Dan pastikan komite ini memiliki representasi dari berbagai fungsi dalam organisasi.
5. **Penetapan Kebijakan dan Prosedur**: yaitu melakukan pengembangan kebijakan dan prosedur yang merinci cara TI akan dikelola, termasuk keamanan siber, manajemen risiko, pengelolaan proyek TI, dan kepatuhan regulasi.
6. **Menggunakan framework**: Organisasi dapat menggunakan framework seperti ITIL, ISO/IEC 17799, COSO, dan COBIT 5 untuk audit dan proses pengelolaan sistem informasi.
7. **Penilaian Risiko TI**, dengan melakukan Identifikasi dan evaluasi risiko-risiko yang terkait dengan TI, termasuk risiko keamanan siber, kegagalan sistem, dan ketidakpatuhan regulasi. Buat rencana mitigasi risiko yang efektif.
8. **Penyusunan Anggaran TI** , meliputi kegiatan menentukan jumlah anggaran TI yang mencerminkan strategi dan

kebutuhan bisnis dan pastikan anggaran mencakup investasi untuk inovasi dan pengembangan TI.

9. **Pemantauan Kinerja TI**: Pembantaian dilakukan terhadap implementasikan metrik dan indikator kinerja untuk mengukur kinerja TI dan memastikan bahwa TI memberikan nilai bisnis yang diharapkan. Dan lakukan audit secara berkala untuk mengevaluasi kepatuhan dan kinerja TI.
10. **Manajemen Proyek TI** dengan menerapkan metodologi manajemen proyek yang efektif untuk mengelola proyek-proyek TI dengan baik, termasuk pengendalian anggaran, jadwal, dan risiko.
11. **Keamanan Sistem dan Data**; yang harus dilakukan adalah melindungi data dan sistem TI dengan menerapkan praktik keamanan siber terbaik. Lakukan evaluasi keamanan secara berkala dan pelatihan untuk staf.
12. **Pelaporan dan Komunikasi**:
    a. Sampaikan laporan berkala tentang kinerja TI dan kepatuhan kepada komite IT governance dan pemangku kepentingan lainnya.
    b. Pastikan komunikasi yang efektif antara TI dan berbagai departemen bisnis.
13. **Evaluasi dan Peningkatan Berkelanjutan**: Evaluasi secara berkala kerangka kerja IT governance dan lakukan perbaikan berkelanjutan berdasarkan pengalaman dan perubahan dalam lingkungan bisnis dan teknologi.
14. **Pelatihan dan Pengembangan SDM TI**: Ini penting untuk dilakukan karena Berinvestasi dalam pelatihan dan pengembangan tim TI agar mereka terus meningkatkan keterampilan dan pengetahuan mereka.
15. **Manajemen Vendor**: lakukan manajemen vendor yang baik, Kelola hubungan dengan penyedia layanan TI (vendor) dengan baik, termasuk pemilihan, pengawasan, dan pemantauan layanan yang disediakan.
16. **Evaluasi Proyek TI**: Evaluasi proyek-proyek TI secara berkala untuk memastikan bahwa mereka mencapai tujuan bisnis dan memenuhi kebutuhan organisasi.

17. **Kepatuhan Regulasi**:Pastikan kepatuhan penuh terhadap peraturan dan regulasi yang berlaku, seperti perlindungan data pribadi dan peraturan industri yang relevan.
    Implementasi tata kelola TI yang efektif memungkinkan perusahaan untuk mengoptimalkan penggunaan sumber daya TI, mengelola risiko dengan baik, dan menghadirkan nilai bisnis yang signifikan melalui teknologi (Tjong *et al.*, 2018). Itu juga memastikan bahwa TI mendukung strategi dan tujuan bisnis yang lebih luas.

6.5 Good IT Governance dan Good Corporate Governance

Tata kelola TI yang baik (GIG) dan tata kelola perusahaan yang baik (GCG) saling terkait dan dapat mendukung satu sama lain dalam menciptakan lingkungan bisnis yang sehat dan berkelanjutan(De Haes *et al.*, 2020). Tata kelola TI yang baik dan tata kelola perusahaan yang baik keduanya penting bagi organisasi untuk mencapai kinerja yang optimal dan memastikan akuntabilitas, transparansi, dan fairness. Keterkaitan antara keduanya dapat dilihat dalam beberapa cara:

1. **Strategi dan Pencapaian Tujuan**: GIG memastikan bahwa TI mendukung strategi bisnis perusahaan, yang pada gilirannya mendukung tujuan bisnis. GCG memastikan bahwa pengambilan keputusan perusahaan secara keseluruhan sesuai dengan tujuan bisnis dan kepentingan pemegang saham.
2. **Manajemen Risiko**: Baik GIG maupun GCG memiliki fokus pada manajemen risiko. GIG berkaitan dengan risiko terkait TI, sedangkan GCG berkaitan dengan risiko perusahaan secara keseluruhan. Keduanya berkontribusi untuk mengidentifikasi, mengevaluasi, dan mengelola risiko-risiko yang dapat mempengaruhi keseluruhan kinerja perusahaan.
3. **Pertanggungjawaban dan Transparansi**: Baik GIG maupun GCG menekankan pertanggungjawaban dan transparansi dalam pengambilan keputusan dan pelaksanaan strategi. GIG memastikan pertanggungjawaban dalam penggunaan TI, sementara GCG memastikan pertanggungjawaban dalam pengelolaan perusahaan secara keseluruhan.

4. **Kepatuhan dan Etika**: GIG dan GCG sama-sama menekankan kepatuhan terhadap hukum dan etika dalam tata kelola dan pengambilan keputusan perusahaan.

Dalam rangka menciptakan perusahaan yang berkinerja tinggi dan berkelanjutan, penting untuk memiliki GIG yang baik yang terintegrasi dengan GCG yang baik. Keduanya bersama-sama membantu menciptakan lingkungan yang mendukung pertumbuhan, inovasi, dan keberlanjutan perusahaan.

DAFTAR PUSTAKA

Dadoukis, A., Fiaschetti, M. and Fusi, G. 2021. 'IT adoption and bank performance during the Covid-19 pandemic', *Economics Letters*, 204, p. 109904. doi: 10.1016/j.econlet.2021.109904.

De Haes, S. *et al.* 2020. 'Enterprise Governance of IT, Alignment, and Value', *Management for Professionals*, Part F574(January 2020), pp. 1–13. doi: 10.1007/978-3-030-25918-1_1.

Matta, M., Cavusoglu, H. and Benbasat, I. 2018. 'Understanding the Board's Involvement in Information Technology Governance: Theory, Review and Research Agenda', *SSRN Electronic Journal*. doi: 10.2139/ssrn.2778811.

Ravichandran, T. 2018. 'Exploring the relationships between IT competence, innovation capacity and organizational agility', *Journal of Strategic Information Systems*, 27(1), pp. 22–42. doi: 10.1016/j.jsis.2017.07.002.

Tjong, Y. *et al.* 2018. 'Benefits to implementing IT governance in higher education

BAB 7
PENGAUDITAN TEKNOLOGI INFORMASI AKUNTANSI DAN BISNIS

Oleh Nano Suyatna

7.1 Pendahuluan

Pengauditan sering disebut Auditing adalah akumulasi dan evaluasi bukti tentang informasi untuk menentukan dan melaporkan tingkat kesesuaian antara informasi dan kriteria yang ditetapkan. Audit harus dilakukan oleh orang independen yang kompeten.(Alvin A. Arens, Randal J. Elder, 2012).

Pengauditan Teknologi Informasi (TI) adalah proses evaluasi sistem informasi organisasi untuk memastikan pengelolaan, kontrol, dan sumber daya TI digunakan secara efisien, aman, dan sejalan dengan strategi dan tujuan organisasi. Pengauditan TI melibatkan evaluasi terhadap infrastruktur TI, perangkat lunak, data, dan operasi TI. Melalui pengauditan TI, sebuah organisasi bisa mengidentifikasi kelemahan dan masalah potensial dalam sistem TI, dan memastikan kepatuhan terhadap standar dan regulasi industri serta hukum yang berlaku. Pengauditan Teknologi Informasi Sistem Akuntansi adalah proses evaluasi dan pemeriksaan sistem informasi yang digunakan dalam operasional akuntansi sebuah organisasi atau perusahaan. Proses ini bertujuan untuk memastikan bahwa sistem akuntansi berfungsi dengan baik, aman, dan dapat diandalkan dalam mencatat, mengelola, dan melaporkan transaksi keuangan. Pengauditan ini juga mencakup evaluasi atas pengendalian internal dan prosedur keamanan sistem untuk menghindari potensi kecurangan atau kehilangan data. Dengan melaksanakan pengauditan TI sistem akuntansi, perusahaan dapat meningkatkan efisiensi operasionalnya dan memenuhi persyaratan regulasi yang berlaku(Hayes et al., 2014). Pengauditan Teknologi Informasi (TI) melibatkan evaluasi komprehensif terhadap sistem informasi dan infrastruktur TI suatu organisasi untuk memastikan

efisiensi, keamanan, dan kepatuhan terhadap regulasi yang berlaku. Ini mencakup pemeriksaan infrastruktur TI, perangkat lunak, dan operasi terkait untuk mengidentifikasi kelemahan dan memastikan keselarasan dengan tujuan organisasi. Sementara itu, pengauditan TI pada sistem akuntansi fokus pada evaluasi sistem informasi yang digunakan dalam fungsi akuntansi, termasuk penilaian terhadap pengendalian internal dan keamanan data, dengan tujuan untuk mencegah kecurangan dan kehilangan data, sekaligus memastikan efisiensi operasional dan kepatuhan terhadap persyaratan regulasi(Landoll, 2016).

Pengauditan sistem informasi akuntansi penting dalam pengauditan laporan keuangan karena sistem informasi akuntansi seringkali menjadi basis dari data keuangan yang dicatat. Dengan memeriksa keakuratan, keamanan, dan efisiensi sistem informasi, auditor bisa lebih yakin bahwa laporan keuangan perusahaan adalah akurat dan dapat diandalkan.

7.2 Pengenalan Pengauditan Teknologi Informasi Akuntansi dan Bisnis

Pengauditan Teknologi Informasi Akuntansi dan Bisnis merupakan pendekatan pengauditan yang fokus pada penggunaan teknologi informasi dalam sistem akuntansi dan operasi bisnis suatu perusahaan. Tujuan utamanya adalah untuk memastikan bahwa teknologi informasi digunakan secara efektif dan efisien dalam mendukung proses bisnis dan pelaporan keuangan, serta untuk memeriksa keamanan data dan integritas sistem untuk menghindari potensi risiko dan fraud.(Robertson, 2010).

7.2.1 Definisi Pengauditan Teknologi Informasi Akuntansi dan Bisnis

Pengauditan Teknologi Informasi adalah proses pemeriksaan, evaluasi, dan verifikasi sistem teknologi informasi suatu organisasi, termasuk perangkat keras (*hardware*), perangkat lunak (*software*), infrastruktur jaringan, dan prosedur-prosedur terkait, dengan tujuan untuk menilai efektivitas, keamanan, integritas, dan ketaatan terhadap kebijakan dan standar yang berlaku, serta mengidentifikasi potensi risiko dan rekomendasi

perbaikan yang diperlukan untuk mendukung tujuan bisnis dan melindungi aset informasi perusahaan(Champlain, 2019).

Pengauditan Teknologi Informasi adalah proses pemeriksaan, evaluasi, dan verifikasi infrastruktur teknologi informasi, sistem, dan praktik yang digunakan dalam suatu organisasi. Tujuannya adalah untuk memastikan keandalan, keamanan, dan kepatuhan terhadap kebijakan serta regulasi yang berlaku(Peret, 2022).

Pengauditan Teknologi Informasi adalah metode pemeriksaan dan penilaian terhadap sistem teknologi informasi untuk mengidentifikasi potensi risiko, mengukur efisiensi operasional, dan memastikan kepatuhan terhadap peraturan dan standar yang berlaku(Robert & Brown, 2004).

Pengauditan Teknologi Informasi adalah pemeriksaan independen terhadap sistem informasi suatu entitas untuk menilai kualitas dan keefektifan kontrol internal, serta mengidentifikasi potensi risiko yang terkait dengan teknologi informasi (Hall, 2011).

Pengauditan Teknologi Informasi adalah proses pemeriksaan sistem teknologi informasi, termasuk perangkat keras, perangkat lunak, data, dan praktik operasional yang terkait, dengan tujuan untuk memastikan integritas data, keamanan informasi, dan ketaatan terhadap regulasi. Pengauditan Teknologi Informasi (TI) adalah proses evaluasi sistem informasi organisasi untuk memastikan pengelolaan, kontrol, dan sumber daya TI digunakan secara efisien, aman, dan sejalan dengan strategi dan tujuan organisasi. Ini melibatkan evaluasi infrastruktur TI, perangkat lunak, data, dan operasi TI. Dengan pengauditan TI, organisasi dapat mengidentifikasi kelemahan dan masalah potensial dalam sistem TI mereka serta memastikan kepatuhan terhadap standar dan regulasi industri serta hukum yang berlaku(Turner & Weickgenannt, 2008).

Pengauditan TI Sistem Akuntansi adalah evaluasi sistem informasi yang digunakan dalam operasional akuntansi sebuah organisasi. Tujuannya adalah memastikan bahwa sistem akuntansi berfungsi dengan baik, aman, dan dapat diandalkan dalam mencatat, mengelola, dan melaporkan transaksi keuangan. Ini juga mencakup pengendalian internal dan keamanan sistem untuk mencegah

potensi kecurangan atau kehilangan data(Alvin A. Arens, Randal J. Elder, 2012).

Pengauditan Teknologi Informasi Akuntansi dan Bisnis adalah pendekatan yang fokus pada penggunaan teknologi informasi dalam sistem akuntansi dan operasi bisnis. Ini bertujuan untuk memastikan efektivitas dan efisiensi penggunaan teknologi informasi dalam mendukung proses bisnis dan pelaporan keuangan, serta untuk memeriksa keamanan data dan integritas sistem guna menghindari risiko dan fraud(Sigler & Rainey, 2016).

Semua definisi tersebut diatas mencakup pemeriksaan dan evaluasi terhadap infrastruktur TI, perangkat lunak, dan praktik operasional untuk mengidentifikasi risiko, memastikan kepatuhan, dan meningkatkan efisiensi dalam konteks organisasi.

7.2.2 Tujuan Pengauditan Teknologi Informasi Akuntansi dan Bisnis

Tujuan Pengauditan Teknologi Informasi Akuntansi dan Bisnis adalah untuk memastikan bahwa teknologi informasi digunakan secara efektif, efisien, dan aman dalam mendukung proses akuntansi dan operasi bisnis suatu organisasi. Ini mencakup pemeriksaan terhadap sistem akuntansi, pengendalian internal, keamanan data, serta ketaatan terhadap regulasi dan kebijakan yang berlaku. Dengan demikian, tujuan utama dari pengauditan ini adalah untuk mengidentifikasi potensi risiko, melindungi aset perusahaan, dan memastikan integritas informasi keuangan. Menjelaskan tujuan dan konsep pengauditan teknologi informasi, termasuk dalam konteks akuntansi dan bisnis (Hall, 2011), juga mencakup tujuan pengauditan teknologi informasi dalam lingkungan bisnis.

7.2.3 Peran Auditor Teknologi Informasi Akuntansi dan Bisnis

Peran Auditor Teknologi Informasi Akuntansi dan Bisnis adalah sangat penting dalam memastikan keandalan dan keamanan sistem teknologi informasi yang digunakan dalam proses akuntansi dan operasi bisnis suatu organisasi. Berikut adalah beberapa peran utama auditor dalam konteks ini (Hall, 2011):

1. Pemeriksaan Sistem: Auditor melakukan pemeriksaan menyeluruh terhadap sistem teknologi informasi, termasuk perangkat keras, perangkat lunak, basis data, dan infrastruktur jaringan, untuk memastikan bahwa sistem tersebut beroperasi dengan baik dan sesuai dengan kebutuhan bisnis.
2. Evaluasi Pengendalian Internal: Auditor mengevaluasi pengendalian internal yang diterapkan dalam sistem teknologi informasi, seperti prosedur otentikasi, pengendalian akses, dan pemantauan aktivitas, untuk memastikan bahwa risiko kecurangan dan kesalahan dapat diminimalkan.
3. Penilaian Keamanan: Auditor memeriksa keamanan sistem untuk melindungi data sensitif dan mengidentifikasi potensi kerentanan yang dapat dieksploitasi oleh pihak yang tidak sah.
4. Ketaatan Terhadap Regulasi: Auditor memastikan bahwa organisasi mematuhi semua regulasi yang berlaku terkait dengan penggunaan teknologi informasi dalam akuntansi dan operasi bisnis.
5. Rekomendasi Perbaikan: Auditor memberikan rekomendasi perbaikan yang diperlukan untuk mengatasi masalah yang teridentifikasi dalam pemeriksaan, sehingga organisasi dapat meningkatkan efisiensi, keamanan, dan kepatuhan.

Menjelaskan peran dan tanggung jawab auditor dalam pengauditan teknologi informasi, termasuk dalam konteks akuntansi dan bisnis. Mencakup peran auditor dalam pengauditan teknologi informasi dan bagaimana hal ini berhubungan dengan bisnis dan akuntansi(Alvin A. Arens, Randal J. Elder, 2012)

7.2.4 Proses Audit Teknologi Informasi Akuntansi dan Bisnis

Proses Audit Teknologi Informasi Akuntansi dan Bisnis melibatkan serangkaian tahapan yang dilakukan oleh auditor untuk mengevaluasi efektivitas, keamanan, dan kepatuhan terhadap standar dalam penggunaan teknologi informasi dalam konteks

akuntansi dan bisnis. Berikut adalah tahapan-tahapan utama dalam proses ini (Hall, 2011):

1. Perencanaan Audit:
   a. Menentukan tujuan audit dan lingkupnya.
   b. Mengidentifikasi risiko yang terkait dengan teknologi informasi.
   c. Memilih dan mengumpulkan tim audit yang sesuai.
   d. Merancang program audit yang mencakup pemeriksaan teknis dan fungsional.
2. Evaluasi Pengendalian Internal: Memeriksa pengendalian internal yang diterapkan dalam sistem teknologi informasi, seperti pengendalian akses, otentikasi, pemantauan, dan prosedur keamanan. Menilai efektivitas pengendalian internal dalam mengurangi risiko kesalahan dan penyalahgunaan.
3. Pemeriksaan Teknis: Melakukan pemeriksaan teknis terhadap sistem, termasuk uji penetrasi dan pemindaian keamanan untuk mengidentifikasi kerentanan dan potensi risiko keamanan.
4. Pemeriksaan Fungsional: Memeriksa operasionalitas sistem dan proses bisnis yang melibatkan teknologi informasi. Memeriksa keakuratan, keandalan, dan integritas data yang dihasilkan oleh sistem.
5. Pemeriksaan Ketaatan Regulasi: Memastikan bahwa organisasi mematuhi semua regulasi dan kebijakan yang berlaku terkait dengan penggunaan teknologi informasi dalam akuntansi dan bisnis.
6. Pelaporan Hasil Audit: Menyusun laporan audit yang mencakup temuan, rekomendasi, dan tindakan perbaikan yang diperlukan. Berkomunikasi dengan manajemen organisasi tentang hasil audit.
7. Tindak Lanjut: Memantau implementasi tindakan perbaikan yang direkomendasikan. Melakukan tindak lanjut untuk memastikan bahwa masalah yang teridentifikasi telah diatasi.

Yang memberikan panduan yang mendalam mengenai proses audit teknologi informasi dalam konteks akuntansi dan

bisnis (Hall, 2011). Mencakup langkah-langkah dan konsep dalam proses audit teknologi informasi yang terkait dengan bisnis dan akuntansi(Alvin A. Arens, Randal J. Elder, 2012)

7.2.5 Standar Audit Teknologi Informasi Akuntansi dan Bisnis

Standar Audit Teknologi Informasi Akuntansi dan Bisnis adalah pedoman dan kerangka kerja yang digunakan oleh auditor untuk melakukan pengauditan teknologi informasi dalam konteks akuntansi dan bisnis. Standar ini membantu memastikan bahwa pengauditan dilakukan secara konsisten, profesional, dan efektif. Beberapa standar yang umumnya digunakan dalam pengauditan teknologi informasi antara lain:

1. **Standar Audit Umum (*Generally Accepted Auditing Standards* - GAAS)**

   Standar ini mencakup prinsip-prinsip dasar yang harus diikuti oleh auditor dalam melakukan pengauditan, termasuk pengauditan teknologi informasi dalam konteks akuntansi dan bisnis. Standar Audit Umum (GAAS) dan Standar AICPA dapat ditemukan dalam "*AU-C Section 300: Planning and Supervision*" dari "*Generally Accepted Auditing Standards*" yang diterbitkan oleh AICPA. (www.aicpa-cima.com). Untuk lingkup Indonesia dikeluarkan oleh IAPI. (https://iapi.or.id/standar-profesional-akuntan-publik/).

2. **Standar ISACA**

   ISACA (*Information Systems Audit and Control Association*) memiliki standar audit khusus yang digunakan dalam pengauditan teknologi informasi, seperti COBIT (*Control Objectives for Information and Related Technologies*) dan ITAF (IT *Assurance Framework*). Standar ISACA seperti COBIT dapat ditemukan di situs web resmi ISACA. (www.isaca.org).

   ISACA's COBIT (Control Objectives for Information and Related Technologies) adalah kerangka kerja yang dirancang untuk membantu organisasi dalam mengelola dan mengendalikan teknologi informasi (TI) dengan lebih efektif. Berikut adalah rincian peran utama COBIT(ISACA Governance and Manajement, 2019):

a. Membantu dalam Pengelolaan dan Kendali TI: COBIT memberikan panduan dan kontrol yang jelas untuk mengelola TI dalam organisasi. Ini membantu organisasi memahami bagaimana TI mendukung tujuan bisnis mereka dan bagaimana mengendalikan risiko yang terkait dengan TI.
b. Menyediakan Struktur Kerja: COBIT menyediakan kerangka kerja yang terstruktur untuk pengelolaan TI. Ini mencakup proses-proses, tugas, dan tanggung jawab yang harus diterapkan dalam organisasi untuk mencapai tujuan bisnis dan menjaga keamanan TI.
c. Meningkatkan Transparansi dan Akuntabilitas: Kerangka kerja COBIT meningkatkan transparansi dalam pengelolaan TI dengan mengidentifikasi objektif kontrol yang jelas. Ini membantu organisasi untuk lebih akuntabel dalam hal bagaimana mereka mengelola dan melindungi informasi.
d. Menghubungkan TI dengan Tujuan Bisnis: Salah satu peran utama COBIT adalah menghubungkan TI dengan tujuan bisnis. Ini membantu organisasi memahami bagaimana TI dapat mendukung pencapaian tujuan bisnis dan mengukur kinerja TI secara efektif.
e. Mengidentifikasi Risiko dan Peluang: COBIT membantu organisasi mengidentifikasi risiko dan peluang yang terkait dengan TI. Dengan pemahaman ini, organisasi dapat mengambil tindakan yang sesuai untuk mengurangi risiko dan memanfaatkan peluang dengan lebih baik.
f. Menyediakan Panduan Terkini: COBIT terus diperbarui dan ditingkatkan sesuai dengan perkembangan teknologi dan tren bisnis. Ini memastikan bahwa organisasi selalu memiliki panduan terkini untuk mengelola TI mereka.
g. Mendukung Kepatuhan dan Audit: COBIT membantu organisasi mempersiapkan diri untuk audit dan memenuhi persyaratan kepatuhan, seperti GDPR, HIPAA, dan lainnya. Ini adalah aspek penting dalam menjaga kepercayaan pelanggan dan kepatuhan hukum.

h. Meningkatkan Efisiensi dan Efektivitas Operasional: Dengan menerapkan COBIT, organisasi dapat meningkatkan efisiensi operasional mereka dalam pengelolaan TI, mengurangi biaya, dan meningkatkan kualitas layanan TI.

COBIT adalah alat yang sangat berharga bagi organisasi untuk mengelola dan mengendalikan TI mereka secara efektif, memastikan bahwa TI mendukung tujuan bisnis, dan mengidentifikasi serta mengelola risiko dengan lebih baik dalam lingkungan yang selalu berubah.

3. Standar AICPA

AICPA (*American Institute of Certified Public Accountants*) mengeluarkan standar dan pedoman terkait pengauditan teknologi informasi, termasuk *Statement on Auditing Standards* (SAS) No. 94 yang berkaitan dengan pengauditan teknologi informasi. (www.aicpa-cima.com).(www.aicpa-cima.com).

4. Standar ISO/IEC 27001

Standar ini fokus pada pengendalian keamanan informasi dan dapat digunakan sebagai referensi dalam pengauditan teknologi informasi terutama dalam konteks keamanan data.

ISO/IEC 27001:2013 adalah standar internasional yang berfokus pada manajemen keamanan informasi. Berikut adalah penjelasan singkat mengenai peranannya(Wibowo & Sc, 2005):

a. Menetapkan Kerangka Kerja Manajemen Keamanan Informasi: ISO/IEC 27001:2013 memberikan kerangka kerja yang jelas untuk mengelola keamanan informasi dalam sebuah organisasi. Ini mencakup pemahaman risiko, perencanaan, implementasi kontrol keamanan, serta pemantauan dan perbaikan berkelanjutan.
b. Identifikasi dan Pengelolaan Risiko: Standar ini membantu organisasi mengidentifikasi dan mengevaluasi risiko keamanan informasi yang mungkin mereka hadapi. Dengan pemahaman yang lebih baik tentang risiko-risiko ini, organisasi dapat mengambil tindakan untuk mengurangi atau mengelolanya dengan lebih efektif.

c. Menjamin Kepatuhan Hukum dan Peraturan: ISO/IEC 27001:2013 membantu organisasi untuk mematuhi hukum dan peraturan yang berkaitan dengan keamanan informasi. Ini sangat penting dalam menghindari sanksi hukum dan menjaga reputasi organisasi.
d. Meningkatkan Kesadaran Keamanan: Standar ini mendorong organisasi untuk meningkatkan kesadaran keamanan informasi di seluruh organisasi. Ini mencakup pelatihan karyawan, komunikasi kebijakan keamanan, dan pengawasan yang lebih baik.
e. Meningkatkan Kepercayaan Pelanggan dan Mitra Bisnis: Dengan sertifikasi ISO/IEC 27001:2013, organisasi dapat membuktikan kepada pelanggan dan mitra bisnis bahwa mereka telah mengadopsi praktik terbaik dalam mengelola keamanan informasi. Ini dapat meningkatkan kepercayaan dan memungkinkan pertumbuhan bisnis.
f. Pemantauan dan Perbaikan Berkelanjutan: Standar ini mendorong siklus pemantauan dan perbaikan berkelanjutan. Organisasi diharapkan untuk terus memeriksa dan meningkatkan sistem manajemen keamanan informasi mereka untuk menjaga efektivitasnya.

Dengan menerapkan ISO/IEC 27001:2013, organisasi dapat meningkatkan tingkat keamanan informasi mereka, mengurangi risiko, dan memberikan bukti konkret tentang kewajiban mereka terhadap keamanan informasi kepada berbagai pihak yang terkait.

Standar ISO/IEC 27001 dapat diakses melalui situs web resmi *International Organization for Standardization* (ISO) atau *International Electrotechnical Commission* (IEC) (www.iso.org).

5. Standar NIST

NIST Special Publication 800-34, "*Contingency Planning Guide for Federal Information Systems,"* adalah panduan yang diterbitkan oleh National Institute of Standards and Technology (NIST) di Amerika Serikat. Dokumen ini dirancang untuk

membantu lembaga pemerintah federal dan organisasi lainnya dalam merencanakan dan mengimplementasikan langkah-langkah darurat untuk melindungi sistem informasi mereka. Panduan ini mencakup pengidentifikasian risiko, perencanaan respons darurat, pemulihan, dan pengujian untuk memastikan bahwa sistem informasi tetap beroperasi jika terjadi gangguan atau bencana(Marwan, 2018).

6. Standar IIA

IIA (*Institute of Internal Auditors*) memiliki standar audit internal yang dapat digunakan dalam pengauditan teknologi informasi dari perspektif audit internal. Standar IIA dapat ditemukan di situs web resmi Institute of Internal Auditors (IIA) (www.theiia.org).

7.2.6 Kasus Audit Teknologi Informasi Akuntansi dan Bisnis di Indonesia

Tim Riset CNBC Indonesia mencoba merangkum beberapa kasus terkait dugaan dan manipulasi lapkeu emiten di pasar modal RI, termasuk emiten obligasi(Sandria, 2021).

1. PT Kereta Api Indonesia (Persero)

Pada tahun 2006, KAI (Kereta Api Indonesia) mengalami masalah dalam laporan keuangannya. Laporan keuangan tahun sebelumnya menunjukkan laba sebesar Rp 6,9 miliar, padahal seharusnya perusahaan mengalami kerugian sekitar Rp 63 miliar. Salah satu komisaris KAI, Hekinus Manao, menolak menandatangani laporan keuangan tersebut, yang mengakibatkan penundaan RUPST KAI. Ketiga kesalahan dalam laporan keuangan KAI adalah:

a. Kewajiban perusahaan untuk membayar pajak pertambahan nilai (PPN) sebesar Rp 95,2 miliar disajikan dalam laporan keuangan sebagai piutang kepada pelanggan yang seharusnya membayar beban pajak tersebut.
b. Penurunan nilai persediaan suku cadang dan perlengkapan sekitar Rp 24 miliar yang diakui sebagai kerugian oleh manajemen KAI, namun diamortisasi

selama 5 tahun, sehingga saldo penurunan nilai yang belum dibebankan sekitar Rp 6 miliar.

c. Bantuan dari pemerintah senilai Rp 674,5 miliar dan penyertaan modal negara Rp 70 miliar yang disajikan dalam neraca sebagai bagian dari utang, padahal statusnya belum ditentukan.

2. PT Kimia Farma Tbk (KAEF)

Pada tahun 2001, Kimia Farma melakukan penawaran saham perdana untuk publik (IPO) dan melaporkan laba bersih sebesar Rp 132 miliar dalam laporan keuangannya yang diaudit oleh Hans Tuanakotta & Mustofa (HTM). Namun, Kementerian BUMN dan Bapepam (kini OJK) menganggap laba tersebut terlalu besar dan dicurigai mengandung rekayasa. Pada tanggal 3 Oktober 2002, dilakukan audit ulang terhadap laporan keuangan Kimia Farma tahun 2001, dan hasilnya laporan keuangan tersebut disajikan kembali (restated). Ternyata, laba perusahaan sebenarnya hanya sekitar Rp 99,56 miliar, yang lebih rendah sebesar Rp 32,6 miliar atau turun sekitar 24,7% dari laba awal yang dilaporkan. Kesalahan terjadi dalam beberapa unit bisnis Kimia Farma, termasuk overstated penjualan, persediaan barang yang terlalu tinggi, dan kesalahan dalam laporan penjualan dan persediaan.

3. PT Garuda Indonesia (Persero) Tbk (GIAA)

Polemik laporan keuangan Garuda Indonesia dimulai pada Rapat Umum Pemegang Saham (RUPS) pada 24 April 2019, di mana salah satu agendanya adalah pengesahan laporan keuangan tahun 2018. Dalam RUPS tersebut, dua komisaris menolak menandatangani laporan keuangan tersebut. Terungkap bahwa laporan keuangan 2018 mencatat laba bersih yang didorong oleh kerja sama dengan PT Mahata Aero Terknologi senilai US$ 239,94 juta atau sekitar Rp 3,48 triliun. Dana ini seharusnya masih dalam bentuk piutang dengan kontrak 15 tahun ke depan, tetapi sudah dicatatkan sebagai pendapatan dalam tahun pertama dan diakui sebagai pendapatan lain-lain. Hal ini mengubah perusahaan yang sebelumnya mengalami kerugian menjadi mencetak laba. Dua komisaris Garuda Indonesia, yakni Chairal Tanjung dan Dony

Oskaria, menolak menandatangani laporan keuangan 2018 karena permasalahan ini. Audit dilakukan oleh Pusat Pembinaan Profesi Keuangan (PPPK) Kementerian Keuangan, Bursa Efek Indonesia (BEI), Otoritas Jasa Keuangan (OJK), dan BPK. PPPK dan OJK menyimpulkan bahwa ada kesalahan dalam penyajian laporan keuangan 2018, dan perusahaan diminta untuk menyajikan ulang laporan keuangannya. Perusahaan, direksi, dan komisaris yang menandatangani laporan keuangan tersebut dikenai denda Rp 100 juta. Setelah penyesuaian pencatatan, Garuda Indonesia mencatatkan kerugian sebesar US$ 175 juta atau sekitar Rp 2,53 triliun, berbeda dengan laporan keuangan awal yang mencatatkan keuntungan sebesar US$ 5 juta atau sekitar Rp 72,5 miliar pada tahun 2018..

4. PT Asuransi Jiwasraya (Persero)

Kasus megakorupsi Jiwasraya dimulai dari manipulasi laporan keuangan yang terjadi lebih dari satu dekade lalu, pada tahun 2006, di mana laporan keuangan menunjukkan ekuitas Jiwasraya negatif sebesar Rp 3,29 triliun karena aset yang lebih kecil daripada kewajiban. BPK memberikan opini disclaimer untuk laporan keuangan tahun 2006 dan 2007 karena ketidakpastian informasi cadangan. Pada tahun 2015, OJK melakukan pemeriksaan terhadap JS, yang merupakan mantan Direktur Keuangan Jiwasraya, dengan fokus pada investasi dan pertanggungan. Hasil audit BPK pada tahun 2015 mencurigai penyalahgunaan wewenang oleh JS dan juga adanya penyajian informasi aset investasi keuangan yang terlalu tinggi dan kewajiban yang terlalu rendah. Pada Mei 2018, terjadi pergantian direksi di Jiwasraya, dan direksi yang baru melaporkan adanya kejanggalan dalam laporan keuangan kepada Kementerian BUMN. Sebagai respons, KAP yang melakukan audit atas laporan keuangan Jiwasraya tahun 2017 menemukan kesalahan, termasuk koreksi laporan keuangan interim yang awalnya mencatatkan laba sebesar Rp 2,4 triliun menjadi Rp 428 miliar.

5. PT Indofarma Tbk (INAF)

Pada tahun 2004, Bapepam (sekarang OJK) memberikan sanksi administratif berupa denda sebesar Rp 500 juta kepada

direksi Indofarma yang menjabat saat laporan keuangan tahun 2001 diterbitkan. Kasus ini bermula dari penelaahan oleh Bapepam terkait dugaan pelanggaran aturan pasar modal, terutama terkait penyajian laporan keuangan oleh Indofarma. Hasil penelitian menemukan bahwa ada ketidaksesuaian dalam penyajian nilai persediaan barang dalam proses pada tahun 2001, yang mengakibatkan kesalahan dalam perhitungan harga pokok penjualan dan laba bersih dengan nilai yang sama sebesar Rp 28,87 miliar.

6. PT Hanson International Tbk (MYRX)

OJK memberikan sanksi kepada Benny Tjokrosaputro alias Bentjok, Direktur Utama Hanson International, dengan denda sebesar Rp 5 miliar karena melanggar undang-undang pasar modal. Pelanggaran tersebut terkait pengakuan pendapatan yang tidak tepat dan ketidakpenyajian perjanjian jual beli dalam laporan keuangan MYRX tahun 2016. Salah satu poin yang mencolok adalah pengakuan pendapatan sebesar Rp 732 miliar dari penjualan kavling siap bangun (KASIBA) dengan metode akrual penuh dalam laporan keuangan, yang menyebabkan laporan keuangan Desember 2016 menjadi terlalu tinggi sebesar Rp 613 miliar.

7. PT Envy Technologies Indonesia Tbk (ENVY)

Bursa Efek Indonesia (BEI) menghadapi situasi yang mengejutkan terkait dugaan manipulasi laporan keuangan tahunan (LKT) tahun 2019 yang melibatkan salah satu emiten di bidang jasa dan perdagangan teknologi informasi, yaitu PT Envy Technologies Indonesia Tbk (ENVY) dan anak usahanya. Dalam sebuah surat keterangan yang diterbitkan dalam keterbukaan informasi, ENVY menjelaskan permasalahan terkait dugaan manipulasi dalam laporan keuangan anak usahanya, PT Ritel Global Solusi (RGS) untuk tahun 2019. Laporan keuangan RGS tersebut kemudian digabungkan ke dalam laporan keuangan tahunan ENVY untuk tahun 2019. RGS adalah anak perusahaan ENVY dengan kepemilikan saham sebanyak 70% yang bergerak dalam bidang jasa perdagangan secara online melalui aplikasi "KO-IN." ENVY juga mengklarifikasi bahwa pihak manajemen saat ini tidak memiliki

pemahaman yang jelas tentang proses yang terjadi pada saat pembuatan laporan konsolidasi tersebut. Oleh karena itu, mereka sedang berupaya untuk meminta klarifikasi dari pihak auditor, termasuk laporan keuangan RGS. Perseroan berencana untuk menyelesaikan masalah ini dengan berkolaborasi bersama KAP Kosasih, Nurdiyaman, Mulyadi, Tjahjo & Rekan, yang merupakan firma akuntan publik yang bertugas pada saat itu. Seiring dengan hal tersebut, sebelumnya juga pernah terjadi pelanggaran laporan keuangan di sektor perbankan pada tahun 2018, yang menimpa PT Bank KB Bukopin Tbk (BBK) ketika masih dikenal sebagai Bank Bukopin, sebelum masuknya investor dari Korea Selatan, KB Kookmin.

7.3 Pentingnya Pengauditan Teknologi Informasi dalam Dunia Bisnis.

Masa Era digitalisasi, Pengauditan Teknologi Informasi (TI) memegang peran yang sangat penting dalam dunia bisnis saat ini, di mana informasi dan digitalisasi telah menjadi tulang punggung operasional dunia bisnis. Berikut adalah beberapa alasan mengapa pengauditan TI sangat penting:

1. **Mencegah Kecurangan dan Kehilangan Data**
   Dengan mengidentifikasi kelemahan di sistem, pengauditan TI membantu dalam mencegah potensi kecurangan dan kehilangan data yang bisa berdampak sangat besar, termasuk kerugian finansial dan reputasi.
2. **Memastikan Kepatuhan terhadap Regulasi**
   Banyak industri memiliki serangkaian regulasi ketat yang harus diikuti. Pengauditan TI memastikan bahwa perusahaan mematuhi semua persyaratan hukum dan regulasi, sehingga menghindari denda dan sanksi.
3. **Efisiensi Operasional**
   Dengan mengoptimalkan sistem dan proses, pengauditan TI dapat meningkatkan efisiensi operasional perusahaan, yang pada gilirannya dapat mengarah pada penghematan biaya dan profitabilitas yang lebih baik.

4. **Keamanan Informasi**
   Keamanan informasi adalah aspek vital dari setiap bisnis. Pengauditan TI membantu dalam mengidentifikasi dan memperkuat area-area yang rentan terhadap serangan siber, melindungi data sensitif dari akses yang tidak sah.
5. **Kontinuitas Bisnis**
   Pengauditan TI membantu memastikan bahwa strategi pemulihan bencana yang memadai di tempat, memungkinkan kontinuitas bisnis di hadapan kegagalan sistem atau bencana lainnya.
6. **Meningkatkan Kepercayaan Stakeholder**
   Pelaporan dan transparansi yang ditingkatkan melalui pengauditan TI dapat membangun kepercayaan yang lebih besar di antara pemegang saham, investor, dan pelanggan, yang pada gilirannya dapat memiliki dampak positif terhadap reputasi perusahaan.
7. **Membantu dalam Pengambilan Keputusan**
   Dengan memberikan gambaran yang jelas tentang kesehatan sistem TI, pengauditan membantu manajemen dalam pengambilan keputusan yang lebih baik, berdasarkan pada informasi yang akurat dan terkini.
8. **Mendorong Inovasi**
   Melalui pengauditan TI, perusahaan dapat mengidentifikasi area di mana teknologi baru dapat diadopsi untuk memberikan keunggulan kompetitif, mendorong inovasi dan pertumbuhan bisnis.
9. **Evaluasi ROI TI**
   Pengauditan TI juga memungkinkan perusahaan untuk mengukur ROI (Return on Investment) dari investasi TI mereka, memastikan bahwa mereka mendapatkan nilai maksimal dari investasi ini.
10. **Penilaian Resiko**
    Pengauditan TI membantu dalam identifikasi dan penilaian risiko yang terkait dengan teknologi informasi dan membantu dalam merumuskan strategi untuk mitigasi risiko ini.

Dengan mempertimbangkan aspek-aspek penting ini, jelas bahwa pengauditan TI adalah elemen kunci dalam menjaga kestabilan, keamanan, dan kinerja bisnis di era digital saat ini.

7.4 Identifikasi Risiko Teknologi Informasi

Mengidentifikasi risiko-risiko teknologi informasi dalam audit melibatkan pemahaman mendalam tentang bagaimana teknologi informasi berinteraksi dengan operasi bisnis suatu organisasi. Mengidentifikasi Risiko-risiko Teknologi Informasi dalam Audit:

7.4.1 Risiko Keamanan Data: Identifikasi potensi pelanggaran keamanan data seperti peretasan, pencurian data, atau akses tidak sah.

Untuk mengidentifikasi dan mengatasi masalah pengendalian TI dan risiko terkait. Ini membantu dalam mengoptimalkan operasi TI dan memastikan kepatuhan terhadap kebijakan dan regulasi yang relevan. Risiko Ketersediaan Sistem: Evaluasi risiko kegagalan sistem atau infrastruktur teknologi yang dapat mengganggu operasi bisnis.(Marwan, 2018)

Risiko ketersediaan sistem adalah potensi kegagalan atau *downtime* dari sistem atau infrastruktur teknologi yang esensial untuk operasi bisnis. Risiko ini bisa disebabkan oleh berbagai hal, seperti serangan DDoS, kegagalan perangkat keras, atau *error* manusia. Dampaknya bisa meliputi hilangnya pendapatan, kerusakan reputasi, dan potensi hukuman hukum(Marwan, 2018).

7.4.2 Risiko Kesalahan Manusia: Identifikasi risiko kesalahan yang mungkin terjadi karena tindakan manusia seperti penggunaan yang tidak benar atau kelalaian.

Risiko Kesalahan Manusia mengacu pada potensi *error* atau kelalaian yang bisa terjadi akibat tindakan manusia. Ini bisa termasuk input data yang salah, penghapusan file penting, atau konfigurasi yang tidak tepat. Penyebabnya bisa bervariasi, mulai dari kurangnya pelatihan, kelelahan, hingga kelalaian dalam mematuhi prosedur. Risiko Kesalahan Manusia adalah potensi kesalahan atau kelalaian yang disebabkan oleh tindakan manusia

dalam sistem informasi. Ini relevan dalam konteks NIST Special Publication 800-53, yang merupakan panduan untuk kontrol keamanan dan privasi informasi untuk organisasi federal di AS. Dokumen ini menekankan pentingnya melatih staf, menerapkan prosedur yang tepat, dan menggunakan teknologi untuk mengurangi risiko kesalahan manusia yang bisa merusak keamanan dan privasi data. Dampaknya bisa meliputi kegagalan sistem, kebocoran data, atau gangguan operasional. Untuk mengurangi risiko ini, pelatihan dan prosedur yang jelas sangat penting. Relevansinya terletak pada bagaimana NIST Special Publication 800-53 merekomendasikan kontrol dan prosedur yang bisa mengurangi atau mitigasi risiko kesalahan manusia. Dokumen ini mencakup pedoman untuk pelatihan keamanan, autentikasi, akses terkontrol, dan kebijakan lain yang dirancang untuk meminimalkan potensi kesalahan atau kelalaian oleh staf. Ini membantu organisasi dalam mengidentifikasi dan mengelola risiko yang terkait dengan tindakan manusia(FORCE, 2013).

NIST Special Publication 800-53 dan ISO/IEC 27002:2013 keduanya adalah standar untuk kontrol keamanan informasi, tetapi mereka berasal dari lembaga yang berbeda dan digunakan untuk tujuan yang berbeda. Keduanya menawarkan pedoman untuk mengelola risiko keamanan, termasuk risiko kesalahan manusia. ISO/IEC 27002:2013 fokus pada prinsip-prinsip keamanan informasi yang lebih umum dan dapat diaplikasikan secara global, tidak terbatas pada organisasi pemerintah. Pedoman ini mencakup aspek seperti manajemen akses, penggunaan kriptografi, dan pelatihan keamanan, yang semuanya bisa membantu dalam mengurangi risiko kesalahan manusia(ISO/IEC, 2013). Sedangkan NIST 800-53 lebih spesifik kepada kebutuhan pemerintah federal AS tetapi juga secara luas digunakan di luar itu, seperti di Indonesia. Dokumen ini juga mencakup kontrol untuk mitigasi risiko kesalahan manusia. Keduanya dapat digunakan bersamaan atau secara terpisah untuk membangun kerangka kerja keamanan informasi yang kokoh. Dalam konteks risiko kesalahan manusia, keduanya menekankan pentingnya pelatihan, prosedur, dan kontrol teknis untuk memitigasi risiko. SO/IEC TR 27008 berfokus pada "Human Factors in Information Security Management Systems" dan

memberikan pandangan mendalam tentang bagaimana faktor manusia mempengaruhi keamanan informasi. Dokumen ini mengakui bahwa teknologi saja tidak cukup untuk mengamankan sistem; orang-orang yang mengoperasikannya juga memainkan peran kritis.

NIST Special Publication 800-53, ISO/IEC 27002:2013, dan ISO/IEC TR 27008 semuanya mencakup aspek risiko kesalahan manusia dalam keamanan informasi. Sementara NIST dan ISO/IEC 27002 lebih fokus pada kontrol dan prosedur, ISO/IEC TR 27008 menyoroti bagaimana perilaku manusia dan faktor-faktor humanis lainnya dapat menjadi titik kelemahan dalam sistem keamanan. Jika Anda menggunakan NIST atau ISO/IEC 27002 sebagai kerangka kerja keamanan Anda, memperhatikan ISO/IEC TR 27008 dapat membantu Anda memahami dan mengatasi aspek-aspek humanis yang mungkin tidak sepenuhnya dijelaskan dalam dua standar lain tersebut. Ini akan memberikan pendekatan yang lebih holistik terhadap keamanan informasi, memperhitungkan tidak hanya teknologi tetapi juga elemen manusia. (www.iso.org, n.d.)

7.4.3 Risiko Perangkat Lunak dan Aplikasi: Penilaian risiko terkait dengan kerentanan perangkat lunak dan aplikasi terhadap ancaman siber seperti malware atau perangkat lunak berbahaya.

Risiko Perangkat Lunak dan Aplikasi mengacu pada potensi kerentanan dalam perangkat lunak atau aplikasi yang bisa dieksploitasi oleh ancaman siber seperti malware atau perangkat lunak berbahaya. Penyebabnya bisa termasuk kelemahan dalam desain perangkat lunak, kurangnya pembaruan keamanan, atau instalasi perangkat lunak dari sumber yang tidak terpercaya. Dampaknya bisa meliputi kebocoran data, kehilangan integritas data, atau downtime sistem. Untuk mitigasi, pembaruan dan patch keamanan perlu diterapkan secara rutin.

Risiko Perangkat Lunak dan Aplikasi berkaitan erat dengan NIST Special Publication 800-40 pada teknologi manajemen patch di perusahaan. Risiko ini mencakup kerentanan dalam perangkat lunak atau aplikasi yang bisa dieksploitasi untuk melakukan serangan siber. NIST 800-40 memberikan panduan tentang

bagaimana mengidentifikasi, memprioritaskan, dan menerapkan patch keamanan untuk mitigasi risiko ini. Dalam konteks ini, mengikuti rekomendasi dari NIST 800-40 akan membantu organisasi meminimalkan risiko yang dihadapi, termasuk kebocoran data, kehilangan integritas data, atau downtime sistem. Panduan ini menekankan pentingnya proses yang terstruktur dan otomatisasi dalam manajemen patch untuk menjaga keamanan sistem yang optimal(Souppaya & Scarfone, 2022).

Risiko Perangkat Lunak dan Aplikasi, terutama yang berhubungan dengan aplikasi web, sangat relevan dengan OWASP Top 10. Daftar OWASP memuat sepuluh risiko keamanan aplikasi web paling kritis yang sering dihadapi organisasi, seperti injeksi SQL, kelemahan autentikasi, dan eksposur data sensitif. NIST Special Publication 800-40, yang fokus pada manajemen patch, dapat dianggap sebagai salah satu alat untuk mitigasi beberapa risiko yang disebutkan dalam OWASP Top 10(Owasp.org, 2017). Banyak dari risiko ini timbul dari kelemahan dalam desain perangkat lunak atau kurangnya pembaruan keamanan, masalah yang bisa diatasi dengan penerapan patch keamanan yang tepat. Jadi, memahami OWASP Top 10 akan membantu organisasi mengidentifikasi area yang paling rentan dalam aplikasi web mereka, sementara panduan dari NIST 800-40 bisa membantu dalam mengatasi masalah-masalah tersebut melalui manajemen patch yang efektif. Keduanya bekerja bersama untuk memberikan pendekatan yang lebih komprehensif terhadap keamanan perangkat lunak dan aplikasi.

Risiko Perangkat Lunak dan Aplikasi sangat relevan dengan ISO/IEC 27001:2013, yang merupakan standar internasional untuk sistem manajemen keamanan informasi (ISMS). Standar ini memberikan kerangka kerja untuk manajemen risiko keamanan informasi, yang mencakup identifikasi, penilaian, dan mitigasi risiko, termasuk risiko pada perangkat lunak dan aplikasi. ISO/IEC 27001 menekankan pentingnya pembaruan keamanan dan prosedur kontrol keamanan lainnya yang dapat membantu mengurangi risiko terkait perangkat lunak dan aplikasi. Ini sejalan dengan rekomendasi dari NIST 800-40, yang menyarankan penerapan patch keamanan secara rutin sebagai salah satu langkah mitigasi. Dengan memadukan panduan dari ISO/IEC 27001 dan NIST 800-40,

sebuah organisasi dapat membangun sistem keamanan informasi yang lebih kuat dan tahan terhadap berbagai jenis risiko, termasuk kerentanan pada perangkat lunak dan aplikasi(Bernardino, 2021; Sanchez & Enrique, 2017).

7.4.4 Risiko Manajemen Identitas: Evaluasi risiko yang terkait dengan manajemen identitas dan akses yang tidak tepat.

Risiko Manajemen Identitas berkaitan dengan potensi bahaya yang muncul dari pengelolaan identitas dan akses yang tidak tepat atau lemah dalam sebuah sistem. Penyebabnya bisa termasuk kebijakan kata sandi yang lemah, penggunaan hak akses yang berlebihan, atau kurangnya autentikasi dua faktor. Dampaknya bisa meliputi kebocoran data, akses yang tidak sah ke informasi sensitif, dan potensi penyalahgunaan sistem. Untuk mengatasi ini, kebijakan akses yang kuat dan pelatihan keamanan adalah penting.(ISACA Governance and Manajement, 2019) .

Risiko Manajemen Identitas berkaitan dengan bagaimana identitas digital dan hak akses dikelola dalam sebuah sistem. NIST Special Publication 800-63, "*Digital Identity Guidelines*," memberikan panduan komprehensif mengenai autentikasi dan manajemen siklus hidup identitas. Ini mencakup rekomendasi untuk autentikasi kuat, termasuk penggunaan autentikasi dua faktor, serta pedoman untuk kebijakan kata sandi yang aman. Kegagalan dalam manajemen identitas, seperti kebijakan kata sandi yang lemah atau hak akses yang berlebihan, bisa berdampak serius seperti kebocoran data atau akses tidak sah ke informasi sensitif. Oleh karena itu, mengikuti pedoman dari NIST 800-63 dapat membantu organisasi memitigasi risiko ini. NIST 800-63 dan isu-isu risiko manajemen identitas saling terkait dan komplementer. Implementasi pedoman NIST untuk manajemen identitas akan membantu sebuah organisasi mengidentifikasi dan mengurangi potensi risiko yang terkait dengan autentikasi dan akses. NIST Special Publication 800-63, "*Digital Identity Guidelines*," memberikan panduan detil tentang bagaimana mendesain dan menerapkan solusi identitas digital yang aman. Ini termasuk rekomendasi untuk autentikasi kuat, termasuk penggunaan autentikasi multi-faktor, dan kebijakan kata sandi yang aman.

Ketika membahas Risiko Manajemen Identitas—seperti kelemahan dalam kebijakan kata sandi, hak akses yang berlebihan, atau kurangnya autentikasi dua faktor—pedoman dari NIST 800-63 dapat dijadikan sebagai sumber rujukan untuk mitigasi risiko ini. Implementasi rekomendasi dari NIST 800-63 akan memperkuat manajemen identitas dan akses dalam organisasi, sehingga mengurangi potensi kebocoran data, akses tidak sah, dan penyalahgunaan sistem. Jadi, NIST 800-63 dan risiko manajemen identitas saling berkaitan: satu memberikan panduan untuk mengatasi dan memitigasi risiko yang diidentifikasi oleh yang lain(Grassi et al., 2020).

ISO/IEC 27002:2013 memberikan panduan umum tentang kontrol keamanan informasi, termasuk manajemen identitas dan akses. Ini mencakup rekomendasi untuk kebijakan akses, otentikasi, otorisasi, dan pengelolaan hak akses, antara lain. Ketika membahas Risiko Manajemen Identitas—seperti kebijakan kata sandi yang lemah atau hak akses yang berlebihan—ISO/IEC 27002:2013(Sanchez & Enrique, 2017) dapat digunakan sebagai kerangka kerja untuk membantu mengidentifikasi dan menerapkan kontrol keamanan yang tepat. Ini akan membantu dalam mitigasi risiko seperti kebocoran data atau akses tidak sah. Keduanya, ISO/IEC 27002 dan NIST 800-63, saling melengkapi. Sementara NIST 800-63 lebih fokus pada pedoman teknis untuk autentikasi dan manajemen identitas digital, ISO/IEC 27002 memberikan panduan yang lebih luas mengenai kontrol keamanan informasi, termasuk manajemen identitas. Menerapkan kedua set pedoman ini akan memberikan pendekatan yang lebih komprehensif untuk mengatasi Risiko Manajemen Identitas.

ISACA's COBIT (Control Objectives for Information and Related Technologies) adalah kerangka kerja untuk tata kelola dan manajemen TI yang mencakup berbagai aspek, termasuk keamanan informasi dan manajemen risiko. COBIT membantu organisasi memastikan bahwa teknologi informasi dan proses bisnisnya sejalan dengan tujuan strategisnya. Dalam konteks Risiko Manajemen Identitas, COBIT bisa digunakan untuk membangun dan mempertahankan sebuah kerangka kerja manajemen identitas dan akses yang kuat. COBIT memberikan kontrol dan metrik yang bisa

membantu organisasi mengidentifikasi dan mengelola risiko, termasuk risiko yang berkaitan dengan autentikasi, otorisasi, dan administrasi akses(ISACA Governance and Manajement, 2019). Jika NIST 800-63 memberikan panduan teknis tentang bagaimana mengimplementasikan mekanisme identitas digital yang aman, dan ISO/IEC 27002 menawarkan panduan umum mengenai kontrol keamanan informasi, COBIT menyediakan panduan tata kelola yang membantu memastikan bahwa kontrol tersebut dikelola dan diterapkan secara efektif dalam konteks bisnis. Oleh karena itu, menggunakan COBIT bersama-sama dengan NIST 800-63 atau ISO/IEC 27002 bisa memberikan pendekatan yang lebih holistik dan terstruktur dalam mengelola Risiko Manajemen Identitas.

7.4.5 Risiko Kepatuhan Regulasi: Menilai risiko ketidakpatuhan terhadap regulasi seperti GDPR, HIPAA, atau peraturan sektor tertentu.

Risiko Kepatuhan Regulasi mengacu pada potensi konsekuensi dari tidak mematuhi hukum dan regulasi yang relevan, seperti GDPR di Uni Eropa atau HIPAA di Amerika Serikat. Penyebabnya bisa termasuk kurangnya pemahaman tentang regulasi, kegagalan dalam pelaksanaan kebijakan, atau keterbatasan sumber daya untuk mematuhi standar. Dampaknya bisa meliputi denda finansial yang signifikan, tindakan hukum, dan kerusakan reputasi. Mengatasi risiko ini memerlukan pemahaman yang mendalam tentang regulasi dan implementasi kebijakan dan prosedur yang sesuai(Regulation, 2018).

Risiko Kepatuhan Regulasi berkaitan erat dengan kebutuhan untuk mematuhi berbagai regulasi dan standar industri, seperti GDPR untuk perlindungan data pribadi atau HIPAA untuk keamanan informasi kesehatan. Tidak mematuhi ini bisa berdampak finansial dan reputasional yang serius. HIPAA, sebagai contoh, memberikan pedoman spesifik tentang bagaimana informasi kesehatan harus dihandle dan disimpan untuk melindungi privasi pasien. Untuk mitigasi Risiko Kepatuhan Regulasi, perlu ada pemahaman mendalam tentang apa yang diminta oleh HIPAA dan implementasi kebijakan serta prosedur yang sesuai.

Kerangka kerja seperti COBIT atau standar ISO/IEC 27001 bisa digunakan untuk membantu memastikan bahwa kontrol keamanan yang tepat diterapkan dan dijaga sesuai dengan regulasi. Penggunaan kerangka kerja ini akan membantu organisasi tidak hanya memenuhi regulasi tapi juga meningkatkan tata kelola dan manajemen risiko secara keseluruhan. Dengan kata lain, untuk mengatasi Risiko Kepatuhan Regulasi, penting untuk memadukan pemahaman regulasi seperti HIPAA dengan implementasi kebijakan dan prosedur yang sesuai, dan ini lebih mudah dicapai dengan menggunakan kerangka kerja keamanan informasi yang telah ada(Caplan, 2003).

ISO/IEC 27001:2013 adalah standar internasional untuk sistem manajemen keamanan informasi (ISMS) yang membantu organisasi mengidentifikasi, mengelola, dan memitigasi berbagai jenis risiko keamanan informasi, termasuk Risiko Kepatuhan Regulasi. Standar ini menawarkan kerangka kerja untuk pengembangan kebijakan, prosedur, dan kontrol yang membantu memastikan kepatuhan terhadap hukum dan regulasi yang berlaku. Dalam konteks Risiko Kepatuhan Regulasi, ISO/IEC 27001 membantu organisasi membangun, memelihara, dan meningkatkan ISMS yang mencakup persyaratan kepatuhan. Misalnya, jika sebuah organisasi perlu mematuhi GDPR atau HIPAA, ISO/IEC 27001 bisa membantu memastikan bahwa kontrol dan proses yang diperlukan telah diterapkan dan dijaga. Penerapan ISO/IEC 27001 akan membantu organisasi secara sistematis mengevaluasi informasi mereka untuk risiko keamanan, termasuk risiko kepatuhan, dan menentukan kontrol yang tepat untuk mitigasi. Ini juga akan membantu dalam mendokumentasikan kepatuhan, yang bisa sangat berguna saat audit atau inspeksi kepatuhan. Oleh karena itu, ISO/IEC 27001 bisa dianggap sebagai alat yang sangat berguna dalam mengidentifikasi dan mengelola Risiko Kepatuhan Regulasi(Wibowo & Sc, 2005).

Dalam konteks GDPR, risiko kepatuhan regulasi berkaitan dengan potensi konsekuensi hukum dan finansial karena tidak mematuhi standar perlindungan data pribadi yang ditetapkan oleh Uni Eropa. Penyebabnya bisa termasuk kegagalan dalam mengidentifikasi data pribadi yang diproses, tidak adanya

mekanisme keamanan yang memadai, atau kurangnya persetujuan yang tepat dari subjek data. Jika sebuah organisasi tidak mematuhi GDPR, konsekuensinya bisa sangat serius, termasuk denda hingga €20 juta atau 4% dari pendapatan tahunan global, tergantung mana yang lebih besar. Selain itu, reputasi perusahaan juga bisa terkena dampak(Regulation, 2018). Hubungan antara GDPR dan *Article 29 Working Party Guidelines on Data Protection Impact Assessment* (DPIA) adalah sebagai berikut: Keduanya bertujuan untuk meningkatkan kepatuhan regulasi perlindungan data. DPIA adalah alat yang direkomendasikan dalam pedoman Article 29 untuk membantu organisasi mengidentifikasi dan mengelola risiko terkait perlindungan data. Dengan melakukan DPIA, organisasi bisa lebih memahami bagaimana data diproses dan bagaimana meminimalisir risiko pelanggaran GDPR. Sehingga, DPIA membantu organisasi dalam mematuhi standar GDPR dan mengurangi risiko denda atau konsekuensi hukum lainnya(Article 29 Working Party, 2017).

7.4.6 Studi Kasus: Analisis Risiko Teknologi Informasi pada Perusahaan Tertentu

Risiko Teknologi Informasi pada sebuah perusahaan dapat gagal beroperasi karena berbagai penyebab. Beberapa penyebab umum termasuk(Bernardino, 2021):

1. **Kegagalan Perangkat Keras atau Perangkat Lunak**: Perangkat keras atau perangkat lunak yang bermasalah atau mengalami kerusakan dapat menyebabkan sistem berhenti beroperasi.
2. **Serangan Siber**: Ancaman siber seperti serangan malware, serangan DDoS, atau peretasan data dapat mengganggu operasi sistem dan infrastruktur TI perusahaan.
3. **Ketidaksesuaian Teknologi**: Penggunaan teknologi yang sudah usang atau tidak sesuai dengan kebutuhan perusahaan dapat mengakibatkan kerentanannya terhadap risiko dan kegagalan operasional.
4. **Kegagalan Proses Bisnis**: Ketidakmampuan untuk mengelola atau mendukung proses bisnis yang kritis dengan tepat dapat menyebabkan kerusakan operasional.

5. **Kesalahan Manusia**: Kesalahan manusia seperti penghapusan data yang salah atau konfigurasi yang tidak benar dapat berdampak negatif pada operasi TI.
6. **Keterbatasan Sumber Daya**: Kurangnya sumber daya, baik dalam hal personil maupun anggaran, dapat menghambat kemampuan perusahaan untuk menjaga dan memulihkan sistem TI.
7. **Kegagalan Rencana Bencana**: Jika perusahaan tidak memiliki rencana bencana yang efektif, risiko operasional saat terjadi gangguan atau bencana dapat meningkat(Swanson et al., 2010).

Risiko 1: Keamanan Data

Kasus 1: Data pelanggan IndiHome

Pada bulan Agustus, sekitar 26 juta data yang diduga milik pelanggan IndiHome ditemukan telah bocor dan dijual di forum BreachForums oleh pengguna dengan nama Bjorka. Data-data yang bocor ini mencakup berbagai informasi, seperti riwayat pencarian, kata kunci yang dicari, informasi pengguna seperti alamat email, nama, jenis kelamin, dan bahkan Nomor Induk Kependudukan (NIK). Dalam konteks ini, "riwayat pencarian" mengacu pada data yang mencatat aktivitas pencarian yang dilakukan oleh pelanggan IndiHome, yang dapat mencakup apa yang mereka cari secara online atau di platform yang digunakan. Data ini juga mencakup informasi pengguna seperti nama dan alamat email, yang dapat digunakan untuk mengidentifikasi pelanggan secara pribadi. Selain itu, NIK (Nomor Induk Kependudukan) juga merupakan informasi yang sangat sensitif karena dapat digunakan untuk tujuan identifikasi resmi di banyak negara. Fakta bahwa data ini ditemukan di forum BreachForums dan dijual oleh Bjorka menunjukkan bahwa data tersebut telah disusupi oleh pihak yang tidak berwenang, dan mungkin ada risiko pencurian identitas atau penyalahgunaan informasi pribadi pelanggan IndiHome yang terkena dampaknya. Keamanan data pelanggan harus dijaga dengan sangat serius untuk mencegah kerentanannya terhadap serangan siber dan pelanggaran data semacam ini.

Kasus 2: Data pelanggan PLN

Pada bulan Agustus, sekitar 17 juta data yang diduga milik pelanggan PLN (Perusahaan Listrik Negara) diketahui telah bocor dan muncul di sebuah forum yang sering digunakan oleh para peretas. Informasi tentang penjualan data yang bocor ini diunggah oleh seorang pengguna akun dengan nama @loliyta. Artinya, sejumlah besar informasi pribadi dan data pelanggan PLN, seperti nama, alamat, nomor kontak, dan mungkin informasi akun atau tagihan, telah menjadi tersedia secara tidak sah di ruang publik melalui forum yang digunakan oleh para peretas. Ini adalah masalah serius karena informasi pribadi pelanggan yang terekspos dapat disalahgunakan untuk tujuan jahat, termasuk pencurian identitas atau penipuan. Dalam hal ini, @loliyta adalah pengguna forum yang membagikan atau menjual informasi tersebut kepada pihak lain, yang dapat menyebabkan risiko keamanan yang signifikan bagi pelanggan PLN yang data mereka telah terdampak.

Kasus 3 :Data internal Jasa Marga

Jasa Marga menjadi target serangan oleh sekelompok peretas yang mengklaim diri sebagai Desorden Group pada bulan Agustus. Dalam serangan ini, peretas berhasil mengakses dan mengungkapkan data dengan kapasitas sekitar 252 GB yang terdapat pada lima server milik instansi tersebut. Data yang dibocorkan mencakup berbagai jenis informasi, termasuk data, kode program (koding), dan dokumen. Serangan semacam ini biasanya dilakukan dengan cara meretas ke dalam sistem komputer atau server instansi tersebut, yang kemungkinan melibatkan eksploitasi celah keamanan yang ada pada sistem tersebut. Setelah berhasil memasuki sistem, peretas dapat mencuri, menyalin, atau mengunduh data yang ada pada server tersebut. Data yang dibocorkan ini kemudian dapat digunakan untuk berbagai tujuan jahat, seperti pemerasan, pencurian identitas, atau penyebaran informasi rahasia. Ketika data sebesar 252 GB ini terekspos, hal ini dapat menjadi ancaman serius bagi Jasa Marga karena data tersebut bisa mencakup informasi yang penting dan rahasia terkait dengan operasi dan bisnis mereka. Selain itu, ini juga dapat merusak reputasi dan integritas organisasi jika data tersebut digunakan

dengan cara yang merugikan. Oleh karena itu, serangan siber seperti ini memerlukan tindakan cepat dan serius untuk mengamankan sistem dan melacak para pelaku di balik serangan tersebut.

Kasus 4 : Data SIM card

Sejumlah besar data pendaftaran kartu SIM, sekitar 1,3 miliar data, diduga bocor dan dijual di forum gelap pada bulan September. Bjorka mengklaim bahwa data ini diperoleh dari Kementerian Komunikasi dan Informatika. Informasi yang terekspos mencakup Nomor Induk Kependudukan (NIK), nomor telepon, nama penyedia layanan, dan tanggal pendaftaran, dengan total kapasitas data sekitar 87 GB. Data tersebut dihargai sekitar US$50 ribu (sekitar Rp743,5 juta) oleh Bjorka, dan ia juga menyediakan sampel data sebesar 2GB sebagai bukti. Lembaga riset *Communication & Information System Security Research Center* (CISSReC) yang menganalisis sampel data yang diberikan oleh Bjorka menyatakan bahwa data yang bocor di forum gelap tersebut valid. Kementerian Komunikasi dan Informatika sendiri telah mengharuskan semua pengguna kartu SIM prabayar untuk mendaftarkan nomor telepon mereka sejak Oktober 2017, dengan syarat melampirkan NIK dan nomor Kartu Keluarga (KK).

Kasus 5 : Data MyPertamina

Bjorka telah mengungkapkan bahwa data sebanyak 44 juta pengguna aplikasi MyPertamina telah terekspos dan dijual seharga Rp392 juta dalam bentuk Bitcoin. Informasi ini terdokumentasikan dalam unggahan terbaru di situs BreachForums yang berjudul 'MYPERTAMINA INDONESIA 44 MILLION', yang dipublikasikan pada tanggal Kamis (10/11) pukul 02.31 AM. MyPertamina adalah platform layanan keuangan digital yang dioperasikan oleh Pertamina dan terintegrasi dengan aplikasi LinkAja. Aplikasi ini digunakan untuk melakukan pembayaran BBM secara non-tunai di SPBU Pertamina. Data yang bocor terdiri dari dua jenis file, yaitu yang terkompresi (6GB) dan yang tidak terkompresi (30GB), dengan jumlah total data mencapai 44.237.264. (*10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah*, n.d.)

Risiko 2: Ketersediaan Sistem

Kasus 1 : Gangguan Layanan

Bank Syariah Indonesia (BSI) baru-baru ini, yang diduga kuat akibat serangan siber ransomware, semestinya menjadi pelajaran bagi perbankan di Indonesia. Bank-bank di Indonesia, menurut pengamat keamanan siber, perlu memperkuat sistem pertahanan digital karena serangan siber telah menjadi semakin kompleks dan canggih. Layanan bank syariah terbesar di Indonesia dilaporkan sempat lumpuh selama kurang-lebih lima hari, membuat kesal para nasabahnya. BSI mengatakan seluruh layanan perbankan sudah berangsur normal dan pulih sejak Kamis (11/05).

Kasus 2 : Peretasan dan Data Pribadi Nasabah

Pada 2021, Bank Jatim dan BRI Life – perusahaan asuransi milik BRI – diretas dan data pribadi nasabah diduga bocor di internet. Bahkan awal 2022 silam Bank Indonesia mengaku kena serangan ransomware. Ini adalah jenis serangan siber yang biasa disebut ransomware. Peretas mengenkripsi data-data berharga milik target kemudian meminta sejumlah uang untuk membukanya kembali. Serangan seperti ini biasanya dapat dimitigasi bila pihak yang diretas memiliki cadangan data yang baik, namun beberapa geng hacker seperti LockBit dan Conti mencuri data-data target sebelum mengenkripsi dan meminta uang tebusan(BBC, n.d.).

Analisis Risiko: Risiko tinggi karena kegagalan sistem dapat mengakibatkan hilangnya pendapatan dan kehilangan pelanggan.

Risiko 3: Risiko Kesalahan Manusia

Sebanyak 540 juta data pengguna Facebook bocor ke publik. Indirmasi itu diketahui perusahaan keamanan digital UpGuard. UpGuard menemukan cache data dalam jumlah besar pada server Amazon tanpa jaminan yang digunakan oleh perusahaan media sosial Meksiko. Informasi itu muncul dari pengunjung halaman Facebook, Cultura Colectiva, dan termasuk nama akun, nomor identitas, komentar, dan reaksi. Facebook mengatakan data itu sekarang telah dihapus dari server(DREAM.CO.ID, n.d.).

Analisis Risiko: Risiko sedang, tetapi masih signifikan karena kesalahan manusia dapat menyebabkan kerugian waktu dan upaya dalam pemulihan data.

Risiko 4: Risiko Perangkat Lunak dan Aplikasi

Badan Siber dan Sandi Negara (BSSN) mencatat peningkatan jumlah serangan yang dilakukan oleh peretas, yang sejalan dengan pertambahan pengguna internet selama pandemi COVID-19. Salah satu jenis perangkat lunak berbahaya yang sering digunakan oleh peretas adalah Trojan. Perangkat lunak ini memiliki potensi merusak sistem atau jaringan. Berbeda dengan virus atau worm, Trojan cenderung tidak terlihat dan sering kali disamarkan sebagai program atau berkas yang tampak wajar, seperti berkas .mp3, perangkat lunak gratis, antivirus palsu, atau game gratis. BSSN juga telah memberikan informasi mengenai berbagai jenis serangan siber yang terjadi, termasuk jenis trojan seperti AllAple dan CobaltStrike.

Berikut 10 serangan dahsyat siber ke Indonesia:

Kasus 1 : AllAple

Win.Trojan.Allaple adalah jenis trojan yang memungkinkan penyerang untuk mengunduh dan menjalankan berkas sewenang-wenang, termasuk malware tambahan. Malware ini secara eksklusif terkait dengan keluarga malware Net-worm:W32/Allaple. Malware Allaple termasuk dalam kategori polymorphic malware yang didesain untuk menyebar melalui *Local Area Network* (LAN) dan Internet. Penemuan malware Allaple berawal pada akhir tahun 2006. Awalnya, malware ini dikembangkan oleh seorang individu yang tidak puas dengan perusahaan asuransi, dengan tujuan melancarkan serangan *Distributed Denial-of-Service* (DDoS) terhadap beberapa situs web di Estonia. Cara penyebarannya adalah melalui unduhan oleh korban. Setelah terunduh, malware ini akan mendekripsi dirinya sendiri setelah mengalokasikan memori, dan kemudian mengambil alih kendali melalui kode yang telah didekripsi di dalam memori. Setelah proses dekripsi yang melibatkan pemanggilan fungsi melalui antarmuka yang dirancang untuk membingungkan, kode ini akan menginstal dirinya sendiri

sebagai layanan dan mencari berkas dengan ekstensi .htm/.html di seluruh drive logis yang ada di sistem. Selama pencarian berkas tersebut, malware akan menginstal salinan dirinya dengan nama acak di dalam direktori system32.

Kasus 2 : ZeroAccess

Win.Trojan.ZeroAccess adalah jenis Trojan Horse yang menyerang sistem operasi Microsoft Windows. Malware ini digunakan untuk mengunduh malware lain ke komputer yang terinfeksi, yang menjadi bagian dari botnet, dan tetap tersembunyi dengan menggunakan teknik rootkit. Nama "ZeroAccess" berasal dari string yang ditemukan dalam kode driver kernel yang mengacu pada folder proyek awal yang disebut "ZeroAccess." Botnet ZeroAccess pertama kali ditemukan sekitar bulan Mei 2011. Rootkit ZeroAccess, yang bertanggung jawab atas penyebaran botnet ini, diyakini telah menyebar ke setidaknya 9 juta sistem. Perkiraan tentang ukuran botnet berbeda-beda dari satu sumber ke sumber lain. Misalnya, vendor antivirus Sophos memperkirakan ada sekitar 1 juta mesin yang terinfeksi dan aktif pada kuartal ketiga tahun 2012, sedangkan firma keamanan Kindsight memperkirakan ada sekitar 2,2 juta sistem yang terinfeksi dan aktif. ZeroAccess menyebar melalui beberapa cara. Beberapa situs web yang telah disusupi mengarahkan lalu lintas ke situs web berbahaya yang berperan sebagai host Trojan.ZeroAccess dan mendistribusikannya menggunakan alat-alat seperti Blackhole Exploit Toolkit dan Bleeding Life Toolkit. Selain itu, Trojan ini juga dapat memperbarui dirinya sendiri melalui jaringan peer-to-peer, memungkinkan pembuat malware untuk memperbaiki dan bahkan menambahkan fungsionalitas baru ke dalamnya.

Kasus 3 : ScadaMoxa

Sistem kontrol industri, dikenal *Industrial Control System* (ICS), yang mencakup sistem kontrol pengawasan dan akuisisi data atau dikenal *Supervisory controland data acquisition* (SCADA), digunakan di berbagai sektor industri seperti penyedia energi, manufaktur, dan penyedia infrastruktur kritikal untuk mengendalikan dan memantau berbagai aspek dari proses industri.

Sistem ICS menggunakan beragam mekanisme dan protokol yang juga ditemui dalam sistem dan jaringan TI konvensional. Pada awalnya, peretas bisa menginfeksi pabrik karena ada kelemahan dalam prosedur keamanannya yang memberi akses ke beberapa stasiun dan jaringan kontrol keamanan. Peretas kemudian menyebarkan RAT (*Remote Access Trojan*) pada tahap kedua serangan mereka, yang pertama kali menargetkan sistem kontrol industri. Malware ini beroperasi dengan menggunakan *shellcode*.

Kasus 4 : WillExec

Trojan.WillExec pertama kali dibuat pada bulan Juni tahun 2009, tetapi pertama kali ditemukan aktif pada bulan November tahun 2017. Jenis trojan ini berupa file eksekusi yang dapat dijalankan pada sistem operasi Windows 32 bit, atau dikenal juga sebagai Win32 EXE. Beberapa perangkat antivirus mendeteksi malware ini dengan berbagai nama, seperti Win.Trojan.WillExec, Win32:Malware-gen, dan Trojan:Win32/Lethic.Q!bit. Malware ini termasuk dalam kategori trojan yang menyamar dan berusaha membingungkan pengguna dengan menyamarkan dirinya sebagai perangkat lunak yang sah. Penyerang menggunakan trojan ini sebagai pintu belakang untuk mengakses data sensitif milik korban. Cara kerja dari malware ini adalah dengan menyuntikkan dirinya ke dalam proses yang ada pada sistem dan menonaktifkan fitur keamanan komputer. Setelah berhasil memasuki proses tersebut, Trojan.WillExec akan mencoba untuk terhubung dengan berbagai domain melalui jaringan UDP. Kemudian, ia akan bersembunyi di dalam proses tersebut dan menunggu instruksi dari penyerang untuk dieksekusi. Malware ini menjalankan modul yang disebut advapi32.dll, yang memiliki peran penting dalam memastikan bahwa suatu aplikasi pada perangkat dapat dieksekusi dengan benar saat pengguna menjalankannya.

Kasus 5 : CVE-2017-11882

Kegagalan Microsoft Office dalam mengatasi objek berbahaya dalam memori telah menciptakan celah kerentanan remote code execution. Penyerang yang berhasil memanfaatkan kerentanan ini dapat menjalankan kode sewenang-wenang pada

komputer korban yang terkena eksploitasi. Jika korban memiliki hak akses admin saat masuk, penyerang bahkan bisa mengambil alih kendali sistem korban. Penyerang selanjutnya dapat memasang perangkat lunak, mengakses, mengubah, atau menghapus data, dan bahkan membuat akun baru dengan hak admin tambahan. Kerentanan CVE-2017-11882 ini juga ditemukan sebagai metode untuk menyebarkan malware berbahaya lainnya yang bertujuan mencuri informasi penting dari korban. Salah satu caranya adalah dengan menyisipkan malware ke dalam file yang telah dirancang khusus untuk digunakan bersama dengan versi Microsoft Office. Dalam penilaian CVSS v3.1, kerentanan ini memiliki skor 7.8, yang dapat dikategorikan sebagai tingkat keamanan "TINGGI".

Kasus 6 : Generic Trojan

Generic Trojan adalah jenis virus yang memiliki struktur program atau file yang menyerupai trojan. Seperti trojan, Generic Trojan adalah program yang berpotensi merusak perangkat yang terinfeksi. Trojan ini diidentifikasi dengan label Malware/Win32.Generic.C1960796. Selain itu, trojan ini termasuk dalam kategori file eksekusi (file exe) yang dapat dijalankan. Keberadaan malware ini pertama kali terdeteksi melalui layanan web VirusTotal pada tahun 2014. Generic Trojan dapat menyebar melalui berbagai metode, termasuk melalui email spam, pembaruan palsu, atau bahkan saat mengklik video di situs web yang mencurigakan. Jika pengguna mengklik tautan yang mengarah ke halaman tersebut, yang diunduh bukanlah video tetapi berkas executable (.exe).

Kasus 7 : Gamarue

Win32/Gamarue adalah jenis malware worm komputer. Malware ini memiliki kemampuan untuk menginfeksi komputer korban dan mengubah pengaturan keamanannya. Perubahan pengaturan keamanan ini memungkinkan malware ini untuk melakukan pengunduhan file tanpa izin pengguna. File yang diunduh oleh malware ini dapat menyebabkan komputer korban menampilkan pop-up iklan yang mengganggu, dan dalam beberapa kasus, bahkan dapat mengakibatkan pencurian informasi

kredensial, termasuk data kartu kredit, sehingga menjadi ancaman serius. Malware ini dapat menyebar melalui berbagai cara, seperti eksploitasi kit atau malware lainnya, melalui lampiran dalam email, atau bahkan melalui perangkat USB Flash Drive yang sudah terinfeksi.

Kasus 8 : Mining Trojan

Mining Trojan, juga dikenal sebagai Trojan.BitCoinMiner, merujuk kepada program yang melakukan aktivitas pertambangan kripto (crypto-currency mining) tanpa sepengetahuan pengguna sistem dan menggunakan sumber daya komputer tanpa izin. Proses pertambangan ini memerlukan sejumlah besar sumber daya komputer, sehingga para penjahat mencoba untuk memanfaatkan mesin orang lain untuk melaksanakan pertambangan tersebut. Program ini mengalokasikan banyak sumber daya untuk mengoptimalkan pendapatan kripto, yang dapat mengakibatkan penurunan kinerja mesin pengguna. Selain dari dampak penurunan kinerja, jika penjahat mengatur mesin untuk bekerja pada tingkat maksimumnya dalam jangka waktu yang lama, hal ini dapat menyebabkan kerusakan pada mesin tersebut.

Kasus 9 : Glupteba

Glupteba adalah sebuah trojan yang berfungsi sebagai pintu belakang untuk menyerang sistem operasi Windows. Glupteba sering dikenal sebagai zombie atau bot, yang dapat diendalikan dari jarak jauh oleh para penjahat yang memanfaatkannya. Pada awalnya, Glupteba mulai menyebar pada tahun 2011 sebagai komponen tambahan yang dimuat oleh Trojan Alureon untuk melakukan clickjacking melalui iklan. Namun, pada bulan September 2019, Glupteba mulai menggunakan teknologi blockchain Bitcoin untuk memperbarui domain C2-nya melalui transaksi Bitcoin yang dilakukan dengan opcode skrip OP_RETURN. Penyerang biasanya menyebarkan file malware ini melalui iklan yang mencurigakan, lampiran email, aplikasi "crack" yang palsu atau bajakan, serta dengan memanfaatkan teknik rekayasa sosial.

Kasus 10 : CobaltStrike

Cobalt Strike sebenarnya adalah sebuah produk berbayar yang digunakan untuk melakukan uji penetrasi. Dengan produk ini, penyerang dapat mengirimkan sebuah agen yang disebut "Beacon" ke perangkat korban. Beacon memiliki beragam kemampuan, termasuk perekaman tombol, pengiriman file, proxy SOCKS, eskalasi hak akses, pemindaian port, serta pergerakan lateral. Selain itu, Cobalt Strike juga dapat digunakan untuk menemukan kerentanan, seperti bug dan kelemahan, yang mungkin ada dalam sistem(Lidya Julita, 2021).

Analisis Risiko: Risiko tinggi karena kerusakan perangkat lunak dapat menghambat operasi bisnis.

Risiko 5: Risiko Manajemen Identitas

Tim Kaspersky telah mengkaji sejauh mana persiapan usaha mikro, kecil, dan menengah (UMKM) menghadapi insiden di dunia maya yang tidak bisa diprediksi. Hasil penelitian ini menunjukkan bahwa hampir setengah dari UMKM yang disurvei merasa kurang yakin bahwa mantan karyawan tidak dapat mengakses data bisnis mereka melalui layanan cloud atau akun perusahaan. Jika mantan karyawan masih memiliki akses ke layanan perusahaan atau sistem informasi, ini bisa menyebabkan kerugian signifikan bagi bisnis yang pernah mereka tempati. UMKM seringkali prihatin dengan ancaman yang kurang jelas, seperti mantan karyawan yang mungkin menggunakan data perusahaan untuk mendirikan bisnis pesaing atau mencuri pelanggan. Namun, konsekuensi yang lebih serius juga perlu diperhatikan. Misalnya, jika mantan karyawan dapat mengakses database pelanggan yang berisi data pribadi, mereka bisa membocorkannya secara publik atau menjualnya di dark web. Ini berpotensi merusak reputasi bisnis, merugikan pelanggan, dan berakibat pada sanksi hukum yang signifikan dari pihak regulator. Tentu saja, sanksi ini bervariasi tergantung pada undang-undang di negara masing-masing, tetapi ada tren global untuk mengintensifkan sanksi terhadap kebocoran data semacam ini.

Analisis Risiko: Risiko tinggi karena akses yang tidak sah dapat membocorkan informasi rahasia.

Risiko 6: Risiko Kepatuhan Regulasi

Studi kasus yang dilakukan oleh Evidon, perusahaan riset pasar berbasis di New York, Amerika Serikat. Menurut hasil riset mereka, perusahaan yang sudah mematuhi aturan GDPR dapat memperbaiki layanan pelanggannya. Ini dilihat dari peningkatan loyalitas customer sebesar 34%, citra baik perusahaan sebesar 33%, dan interaksi konsumen sebesar 30%.5

Dari studi kasus di atas, bisa dilihat bahwa penerapan kebijakan mengenai data sovereignty dapat mendukung perkembangan bisnis di suatu negara. Di Indonesia sendiri, penerapan PP No. 82 mendapatkan pro dan kontra dari pelaku bisnis. Ada pula tanggapan dari pelaku bisnis mengenai dampak penerapannya terhadap menurunnya investasi di Indonesia. Berdasarkan riset yang dilakukan oleh TRPC Research Firm (perusahaan konsultan industri teknologi informasi dan teknologi di Asia-Pasifik), persyaratan lokalisasi data secara menyeluruh mengurangi GDP Indonesia sebesar 0,5-0,7%, membatasi masuknya investasi ke Indonesia sebesar 2,3%, dan meningkatkan biaya kebutuhan komputer sekitar 30-60%(GlobeNewswire, n.d.).

Presentasi Kementerian Komunikasi dan Informatika RI, slide 2(Menkoinfo RI, n.d.).

Analisis Risiko: Risiko tinggi karena pelanggaran dapat mengakibatkan denda besar dan kerugian reputasi.

Dalam studi kasus ini, identifikasi risiko-risiko teknologi informasi sangat penting untuk mengarahkan audit yang tepat dan memberikan rekomendasi untuk mengurangi risiko-risiko tersebut. Auditor akan melakukan evaluasi lebih lanjut dan merancang langkah-langkah pengendalian yang sesuai untuk mengatasi risiko-risiko ini.

7.5 Perencanaan Audit Teknologi Informasi Akuntansi dan Bisnis

Perencanaan Audit Teknologi Informasi Akuntansi dan Bisnis adalah langkah kritis dalam melakukan audit teknologi informasi yang efektif. Berikut adalah beberapa komponen utama dari perencanaan audit teknologi informasi beserta referensi yang relevan:

1. **Penentuan Tujuan Audit:**
   Auditor harus menentukan tujuan audit dengan jelas, termasuk apa yang akan diperiksa dan hasil yang diharapkan.
2. **Penetapan Lingkup Audit:**
   Menentukan ruang lingkup audit dengan mengidentifikasi sistem teknologi informasi, aplikasi, atau proses bisnis yang akan diaudit.
3. **Identifikasi Risiko:**
   Mengidentifikasi potensi risiko yang terkait dengan teknologi informasi, termasuk risiko keamanan, risiko integritas data, dan risiko operasional.
4. **Pemilihan Tim Audit:**
   Memilih anggota tim audit yang memiliki kualifikasi dan keahlian yang sesuai untuk mengaudit teknologi informasi.
5. **Pembuatan Program Audit:**
   Merancang program audit yang mencakup langkah-langkah pemeriksaan teknis dan fungsional yang akan dilakukan selama audit.
6. **Penentuan Sumber Daya:**
   Menentukan sumber daya yang dibutuhkan untuk melaksanakan audit, termasuk anggaran, perangkat keras, perangkat lunak, dan alat audit yang diperlukan.
7. **Penjadwalan Audit:**
   Menjadwalkan waktu dan durasi audit, serta mengkoordinasikan jadwal dengan pihak terkait.
8. **Konsultasi dengan Manajemen:**
   Berkomunikasi dengan manajemen organisasi untuk memahami tujuan bisnis, kebijakan, dan harapan terkait audit, mencakup panduan lengkap tentang perencanaan audit teknologi informasi, termasuk langkah-langkah yang harus diambil dalam tahap perencanaan (Hall, 2011). Mencantumkan informasi terperinci tentang perencanaan audit teknologi informasi dalam konteks akuntansi dan bisnis (Alvin A. Arens, 2017).

7.6 Pelaksanaan Audit Teknologi Informasi Akuntansi dan Bisnis

Pelaksanaan Audit Teknologi Informasi Akuntansi dan Bisnis adalah tahap penting dalam proses audit di mana auditor melakukan pemeriksaan, evaluasi, dan pengujian secara langsung terhadap sistem teknologi informasi yang digunakan dalam operasi bisnis dan proses akuntansi suatu organisasi. Tujuannya adalah untuk mengumpulkan bukti-bukti audit, mengidentifikasi potensi risiko, serta menilai efektivitas, keamanan, dan kepatuhan sistem tersebut terhadap standar dan kebijakan yang berlaku. Pada tahap ini, auditor akan melaksanakan langkah-langkah yang telah direncanakan dalam perencanaan audit, seperti pengujian kontrol internal, uji penetrasi, pemantauan aktivitas sistem, dan pemeriksaan dokumen dan catatan relevan. Selain itu, auditor juga dapat melakukan wawancara dengan personel yang terlibat dalam penggunaan dan pengelolaan teknologi informasi. Hasil dari pelaksanaan audit ini akan menjadi dasar bagi auditor untuk membuat temuan, rekomendasi, dan kesimpulan audit (Hall, 2011), memberikan panduan rinci tentang langkah-langkah yang harus diambil selama pelaksanaan audit teknologi informasi dalam konteks akuntansi dan bisnis. Mencakup informasi terperinci tentang pelaksanaan audit teknologi informasi dan bagaimana mengumpulkan bukti-bukti audit yang relevan selama proses audit (Alvin A. Arens, 2017). Berikut adalah tahapan-tahapan umum dalam pelaksanaan Audit Teknologi Informasi Akuntansi dan Bisnis beserta referensi yang relevan (Hall, 2011):

1. **Identifikasi dan Evaluasi Risiko:**
   Identifikasi risiko yang terkait dengan penggunaan teknologi informasi dalam akuntansi dan bisnis. Evaluasi signifikansi risiko-risiko tersebut.
2. **Pengujian Pengendalian Internal**:
   Melakukan pengujian terhadap pengendalian internal yang telah ditetapkan dalam sistem teknologi informasi. Memastikan bahwa pengendalian tersebut efektif dalam mengurangi risiko kesalahan dan penyalahgunaan.

3. **Pengujian Substansif:**
   Melakukan pengujian substansif untuk memverifikasi keakuratan informasi keuangan yang dihasilkan oleh sistem teknologi informasi. Memeriksa dokumen, catatan, dan transaksi yang relevan.
4. **Pengujian Keamanan dan Pemulihan Bencana:**
   Melakukan pengujian keamanan sistem, termasuk uji penetrasi, untuk mengidentifikasi potensi kerentanan. Menguji rencana pemulihan bencana untuk memastikan keberlanjutan operasi dalam situasi darurat.
5. **Pengujian Ketaatan Terhadap Regulasi:**
   Memastikan bahwa organisasi mematuhi regulasi dan kebijakan yang berlaku terkait dengan teknologi informasi. Mengaudit ketaatan terhadap regulasi seperti GDPR, HIPAA, atau regulasi keuangan.
6. **Pemantauan dan Pemantauan Aktivitas Sistem:**
   Memantau aktivitas sistem secara langsung untuk mendeteksi indikasi penyalahgunaan atau kejadian tidak biasa. Menganalisis log aktivitas dan kejadian keamanan.
7. **Wawancara dan Konsultasi:**
   Melakukan wawancara dengan personel yang terlibat dalam penggunaan dan pengelolaan teknologi informasi. Berkonsultasi dengan manajemen dan staf terkait untuk memahami proses bisnis dan kebijakan yang berlaku.
8. **Pengumpulan dan Dokumentasi Bukti:**
   Mengumpulkan bukti-bukti audit yang relevan seperti dokumen, laporan, log, dan hasil pengujian. Membuat dokumentasi audit yang komprehensif.

James A. Hall memberikan panduan rinci tentang tahapan-tahapan pelaksanaan audit teknologi informasi, termasuk referensi mengenai pengujian kontrol internal, pengujian keamanan, dan pengujian substansif.

Alvin A. Arens, et al. juga mencakup informasi terperinci tentang pelaksanaan audit teknologi informasi dalam konteks akuntansi dan bisnis.

7.7 Keamanan Teknologi Informasi dan Pengendalian

Keamanan Teknologi Informasi dan Pengendalian (*Information Technology Security and Controls*) adalah aspek penting dalam dunia bisnis modern yang berkaitan dengan melindungi aset, data, dan operasi yang menggunakan teknologi informasi dari berbagai ancaman dan risiko. Ini mencakup berbagai tindakan dan pengendalian yang dirancang untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi serta melindungi sistem dan jaringan dari potensi ancaman seperti serangan siber, kebocoran data, atau kerentanan keamanan. Beberapa aspek penting dari Keamanan Teknologi Informasi dan Pengendalian meliputi(Andy Taylor, David Alexander, 2013):

1. **Pengendalian Akses**: Memastikan bahwa hanya individu yang berwenang memiliki akses ke sistem dan data yang sensitif. Ini melibatkan penggunaan otentikasi kuat, manajemen hak akses, dan pengawasan aktivitas pengguna.
2. **Enkripsi**: Menggunakan teknik enkripsi untuk melindungi data saat berpindah melalui jaringan atau saat disimpan di dalam sistem.
3. **Audit Log dan Pemantauan**: Memonitor aktivitas sistem dan pengguna dengan menggunakan audit log. Pemantauan ini membantu mendeteksi potensi ancaman atau aktivitas mencurigakan.
4. **Firewall dan Proteksi Jaringan**: Menggunakan firewall dan perangkat lunak keamanan jaringan untuk melindungi jaringan dari serangan siber dan ancaman luar.
5. **Pemulihan Bencana**: Merencanakan strategi pemulihan bencana untuk memastikan bahwa sistem dan data dapat dipulihkan dalam situasi darurat.
6. **Kebijakan Keamanan dan Pelatihan Karyawan**: Menetapkan kebijakan keamanan yang jelas dan melaksanakannya. Melatih karyawan untuk memahami dan mengikuti praktik keamanan yang baik.

NIST *Special Publication* 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*, yang

diterbitkan oleh *National Institute of Standards and Technology* (NIST) adalah referensi resmi yang digunakan dalam banyak organisasi dan pemerintahan untuk mengembangkan dan mengevaluasi pengendalian keamanan teknologi informasi. Informasi dapat mengaksesnya secara online di situs web NIST. Berikut adalah langkah-langkah umum dalam mengimplementasikan Keamanan Teknologi Informasi dan Pengendalian (*Information Technology Security and Controls*) beserta referensi yang relevan:

1. **Identifikasi Risiko Keamanan**:
   Identifikasi dan penilaian risiko keamanan yang mungkin dihadapi oleh organisasi dalam penggunaan teknologi informasi. NIST SP 800-30 "*Guide for Conducting Risk Assessments*" yang diterbitkan oleh National Institute of Standards and Technology (NIST) memberikan panduan tentang bagaimana melakukan penilaian risiko keamanan(NIST, 2012).
2. **Pembuatan Kebijakan Keamanan:**
   Menetapkan kebijakan keamanan teknologi informasi yang mencakup kebijakan akses, enkripsi data, manajemen kata sandi, dan praktik keamanan lainnya. NIST SP 800-12 "*An Introduction to Computer Security: The NIST Handbook*" memberikan panduan umum tentang pembuatan kebijakan keamanan(Nieles et al., 2017).
3. **Implementasi Pengendalian Keamanan:**
   Melaksanakan pengendalian keamanan yang sesuai berdasarkan kebijakan yang telah ditetapkan, termasuk pengendalian akses, enkripsi, firewall, dan perangkat keamanan lainnya. ISO/IEC 27001 adalah standar internasional yang mencakup implementasi pengendalian keamanan informasi.
4. **Pemantauan dan Pemeliharaan Keamanan:**
   Memantau sistem secara terus-menerus untuk mendeteksi aktivitas yang mencurigakan atau ancaman keamanan. NIST SP 800-137 *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* memberikan panduan tentang pemantauan keamanan berkelanjutan.

5. **Pelatihan dan Kesadaran Keamanan:**
   Memberikan pelatihan kepada karyawan tentang praktik keamanan teknologi informasi dan kesadaran terhadap ancaman. NIST SP 800-50 "*Building an Information Technology Security Awareness and Training Program*" memberikan panduan tentang pelatihan dan kesadaran keamanan.
6. **Penanganan Insiden Keamanan:**
   Mengembangkan rencana penanganan insiden keamanan yang mencakup respons terhadap serangan atau insiden keamanan. NIST SP 800-61 *"Computer Security Incident Handling Guide" memberikan panduan tentang penanganan insiden keamanan.*
7. **Audit dan Evaluasi Keamanan:**
   Melakukan audit dan evaluasi rutin terhadap kebijakan dan pengendalian keamanan untuk memastikan kepatuhan dan efektivitasnya. *Information Technology Control and Audit* oleh Frederick Gallegos dan Sandra Senft memberikan panduan tentang audit dan evaluasi keamanan teknologi informasi. Langkah-langkah ini dapat disesuaikan dengan kebutuhan dan ukuran organisasi Anda serta standar keamanan yang berlaku dalam industri atau sektor Anda.

7.8 Pelaporan Hasil Audit

Pelaporan Hasil Audit adalah tahap penting dalam proses audit di mana auditor menyusun laporan yang berisi temuan, rekomendasi, dan kesimpulan hasil dari audit yang telah dilakukan. Laporan ini disampaikan kepada manajemen organisasi atau pihak yang memiliki wewenang dan tanggung jawab untuk mengambil tindakan berdasarkan hasil audit. Tujuan dari pelaporan hasil audit adalah untuk memberikan informasi yang relevan dan objektif kepada pihak yang berkepentingan agar mereka dapat mengambil langkah-langkah yang diperlukan untuk memperbaiki kontrol, meminimalkan risiko, dan memastikan kepatuhan terhadap standar dan regulasi yang berlaku.

Elemen-elemen utama dalam Pelaporan Hasil Audit meliputi:

1. **Temuan Audit**: Rincian mengenai temuan atau masalah yang diidentifikasi selama audit. Ini termasuk deskripsi

masalah, sumber masalah, serta bukti-bukti audit yang mendukung temuan tersebut.

2. **Rekomendasi:** Saran atau rekomendasi dari auditor tentang langkah-langkah yang harus diambil untuk mengatasi atau memperbaiki masalah yang diidentifikasi. Rekomendasi ini dirancang untuk membantu organisasi memperbaiki pengendalian, proses, atau praktik yang perlu diperbaiki.
3. **Kesimpulan**: Kesimpulan umum tentang hasil audit, termasuk tingkat kepatuhan terhadap standar atau kebijakan yang berlaku, serta kesimpulan mengenai efektivitas sistem pengendalian internal.
4. **Catatan Tambahan**: Informasi tambahan yang relevan, seperti metodologi audit yang digunakan, lingkup audit, dan waktu pelaksanaan audit.
5. **Risiko dan Dampak**: Evaluasi risiko dan dampak yang terkait dengan temuan audit, termasuk potensi kerugian atau konsekuensi jika masalah tidak ditangani.
6. **Tindak Lanjut**: Rencana tindak lanjut yang harus diambil oleh manajemen untuk menangani masalah yang diidentifikasi. Ini termasuk jadwal pelaksanaan, tanggung jawab, dan langkah-langkah konkret yang akan diambil.
7. **Kepatuhan Hukum dan Regulasi**: Penjelasan apakah organisasi telah mematuhi hukum, regulasi, atau standar tertentu yang berlaku dalam konteks audit.
8. **Kesaksian Auditor**: Tanda tangan auditor atau tim audit sebagai bukti bahwa laporan audit telah diperiksa dan disetujui oleh mereka.

Pelaporan Hasil Audit harus disusun dengan jelas, objektif, dan profesional, serta disampaikan kepada pihak yang berkepentingan dengan cepat setelah selesai audit. Laporan ini merupakan dokumen penting yang digunakan sebagai dasar untuk pengambilan keputusan, perbaikan proses, dan manajemen risiko dalam organisasi. Penyusunan Pelaporan Hasil Audit biasanya mengikuti pedoman dan standar yang berlaku dalam profesi audit

dan organisasi, serta memperhatikan kebutuhan pihak-pihak yang akan menerima laporan tersebut.

7.9 Pengauditan Teknologi Informasi Akuntansi dan Bisnis menggunakan Framework COBIT 2019

Berikut adalah detail langkah-langkah dalam pelaksanaan audit TI dengan menggunakan kerangka kerja COBIT 2019(ISACA, 2019):

1. **Pelaksanaan Audit**
   a. Penyusunan Rencana Audit:
      1) Menyusun Rencana: Membuat rencana yang mendetil mengenai tujuan, ruang lingkup, dan pendekatan yang akan diambil selama audit.
      2) Identifikasi Sumber Daya: Menentukan sumber daya yang akan diperlukan selama audit.
   b. Pengidentifikasian dan Evaluasi Kontrol:
      1) Pemilihan Kontrol: Mengidentifikasi dan memilih kontrol yang relevan dari kerangka kerja COBIT 2019.
      2) Penilaian Kontrol: Menilai efektivitas kontrol tersebut dalam menjaga integritas sistem informasi.
2. **Pengumpulan Bukti**
   a. Identifikasi Bukti:
      1) Jenis Bukti: Menentukan jenis-jenis bukti yang perlu dikumpulkan untuk membuktikan kepatuhan terhadap kontrol yang telah diidentifikasi.
      2) Dokumentasi: Memastikan bahwa seluruh dokumentasi terkait dengan kontrol yang dipilih tersedia dan terkini.
   b. Pengumpulan dan Pengujian Bukti:
      1) Metodologi: Menentukan metodologi yang akan digunakan untuk pengumpulan bukti.
      2) Pengujian Substantif: Melaksanakan pengujian substantif untuk memvalidasi bukti yang dikumpulkan

3. Evaluasi Pengendalian

a. Analisis Bukti:
   1) Review: Menganalisis bukti yang dikumpulkan untuk memahami sejauh mana kontrol berfungsi dengan efektif.
   2) Pengidentifikasian Masalah: Mengidentifikasi masalah atau kelemahan dalam kontrol yang ada.

b. Penilaian Risiko:
   1) Identifikasi Risiko: Mengidentifikasi risiko potensial yang dihadapi organisasi.
   2) Penilaian Risiko: Melakukan penilaian risiko untuk mengidentifikasi dan menganalisis potensi risiko yang mungkin dihadapi.

4. Pelaporan

a. Penyusunan Laporan Audit:
   1) Draft Laporan: Membuat draft laporan audit yang memaparkan temuan dan rekomendasi.
   2) Review Laporan: Memastikan bahwa laporan tersebut telah mengidentifikasi semua area risiko dan menyediakan rekomendasi yang sesuai untuk mitigasi.

b. Pembahasan dan Finalisasi:
   1) Diskusi dengan Stakeholder: Mendiskusikan rancangan laporan dengan pihak-pihak terkait untuk mendapatkan masukan mereka.
   2) Finalisasi: Menyelesaikan laporan berdasarkan umpan balik yang diterima dan mempersiapkan untuk penyajian.

Setelah proses ini selesai, langkah selanjutnya adalah menyajikan temuan dan rekomendasi kepada pihak-pihak terkait dan memulai proses tindak lanjut untuk mengatasi area-area yang memiliki kelemahan kontrol atau risiko tinggi. Itu adalah prinsip umum dari pelaksanaan audit TI menggunakan kerangka kerja COBIT 2019.

7.9 Tantangan dan Isu Terkini dalam Pengauditan Teknologi Informasi

Tantangan dan isu terkini dalam pengauditan teknologi informasi adalah sebagai berikut:

1. **Keamanan Data**: Menjamin bahwa sistem dan data yang diaudit terlindungi dari ancaman keamanan seperti peretasan (hacking) dan serangan malware.(ISACA, n.d.)
2. **Kepatuhan Regulasi**: Memastikan bahwa sistem teknologi informasi mematuhi semua peraturan dan regulasi yang berlaku, seperti GDPR, HIPAA, dan peraturan privasi data lainnya.(Gultom et al., 2021; Sudibyo, 2020)
3. **Audit Sumber Terbuka (*Open Source*)**: Mengelola risiko dan keamanan yang terkait dengan penggunaan perangkat lunak sumber terbuka yang semakin populer.(ISACA, 2011)
4. **Kompleksitas *Cloud Computing***: Mengaudit infrastruktur yang berbasis cloud dan memastikan keamanan serta ketaatan terhadap kebijakan dalam lingkungan yang dinamis ini.(ISACA, 2011)
5. **Ketidakpastian Teknologi Baru**: Berurusan dengan teknologi baru seperti *Internet of Things* (IoT), kecerdasan buatan (AI), dan *blockchain* yang memerlukan pemahaman dan pengujian khusus.(JETA, 2018)

Selain tantangan dan isu yang telah disebutkan sebelumnya, berikut adalah beberapa tantangan dan isu terkini lainnya dalam pengauditan teknologi informasi:

1. **Ketidakpastian Privasi Data**: Menangani perhatian yang semakin meningkat terhadap privasi data pengguna, termasuk penggunaan data pribadi dan perizinan yang sesuai.(Gultom et al., 2021; Sudibyo, 2020)
2. **Serangan Siber yang Terus Berkembang**: Menghadapi serangan siber yang semakin canggih dan berbagai jenis ancaman siber, seperti serangan ransomware dan serangan nol hari.(ISACA, 2021c)
3. **Ketidakpastian dalam Audit Remote**: Mengaudit sistem yang semakin sering diakses dari lokasi jarak jauh, sehingga

menghadapi tantangan terkait keamanan dan validasi identitas.("Auditing in the Age of Remote Work," 2020)

4. **Integrasi dengan Kepatuhan *Environmental, Social, and Governance* (ESG)**: Menilai dampak lingkungan, sosial, dan tata kelola (ESG) dalam konteks audit teknologi informasi untuk memenuhi tuntutan keberlanjutan.(Deloitte, 2021)
5. **Ketergantungan pada Perangkat Lunak Pihak Ketiga**: Memahami risiko yang terkait dengan penggunaan perangkat lunak dan layanan pihak ketiga, serta mengevaluasi kontrak dan kepatuhan.(ISACA, 2020)

Tentu, ada beberapa tantangan dan isu terkini lainnya dalam pengauditan teknologi informasi:

1. **Kekurangan Keahlian**: Keterbatasan tenaga ahli dalam pengauditan teknologi informasi yang memahami baik aspek bisnis maupun teknis, serta kesulitan untuk merekrut dan mempertahankan staf berkualitas.(ISACA, 2021b)
2. **Kepatuhan Terhadap Standar Keamanan**: Menilai apakah sistem teknologi informasi mematuhi standar keamanan seperti ISO 27001 atau NIST, dan memastikan bahwa semua kelemahan diatasi(Marwan, 2018).
3. **Ketidakpastian dalam Audit Proses Otomasi**: Mengaudit sistem yang semakin otomatis, seperti proses RPA (*Robotic Process Automation*) dan AI, yang memerlukan pemahaman khusus.("Auditing Artificial Intelligence: Opportunities and Challenges," 2020)
4. **Mengelola Big Data**: Tantangan dalam mengaudit sistem yang menghasilkan dan mengelola data besar (big data) untuk memastikan keakuratan, keamanan, dan kepatuhan.(Manyika et al., 2011)
5. **Audit dalam Lingkungan Berbasis DevOps**: Memahami dan mengaudit proses pengembangan dan pengiriman perangkat lunak dalam lingkungan DevOps yang cepat dan berkelanjutan.(ISACA, 2021a)

DAFTAR PUSTAKA

10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-ramai Bantah. (n.d.). Retrieved September 26, 2023, from https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah

Alvin A. Arens, Randal J. Elder, M. S. B. (2012). *Auditing and assurance services : an integrated approach* (14th ed.). Upper Saddle River, New Jersey : Pearson Education International.

Andy Taylor, David Alexander, A. F. (2013). *Information Security Management Principles* (Andy Tailor, Ed.; Second edi). BCS Learning & Development Ltd All rights reserved.

Article 29 Working Party. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining. *The Working Party on The Protection of Individuals With Regard to The Processing of Personal Data*, *April*, 1–21. ec.europa.eu/newsroom/document.cfm?doc_id=44137%0A

Auditing Artificial Intelligence: Opportunities and Challenges. (2020). *ISACA Journal*, *Volume 5*.

Auditing in the Age of Remote Work. (2020). *Journal of Accountancy*.

BBC. (n.d.). *Perusahaan mengalami kegagalan sistem yang menyebabkan gangguan layanan kepada pelanggan.* BBC News Indonesia. https://www.bbc.com/indonesia/articles/cn01gdr7eero%0A

Bernardino, R. (2021). ISO 27001 ver 2013. *ResearchGate*, *February*. https://www.researchgate.net/publication/349366608_ISO_27001_ver_2013

Caplan, R. M. (2003). HIPAA. Health Insurance Portability and Accountability Act of 1996. *Dental Assistant (Chicago, Ill. : 1994)*, *72*(2), 6–8.

Champlain, J. J. (2019). Auditing Information Systems. In *Information Systems Management*. https://doi.org/10.1002/9781119332497.ch9

Deloitte. (2021). The Role of Auditors in ESG: Challenges and Opportunities. *Deloitte*.

DREAM.CO.ID. (n.d.). *Data 540 Juta Pengguna Facebook Bocor ke Publik*. DREAM.CO.ID. https://www.dream.co.id/lifestyle/data-540-juta-pengguna-facebook-bocor-ke-publik-1904051.html

FORCE, J. T. T. I. (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Publication*, *800*(September 2020), 53.

GlobeNewswire. (n.d.). *Independent Study Commissioned by Evidon Reveals that GDPR Budgets Will Increase in 2018 As Organizations Look to Balance Compliance and Customer Experience*. GlobeNewswire. https://www.globenewswire.com/news-release/2017/12/11/1268647/0/en/Independent-Study-Commissioned-by-Evidon-Reveals-that-GDPR-Budgets-Will-Increase-in-2018-As-Organizations-Look-to-Balance-Compliance-and-Customer-Experience.html

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2020). Digital identity guidelines.(National Institute of Standards and Technology, Gaithersburg, MD). *NIST Special Publicaiton 800-63-3*, *58*(2), 130–137. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

Gultom, O., Saputra, A. F., & Aziz, M. F. (2021). *Perlindungan Data Pribadi Di Indonesia Menyikapi Liberalisasi Ekonomi Digital*. 1–135.

Hayes, R., Wallage, P., & Gortemaker, H. (2014). Principal of Auditing: An Introduction to International Standards on Auditing. *Person Education Limited (UK)*, 6–700. www.booksites.net/hayes

ISACA. (n.d.). *CISA (Certified Information Systems Auditor) Review Manual, 27th Edition.*

ISACA. (2011). Challenges and Concerns in Auditing Cloud Computing. *ISACA Journal*, *Volume 2*.

ISACA. (2019). COBIT 2019 Framework - Introduction and Methodology. In *www.icasa.org/COBITuse*.

ISACA. (2020). Third-Party Risk Management and Compliance. *ISACA Journal*, *Volume 5*.

ISACA. (2021a). "Auditing in a DevOps World. *ISACA Journal*, *Volume 5*.

ISACA. (2021b). *Cybersecurity Skills Shortage," Cybersecurity & Infrastructure Security Agency (CISA)*.

ISACA. (2021c). Ransomware and the Role of Cyber Insurance. *ISACA Journal*, *Volume 6*.

ISACA Governance and Manajement. (2019). *COBIT 2019 Governance and Management Objectives (ISACA)*. https://netmarket.oss.aliyuncs.com/df5c71cb-f91a-4bf8-85a6-991e1c2c0a3e.pdf

ISO/IEC. (2013). *Information technology-Security techniques-Code of practice for information security controls Technologies de l'information-Techniques de sécurité-Code de bonne pratique pour le management de la sécurité de l'information(E) ii COPYRIGHT PROTECTED DOCUMENT*. *2013*. www.iso.org

JETA. (2018). Emerging Technology and Its Impact on Auditing," ,. *Journal of Emerging Technologies in Accounting*.

Landoll, D. (2016). The Security Risk Assessment Handbook. In *The Security Risk Assessment Handbook*. https://doi.org/10.1201/b10937

Lidya Julita. (2021). *Trojan AllAple dan 10 Serangan Siber Dahsyat ke RI, Waspada!* CNBC Indonesia. https://www.cnbcindonesia.com/tech/20210306144357-37-228309/trojan-allaple-dan-10-serangan-siber-dahsyat-ke-ri-waspada

Manyika, J., Chui Brown, M., B. J., B., Dobbs, R., Roxburgh, C., & Hung Byers, A. (2011). Big data: The next frontier for innovation, competition and productivity. *McKinsey Global Institute*, *June*, 156. https://bigdatawg.nist.gov/pdf/MGI_big_data_full_report.pdf

Marwan, A. (2018). *Kerangka Kerja untuk Meningkatkan Keamanan Siber Infrastruktur Kritis*. *April*, 1–51.

Menkoinfo RI. (n.d.). *KOMINFO Perkembangan Ekonomi paska gangguan Keamanan TI*.

Nieles, M., Dempsey, K., & Pillitteri, V. (2017). *An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12* (Vol. 1). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-12.pdf

NIST. (2012). NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments. *NIST Guide for Conducting Risk Assessments*, *September*, 95.

Owasp.org. (2017). OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks. In *The OWASP Foundation*. The OWASP Foundation. https://doi.org/10.1002/kin.550040606

Peret, P. (2022). Information system audit. In *Information System Audit*. https://doi.org/10.1201/9781003230137-3

Regulation, G. D. P. (2018). The General Data Protection Regulation (GDPR) AN EPSU BRIEFING. *General Data Protection Regulation (GDPR)*, 1–40. https://www.epsu.org/sites/default/files/article/files/GDPR_FINAL_EPSU.pdf

Robert, B., & Brown, E. B. (2004). *Handbook Of International Quality Control, Auditing, Review, Other Assurance, and Related Service Pronouncement* (Issue 1). International Federation of Accountants 545 Fifth Avenue, 14th Floor New York, New York 10017 USA.

Robertson, J. (2010). Auditing for Fraud Detection. *Professional Education Service, LP*, 1–308.

Sanchez, R., & Enrique, J. (2017). *INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security*. *2016*.

Sandria, F. (2021). *Deretan Skandal Lapkeu di Pasar Saham RI, Indofarma-Hanson!* CNBC Indonesia. https://www.cnbcindonesia.com/market/20210726191301-17-263827/deretan-skandal-lapkeu-di-pasar-saham-ri-indofarma-hanson

Sigler, K. E., & Rainey, J. L. (2016). Securing an IT organization through governance, risk management, and audit. In *Securing an IT Organization through Governance, Risk Management, and Audit*. https://doi.org/10.1201/b19194

Souppaya, M., & Scarfone, K. (2022). *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

Sudibyo, A. (2020). Perlindungan Data Pengguna Internet: Menelaah GDPR Uni Eropa. *Anggota Dewan Pers*, 174–198. https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20200701-114454-7688.pdf

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency Planning Guide for Federal Information Systems. *NIST Special Publication 800-34 Rev. 1*, *May*, 150.

Turner, L., & Weickgenannt, A. B. (2008). *Accounting Information Systems: Controls and Processes*.

Wibowo, A. M., & Sc, M. (2005). ISO 27001 : 2005 Information Security Management Systems. *Risk Management*.

www.iso.org. (n.d.). *ISO/IEC TR 27008:2011 Information technology — Security techniques — Guidelines for auditors on information security controls*. Www.Iso.Org. https://www.iso.org/standard/45244.html

BAB 8
PROSES DAN PENGENDALIAN ATAS PENDAPATAN SERTA PENERIMAAN KAS

Oleh Ika Prayanthi

8.1 Pendahuluan

Setiap jenis organisasi perlu memahami bahwa sangatlah penting untuk mengelolah pendapatan dan penerimaan kas yang efektif untuk meningkatkan kinerja dan keberlanjutan perusahaan. Dalam hal ini tentu saja akan melibatkan penanganan transaksi keuangan yang sistematis dan efisien serta memastikan bahwa pendapatan dikumpulkan dan dicatat secara akurat dan tepat waktu. Salah satu cara untuk menjaga stabilitas keuangan adalah dengan memastikan manajemen pendapatan dan penerimaan kas efektif. Tanpa manajemen pendapatan dan penerimaan kas yang tepat organisasi akan mengalamai masalah arus kas dan pada akhirnya terjadi ketidakstabilan keuangan bahkan potensi kebangkrutan. Praktik manajemen yang efektif seperti faktur tepat waktu, pencatatan yang akurat, pengumpulan pembayaran yang cepat, arus kas yang stabil dan andal akan mengurangi risiko krisis keuangan.

Manajemen pendapatan dan penerimaan kas yang efektif juga akan memberikan data yang berharga untuk pengambilan keputusan. Melalui data penjualan perusahaan dapat mengidentifikasi produk atau layanan mereka yang paling memberikan keuntungan sehingga perusahaan dapat menentukan target pasar mereka. Disamping itu data juga akan menolong para pengambil keputusan terkait untuk mengalokasikan sumber daya yang tepat, melakukan penetapan harga yang tepat, sehingga memaksimalkan potensi pendapatan perusahaan. Data yang akurat serta tepat waktu tentang pendapatan dan penerimaan kas akan membantu perusahaan membuat keputusan sehingga perusahaan

akan mampu menangkap setiap peluang dan menghindari kinerja keuangan yang buruk.

Efektifnya manajemen pendapatan dan penerimaan kas juga akan berdampak pada efisiensi operasional dalam organisasi. Jika perusahaan menerapkan sistem otomatis dengan menggunakan sistem terkomputerisasi untuk faktur maka hal ini akan menyederhanakan proses keuangan, mengurangi kesalahan manual dan biaya administrasi, dan menghemat waktu dan sumber data untuk pemrosesan pembayaran serta rekonsiliasi dan verifikasi data manual. Praktik manajemen pendapatan dan penerimaan kas yang efektif juga akan memungkinkan organisasi lebih cepat mengidentifikasi dan mengatasi perbedaan atau penyimpangan dalam pendapatan dan penerimaan kas mereka, meminimalkan risiko penipuan atau penyalahgunaan keuangan.

Selain beberapa keuntungan yang sudah dipaparkan sebelumnya, manajemen pendapatan dan penerimaan kas yang efektif juga meningkatkan hubungan baik dengan pelanggan maupun pemangku kepentingan lainnya. Misalnya dalam hal pemrosesan faktur dan pembayaran yang tepat waktu, akurat, penawaran opsi pembayaran yang fleksibel, menyelesaikan masalah pembayaran dengan segera, semuanya ini otomatis menunjukkan profesionalisme, keandalan, kepercayaan serta kepuasan pelanggan. Hal-hal tersebut akan menumbuhkan loyalitas, otomatis akan dipromosikan dari mulut ke mulut dan pada akhirnya akan meningkatkan reputasi perusahaan dan kesuksesan jangka panjang.

Selain hal-hal yang telah diuraikan tersebut, Lasmana et al (2022) dan Saputra et al (2023) menyatakan pentingnya mekanisme sistem informasi akuntansi untuk proses penerimaan kas karena dapat memberikan bukti penjualan dan membantu melacak pendapatan serta sangat penting untuk menjaga laporan keuangan akurat dan dapat diandalkan. Bukti ini juga diperlukan untuk pelaporan pajak dan dapat digunakan sebagai bukti penjualan jika terjadi perselisihan dengan pelanggan atau pengembalian uang. Lebih lanjut dikatakan bahwa dengan memperoleh laporan keuangan yang akurat dan dapat diandalkan, perusahaan dapat membuat anggaran yang realistis yang lebih baik serta membuat keputusan keuangan yang cerdas. Selain itu juga dapat menolong

perusahaan untuk mengidentifikasi potensi kehilangan pendapatan sehingga menghasilkan pendapatan yang lebih tinggi.

Pengaturan dan pengelolaan penerimaan kas yang baik mengurangi risiko kesalahan atau aktivitas penipuan. Hal ini menjaga integritas catatan keuangan dan melindungi bisnis dari potensi kerugian (Pelealu and Sabijono, 2015). Manajemen penerimaan kas yang tepat juga dapat memperbaiki situasi keuangan dan masalah likuiditas entitas. Hal ini juga mempermudah proses audit, meningkatkan kepatuhan terhadap peraturan pajak dan meningkatkan efisiensi operasional secara keluruhan. Perusahaan harus dapat mengklasifikasikan aliran pendapatan dan memantau arus kas masuk untuk memastikan stabilitias dan kesuksesan keuangan. Dengan memahami berbagai sumber pendapatan dan arus kas masuk yang tersedia, bisnis dapat mengidentifikasi peluang untuk menghasilkan lebih banyak uang dan membuat keputusan yang tepat tentang penganggaran, investasi dan masalah keuangan lainnya. Berikut beberapa contoh sumber pendapatan seperti penjualan produk, biaya layanan, hasil investasi, pendapatan iklan, pendapatan berlangganan, lisensi, berbagi keahlian, penyewaan dan penjualan aset. Di era digital sekarang ini sumber pendapatan dari media digital juga telah menjadi alternatif (Vara-miguel *et al.*, 2021).

Arus kas masuk dapat bersumber dari pendapatan penjualan, investasi, pinjaman, aktivitas pendanaan, hibah dari pemerintah, pengembalian investasi dan lain-lain.

8.2 Sistem Informasi Akuntansi untuk Pendapatan dan Penerimaan Kas

8.2.1 Komponen Sistem Informasi Akuntansi

Sistem informasi akuntansi (SIA) yang efektif memainkan peran penting dalam mengelola dan mencatat transaksi keuangan dalam suatu organisasi. Salah satu aspek kunci dari SIA adalah mekanisme yang digunakannya untuk penerimaan pendapatan dan kas. Berikut adalah berbagai komponen dan proses yang terlibat dalam SIA yang memastikan pencatatan pendapatan dan penerimaan kas yang akurat dan andal (Rittenberg and Johnstone, 2017). SIA terdiri dari beberapa komponen yang saling

berhubungan yang bekerja sama untuk memfasilitasi pencatatan dan pemrosesan transaksi keuangan. Komponen utama yang relevan dengan pendapatan dan penerimaan kas meliputi (Needles, Powers and Crosson, 2017):

1. Data Input
   Komponen input data dari SIA bertanggung jawab untuk menangkap dan mengumpulkan informasi keuangan yang relevan. Dalam konteks penerimaan pendapatan dan kas, ini melibatkan pengambilan detail seperti informasi pelanggan, jumlah penjualan, metode pembayaran, dan detail faktur. Data ini dapat dikumpulkan melalui berbagai sumber seperti sistem *point-of-sale*, *gateway* pembayaran *online*, dan entri manual.
2. Penyimpanan Data
   Setelah data dikumpulkan, perlu disimpan dengan cara yang aman dan terorganisir. Komponen penyimpanan data dari SIA memastikan bahwa informasi yang dikumpulkan disimpan dalam database terpusat atau sistem berbasis *cloud*. Hal ini memungkinkan pengambilan dan referensi yang mudah bila diperlukan.
3. Pengolahan Data
   Komponen pemrosesan data SIA melibatkan berbagai operasi seperti verifikasi, klasifikasi, dan peringkasan data keuangan. Dalam konteks penerimaan pendapatan dan penerimaan kas, komponen ini memastikan bahwa transaksi yang dicatat akurat, lengkap, dan dikategorikan dengan benar. Ini juga melibatkan menghasilkan laporan dan laporan keuangan berdasarkan data yang diproses.
4. Pengendalian Internal
   Kontrol internal adalah bagian penting dari SIA untuk menjaga akurasi dan integritas transaksi keuangan. Dalam konteks penerimaan pendapatan dan penerimaan kas, pengendalian internal dapat mencakup pemisahan tugas, prosedur otorisasi, dan rekonsiliasi reguler untuk mencegah penipuan atau kesalahan.

5. Pelaporan
   Komponen pelaporan SIA menghasilkan laporan keuangan dan laporan yang memberikan wawasan tentang pendapatan dan penerimaan kas suatu organisasi. Laporan ini membantu manajemen membuat keputusan berdasarkan informasi dan menilai kesehatan keuangan bisnis. Laporan umum termasuk laporan laba rugi, neraca, dan laporan arus kas.

8.2.2 Pendapatan dan Penerimaan Kas yang Efektif

Manajemen pendapatan dan penerimaan kas yang efektif sangat penting untuk keberhasilan dan keberlanjutan organisasi mana pun (Karamoy, 2013). Manajemen pendapatan dan penerimaan kas yang efektif sangat penting untuk stabilitas keuangan dan pertumbuhan organisasi mana pun. Dengan menerapkan mekanisme pencatatan dan pelacakan yang tepat, serta pengendalian internal, bisnis dapat memastikan keakuratan, keandalan, dan keamanan transaksi keuangan mereka.

Perolehan pendapatan memastikan stabilitas keuangan bisnis, sementara mekanisme penerimaan kas yang tepat menjamin alokasi dan pemanfaatan dana yang efisien. Pada bagian ini akan mengeksplorasi mekanisme yang terlibat dalam penerimaan pendapatan dan kas, menyoroti signifikansi mereka dalam konteks yang lebih luas dari manajemen keuangan.

Manajemen dan penerimaan kas yang efektif melibatkan proses yang terdefinisi dengan baik dalam hal mencatat, melacak, merekonsiliasi transaksi, serta menerapkan kontrol internal untuk melindungi aset.

1. **Pencatatan dan Pelacakan Pendapatan.**
   Pendapatan mengacu pada arus kas masuk aset atau penyelesaian kewajiban yang dihasilkan dari kegiatan bisnis. Ini merupakan indikator penting dari kinerja keuangan dan keberlanjutan perusahaan. Dasar pencatatan akrual akuntansi mengakui pendapatan ketika diperoleh, terlepas dari kapan pembayaran diterima.
   Dasar akrual akuntansi untuk pengakuan pendapatan ketika diperoleh, terlepas dari kapan

pembayaran diterima. Untuk prinsip pencocokan adalah memastikan bahwa pendapatan dicocokkan dengan biaya yang dikeluarkan untuk mendapatkannya. Metode pencatatan pendapatan untuk pendapatan penjualan, dicatat ketika barang atau jasa dikirim ke pelanggan. Untuk pendapatan bunga, diakui sebagai bunga yang timbul atas pinjaman atau investasi sedangkan untuk pendapatan sewa, dicatat ketika properti sewaan disewakan kepada penyewa.

Sebagai upaya untuk melacak pendapatan dapat memanfaatkan *software* akuntansi dalam hal mencatat dan melacak pendapatan secara *real time*. Selain itu perusahaan dapat menerapkan dokumentasi dan kontrol yang tepat untuk memverifikasi keakuratan dan validitas transaksi pendapatan.

2. Penerimaan Kas

Tanda terima kas mengacu pada arus kas masuk, kas aktual dari berbagai sumber, seperti penjualan, pinjaman, atau investasi. Kas ini sangat penting untuk memenuhi biaya operasional sehari-hari dan kewajiban keuangan. Untuk proses penerimaan kas, khusus untuk tanda terima penjualan dihasilkan saat pelanggan melakukan pembayaran tunai untuk barang atau jasa. Untuk bukti kwitansi pinjaman tercatat saat uang tunai diterima dari aktivitas peminjaman dan tanda terima investasi didokumentasikan ketika uang tunai diterima dari aktivitas investasi.

Untuk mengontrol penerimaan kas, sebaikan ada pemisahan tugas dimana memisahkan tanggung jawab antara karyawan yang terlibat dalam penanganan dan pencatatan uang tunai. Selanjutnya membuat rekonsiliasi kas reguler dengan membandingkan penerimaan kas dengan transaksi yang tercatat untuk mengidentifikasi perbedaan.

Laporan kas yang dihasilkan dari catatan penerimaan kas akan berguna untuk memproyeksikan penerimaan kas masa depan dimana berguna untuk memastikan likuiditas

yang cukup. Lakukan juga konsolidasi penerimaan kas dari berbagai sumber untuk mengoptimalkan pemanfaatan kas.

8.2.3 Alur sistem informasi akuntansi untuk pendapatan dan penerimaan kas

Aliran informasi akuntansi untuk penerimaan pendapatan dan penerimaan kas melibatkan beberapa tahap, termasuk identifikasi sumber pendapatan, pencatatan transaksi, dan pembuatan laporan keuangan (Sitorus and Rumapea, 2017; Sitorus, Setiyawati and Mappanyuki, 2019). Setiap langkah penting untuk memastikan pelaporan keuangan yang akurat dan andal. Langkah-langkah tersebut adalah:

1. Identifikasi Sumber Pendapatan. Tahap pertama dalam aliran informasi akuntansi untuk penerimaan pendapatan dan kas adalah identifikasi sumber pendapatan. Organisasi perlu mengenali berbagai aliran pendapatan, seperti penjualan, layanan yang diberikan, atau royalti. Identifikasi ini memungkinkan kategorisasi yang tepat dan pelaporan pendapatan yang akurat dalam laporan keuangan (Romney and Steinbart, 2018).
2. Mencatat Transaksi. Setelah sumber pendapatan diidentifikasi, langkah selanjutnya adalah mencatat transaksi yang sesuai. Ini melibatkan pembuatan entri jurnal untuk mendokumentasikan arus masuk uang tunai dan pendapatan yang diperoleh. Transaksi biasanya dicatat dalam buku besar atau jurnal pendapatan khusus, tergantung pada ukuran dan kompleksitas organisasi (Romney and Steinbart, 2018).
3. Pengendalian Internal: Untuk memastikan keakuratan dan integritas informasi akuntansi, organisasi menerapkan pengendalian internal. Kontrol ini termasuk pemisahan tugas, pemantauan rutin, dan rekonsiliasi akun. Misalnya, pemisahan tugas antara individu yang bertanggung jawab untuk pencatatan dan penanganan uang tunai mengurangi risiko penipuan atau kesalahan dalam melaporkan pendapatan dan penerimaan kas (Hall, 2019).

4. Manajemen penerimaan kas adalah komponen penting dari sistem informasi akuntansi. Organisasi harus menetapkan prosedur untuk mengumpulkan, mencatat, dan menyetor uang tunai yang diterima dari pelanggan. Proses ini sering melibatkan penggunaan mesin kasir, sistem *point-of-sale*, atau platform pembayaran elektronik. Setiap penerimaan kas didokumentasikan, dan transaksi yang sesuai dicatat dalam sistem akuntansi (Hall, 2019).
5. Laporan Keuangan: Tahap terakhir dalam aliran informasi akuntansi untuk penerimaan pendapatan dan kas adalah pembuatan laporan keuangan. Laporan-laporan ini, termasuk laporan laba rugi dan neraca, memberikan gambaran yang komprehensif tentang kinerja dan posisi keuangan organisasi. Informasi akuntansi yang akurat dan andal sangat penting bagi pemangku kepentingan, seperti investor, kreditor, dan otoritas pengatur (Romney and Steinbart, 2018).

Aliran informasi akuntansi untuk pendapatan dan penerimaan kas adalah proses penting dalam suatu organisasi. Dengan mengidentifikasi sumber pendapatan secara akurat, mencatat transaksi, menerapkan pengendalian internal, mengelola penerimaan kas, dan menghasilkan laporan keuangan, organisasi memastikan keandalan dan integritas pelaporan keuangan mereka. Memahami aliran informasi akuntansi ini sangat penting bagi organisasi untuk membuat keputusan berdasarkan informasi dan menjaga transparansi dengan pemangku kepentingan.

8.3 Menerapkan Prinsip Pengakuan Pendapatan Yang Sesuai Dengan Standar Akuntansi Yang Relevan

Pengakuan pendapatan adalah aspek penting dari akuntansi keuangan karena menentukan kapan dan bagaimana bisnis mengakui pendapatan dalam laporan keuangan mereka. Di Indonesia, pengakuan pendapatan dipandu oleh Standar Akuntansi Keuangan Indonesia (PSAK), yang selaras dengan Standar Pelaporan Keuangan Internasional (IFRS). Berikut ini adalah

prinsip-prinsip pengakuan pendapatan sesuai dengan standar akuntansi yang relevan di Indonesia dan memberikan contoh untuk menggambarkan penerapannya.

Standar akuntansi yang diterapkan di Indonesia memastikan transparansi, komparabilitas, dan penyediaan informasi yang berguna untuk tujuan pengambilan keputusan.

Prinsip utama pengakuan pendapatan adalah bahwa pendapatan harus diakui ketika ada kemungkinan bahwa manfaat ekonomi akan mengalir ke entitas, dan manfaat ini dapat diukur secara andal. Menurut PSAK 23, pendapatan harus diakui ketika beberapa kriteria dipenuhi antara lain:

1. Risiko dan imbalan kepemilikan yang signifikan telah ditransfer ke pembeli.
2. Entitas tidak mempertahanka. Keterlibatan manajerial yang berkelanjutan atau kontrol yang efektif atas barang yang dijual.
3. Jumlah pendapatan dapat diukur dengan andal.
4. Ada kemungkinan bahwa manfaat ekonomis yang terkait dengan transaksi akan mengalir ke entitas.

Untuk penjualan barang, pengakuan pendapatan atas penjualan barang ditangani oleh PSAK 48. Standar ini menetapkan bahwa pendapatan harus diakui ketika kondisi berikut terpenuhi:

1. Entitas telah mentransfer kepada pembeli risiko dan manfaat kepemilikian yang signifikan.
2. Entitas tidak mempertahankan keterlibatan manajerial yang berkelanjutan atau kontrol yang efektif atas barang yang dijual.
3. Jumlah pendapatan dapat diukur dengan andal.
4. Ada kemungkinan bahwa manfaat ekonomis yang terkait dengan transaksi akan mengalir ke entitas.

PSAK 23 memberikan panduan tentang pengakuan pendapatan untuk pemberian layanan. Pendapatan diakui jika kondisi berikut terpenuhi :

1. Tahap penyelesaian dapat diukur dengan andal.
2. Jumlah pendapatan dapat diukur dengan andal.

3. Ada kemungkinan bahwa manfaat ekonomis yang terkait dengan transaksi akan mengalir ke entitas.

Dalam beberapa kasus, pengakuan pendapatan melibatkan banyak elemen, seperti penjualan barang yang dikombinasikan dengan penyediaan layanan. PSAK 23 memberikan panduan untuk mengakui pendapatan dalam pengaturan tersebut. Pendapatan harus dialokasikan untuk setiap elemen berdasarkan nilai wajar relatifnya dan diakui ketika kondisi berikut terpenuhi:

1. Jumlah pendapatan dapat diukur dengan andal.
2. Ada kemungkinan bahwa manfaat ekonomis yang terkait dengan transaksi akan mengalir ke entitas.

Menerapkan prinsip pengakuan pendapatan sesuai dengan standar akuntansi yang relevan di Indonesia sangat penting untuk memastikan pelaporan keuangan yang akurat dan transparan.

8.4 Menerapkan Pengendalian Internal Yang Efektif Untuk Menjaga Penerimaan Kas Dan Mencegah Penipuan

Pengendalian internal menjadi sangat penting karena menjaga aset perusahaan dan mencegah penipuan atau penyelewengan dana, serta memastikan kepatuhan terhadap persyaratan hukum dan peraturan (Alabdullah and Maryanti, 2021). Adapun beberapa hal penting berikut ini sangat penting dalam menerapkan pengendalian internal yang efektif untuk menjaga penerimaan kas dan mencegah penipuan:

8.4.1 Memahami pentingnya pengendalian internal dalam menjaga penerimaan kas dan mencegah kecurangan.

Internal kontrol memainkan peran penting dalam menjaga penerimaan kas dan mencegah penipuan dengan menetapkan *checks and balances*, mempromosikan akuntabilitas, dan mengurangi peluang untuk kegiatan penipuan.

1. Menetapkan *check and balances*. Internal kontrol menciptakan sistem *checks and balances* yang membantu memastikan keakuratan dan kelengkapan penerimaan kas.

Dengan menerapkan pemisahan tugas, bisnis dapat memastikan bahwa tidak ada satu individu pun yang memiliki kendali penuh atas semua aspek penanganan uang tunai. Misalnya, individu yang berbeda harus bertanggung jawab untuk menerima uang tunai, mencatat transaksi, dan merekonsiliasi akun. Pemisahan tugas ini mengurangi risiko kolusi dan meningkatkan transparansi, sehingga sulit bagi karyawan untuk memanipulasi penerimaan kas untuk keuntungan pribadi.

2. Mempromosikan akuntabilitas. Kontrol internal mempromosikan akuntabilitas dengan mendefinisikan peran dan tanggung jawab secara jelas dalam proses penanganan uang tunai. Ini termasuk menetapkan pedoman dan prosedur yang jelas untuk penanganan uang tunai, serta secara teratur memantau dan meninjau kontrol ini. Dengan meminta pertanggungjawaban karyawan atas tindakan mereka dan memastikan kepatuhan terhadap kontrol yang ditetapkan, organisasi menciptakan budaya integritas dan mencegah kegiatan penipuan.
3. Mengurangi peluang untuk kegiatan penipuan. Internal kontrol yang efektif secara signifikan mengurangi peluang untuk kegiatan penipuan yang terkait dengan penerimaan kas. Misalnya, menerapkan sistem otorisasi dan persetujuan yang kuat serta memastikan bahwa semua transaksi tunai sah dan memiliki dokumentasi yang tepat. Selain itu, audit rutin dan mendadak dapat membantu mengidentifikasi ketidakkonsistenan atau penyimpangan dalam prosedur penanganan uang tunai, sehingga menghalangi potensi penipu.
4. Meningkatkan Deteksi dan Pencegahan Penipuan: Internal kontrol juga memainkan peran penting dalam mendeteksi dan mencegah kegiatan penipuan. Pemantauan rutin dan rekonsiliasi penerimaan kas memungkinkan organisasi untuk mengidentifikasi perbedaan dan menyelidiki potensi penipuan dengan segera. Selain itu, menerapkan solusi teknologi seperti kamera pengintai, prosedur penanganan uang tunai yang aman, dan sistem pembayaran digital dapat

meningkatkan deteksi dan pencegahan penipuan dengan menciptakan lapisan keamanan tambahan.

8.4.2 Mengidentifikasi dan menilai risiko penipuan yang terkait dengan penerimaan kas

Risiko penipuan yang terkait dengan penerimaan kas menimbulkan ancaman signifikan terhadap stabilitas keuangan dan reputasi bisnis (Li *et al.*, 2023). Uang tunai adalah aset yang sangat likuid dan dapat dengan mudah disalahgunakan jika kontrol yang tepat dan langkah-langkah penilaian risiko tidak ada. Beberapa resiko penipuan terkait penerimaan kas adalah sebagai berikut:

1. *Skimming*. Skimming mengacu pada pengalihan kas yang masuk sebelum dicatat dalam sistem akuntansi. Karyawan yang terlibat dalam skimming biasanya memanipulasi uang tunai fisik yang diterima dan menyalahgunakannya untuk keuntungan pribadi. Hal ini dapat menyebabkan kerugian finansial yang signifikan bagi organisasi.
2. *Lapping*. *Lapping* terjadi ketika seorang karyawan dengan sengaja menyalahgunakan uang tunai yang diterima dari satu pelanggan dan menutupinya dengan menerapkan pembayaran dari pelanggan berikutnya. Ini menciptakan siklus misalokasi yang berkelanjutan, sehingga sulit untuk mendeteksi perbedaan dalam penerimaan kas.
3. Penjualan Fiktif. Penjualan fiktif melibatkan pembuatan faktur atau tanda terima palsu untuk mencatat transaksi yang tidak ada. Karyawan yang tidak jujur dapat membuat penjualan untuk mengalihkan uang tunai ke kantong mereka. Jenis penipuan ini sangat sulit dideteksi tanpa kontrol yang tepat.

Penipuan atas penerimaan kas ini akan berdampak pada kerugian dalam beberapa aspek misalnya kerugian finansial. Penerimaan kas palsu dapat menyebabkan kerugian finansial yang besar bagi organisasi. Uang tunai yang disalahgunakan mempengaruhi profitabilitas, arus kas, dan kesehatan keuangan secara keseluruhan. Kerugian ini pada akhirnya dapat membahayakan stabilitas dan kemampuan organisasi untuk

memenuhi kewajiban keuangannya. Kerugian yang lainnya adalah kerusakan reputasi. Kegiatan penipuan yang terkait dengan penerimaan kas dapat sangat merusak reputasi organisasi. Pelanggan dan pemangku kepentingan kehilangan kepercayaan dalam bisnis, mempengaruhi hubungan, pangsa pasar, dan kelangsungan hidup jangka panjang. Membangun kembali reputasi dan memulihkan kepercayaan bisa menjadi proses yang mahal dan memakan waktu.

Melihat dampak buruk dari aktivitas penipuan terhadap penerimaan kas ini, diperlukan tindakan pencegahan untuk mengurangi resiko penipuan dalam penerimaan kas ini. Contoh tindakan pencegahan adalah dengan melakukan pemisahan tugas. Menerapkan sistem checks and balances sangat penting untuk mencegah dan mendeteksi penipuan penerimaan uang tunai. Memisahkan tugas penanganan, pencatatan, dan rekonsiliasi kas di antara karyawan yang berbeda mengurangi risiko kolusi dan meningkatkan akuntabilitas. Selanjutnya lakukan rekonsiliasi penerimaan kas secara teratur dengan transaksi yang tercatat sehingga membantu mengidentifikasi perbedaan dan penyimpangan dengan segera. Proses ini harus melibatkan membandingkan laporan bank, kaset kasir, dan catatan penjualan untuk memastikan akurasi dan mendeteksi potensi penipuan. Selain itu perlu bagi perusahaan untuk menerapkan pengendalian internal. Perusahaan perlu menetapkan prosedur pengendalian internal yang kuat, seperti mewajibkan dua tanda tangan untuk transaksi tunai besar, melakukan audit mendadak, dan menerapkan sistem pengawasan. Hal-hal tersebut dapat bertindak sebagai pencegah dan meningkatkan kemungkinan deteksi penipuan.

8.4.3 Merancang dan menerapkan prosedur pengendalian internal yang efektif untuk mengurangi risiko kecurangan.

Penipuan merupakan ancaman signifikan bagi organisasi dari semua ukuran, membahayakan stabilitas keuangan dan reputasi mereka. Untuk mengatasi risiko ini, organisasi harus menetapkan prosedur pengendalian internal yang kuat (Yang and Chang, 2020). Berikut adalah elemen-elemen kunci dari sistem

pengendalian internal yang efektif dan memberikan langkah-langkah praktis untuk merancang dan menerapkan prosedur tersebut untuk mengurangi risiko kecurangan.

1. Melakukan pengendalian internal yang mengacu pada kebijakan, proses, dan perlindungan yang diberlakukan oleh organisasi untuk memastikan keandalan pelaporan keuangan, kepatuhan terhadap hukum dan peraturan, dan pengamanan aset. Prosedur pengendalian internal yang efektif harus dirancang untuk mencegah, mendeteksi, dan mencegah kecurangan.
2. Pemisahan Tugas: Elemen penting dari pengendalian internal adalah pemisahan tugas, yang memastikan bahwa tidak ada satu individu pun yang memiliki kendali penuh atas transaksi dari inisiasi hingga penyelesaian. Dengan memisahkan tanggung jawab di antara individu yang berbeda, organisasi mengurangi risiko kolusi dan kegiatan yang tidak sah. Misalnya, orang yang bertanggung jawab untuk menyetujui transaksi seharusnya tidak juga bertanggung jawab untuk memulai atau mencatatnya.
3. Dokumentasi dan Otorisasi: Proses dokumentasi dan otorisasi yang tepat sangat penting dalam mencegah dan mendeteksi penipuan. Semua transaksi harus didukung oleh dokumentasi yang sesuai, seperti faktur, tanda terima, dan kontrak. Selain itu, prosedur otorisasi harus ada untuk memastikan bahwa transaksi disetujui oleh individu dengan otoritas yang sesuai. Ini membantu membangun jejak audit dan mencegah kegiatan yang tidak sah.
4. Rekonsiliasi dan Peninjauan Rutin: Rekonsiliasi dan peninjauan catatan keuangan secara teratur sangat penting untuk mengidentifikasi perbedaan atau penyimpangan yang mungkin mengindikasikan penipuan. Rekening bank, saldo kas, catatan persediaan, dan hutang dan piutang harus direkonsiliasi secara teratur untuk memastikan pelaporan yang akurat. Selain itu, telaah berkala atas laporan keuangan oleh manajemen atau auditor internal dapat membantu mendeteksi aktivitas yang mencurigakan.

5. Menerapkan *Kebijakan Whistleblower*: Organisasi harus menetapkan kebijakan *whistleblower* yang jelas dan rahasia yang mendorong karyawan untuk melaporkan setiap dugaan kegiatan penipuan tanpa takut akan pembalasan. Kebijakan ini harus menyediakan beberapa saluran pelaporan, seperti hotline atau sistem pelaporan anonim. Pengaduan whistleblower harus ditanggapi dengan serius dan diselidiki segera untuk mencegah penipuan meningkat.
6. Program Pelatihan dan Kesadaran Reguler: Menciptakan budaya kesadaran dan kewaspadaan sangat penting untuk mencegah penipuan. Organisasi harus melakukan sesi pelatihan reguler untuk mendidik karyawan tentang berbagai jenis penipuan, bendera merah yang harus diperhatikan, dan pentingnya mematuhi prosedur pengendalian internal. Ini membantu memastikan bahwa semua karyawan memahami peran dan tanggung jawab mereka dalam mencegah dan mendeteksi penipuan.

Sistem pengendalian internal yang kuat sangat penting bagi organisasi untuk memastikan keandalan dan integritas pelaporan keuangan mereka, melindungi aset, dan mengurangi potensi risiko. Namun, efektivitas pengendalian internal dapat berkurang seiring waktu karena perubahan dalam proses bisnis, kemajuan teknologi, dan risiko yang berkembang. Untuk mengatasi tantangan ini, organisasi harus menerapkan strategi untuk memantau dan terus meningkatkan sistem pengendalian internal mereka. Dengan secara teratur memantau dan meningkatkan sistem pengendalian internal, organisasi dapat memperkuat praktik manajemen risiko mereka, meningkatkan efisiensi operasional, dan memastikan kepatuhan terhadap peraturan dan standar.

Dengan mengimplementasikan beberapa strategi berikut diharapkan perusahaan dapat memperkuat praktik manajemen risiko, meningkatkan efisiensi operasional dan memastikan kepatuhan terhadap peraturan dan standar. Strategi-strategi tersebut antara lain adalah penilaian risiko regular, pemantauan berkelanjutan, penilaian mandiri terkait pengendalian internal,

pemisahan tugas, program pelatihan dan kesadaran, dan audit eksternal.

8.4.4 Menerapkan prinsip-prinsip etika dan standar professional dalam konteks prosedur pengendalian internal.

Prinsip-prinsip etika dan standar profesional berikut harus diterapkan dalam konteks prosedur pengendalian internal. Integritas dan nilai-nilai etika merupakan elemen penting dari lingkungan pengendalian, yang mempengaruhi desain, administrasi, dan pemantauan komponen pengendalian internal lainnya (PCAOB, 2007). Kontrol lingkrolungan juga menentukan nada organisasi karena mempengaruhi kesadaran kontrol atas orang-orangnya. Bisa jadi tindakan manajemen untuk menghilangkan atau mengurangi insentif mendorong setiap personel untuk terlibat dalam tindakan tidak jujur, illegal, atau tidak etis sangat penting. Kebijakan yang membahas pengendalian bisnis dan praktik manajemen risiko yang signifikan harus ditetapkan.

Auditor harus menggunakan kehati-hatian profesional, termasuk skeptisisme profesional, ketika melakukan audit atas pengendalian internal atas pelaporan keuangan (PCAOB, 2016).

8.5 Menganalisis dan Menafsirkan Laporan Keuangan Yang Terkait Dengan Penerimaan Kas

Laporan keuangan berperan penting dalam menilai kesehatan keuangan dan kinerja perusahaan. Salah satu laporan tersebut adalah laporan arus kas yang memberikan gambaran yang bermakna tentang penerimaan kas perusahaan yang merupakan arus kas masuk dari kegiatan operasi, investasi dan pendanaan. Para pemangku kepentingan perlu menganalisis dan menafsirkan pernyataan-pernyataan dalam laporan arus kas untuk memahami likuiditas, profitabilitas dan stabilitas keuangan perusahaan secara keseluruhan.

Penerimaan kas biasanya dalam bentuk uang tunai, cek atau transfer elektronik dari berbagai sumber seperti pelanggan, investor

dan kreditor. Dalam laporan arus kas penerimaan kas ini dapat dibagi dalam tiga aktivitas utama yakni:

1. Aktivitas Operasi. Penerimaan kas dari aktivitas operasi ini adalah bersumber dari pendapatan atas penjualan barang atau jasa, bunga yang diterima atas pinjaman dan dividen yang diterima dari investasi. Nilai kas dari kategori aktivitas operasi ini menolong perusahaan menilai kemampuan perusahaan untuk menghasilkan uang tunai dari operasi intinya.
2. Aktivitas Investasi. Aktivitas investasi ini dapat berupa penjualan aset seperti pabrik, peralatan, property atau dari penjualan investasi. Akibat aktivitas investasi ini perusahaan menerima kas. Penting untuk mengevaluasi penerimaan kas dari aktivitas investasi ini untuk memahami keputusan alokasi modal perusahaan dan kemampuannya untuk menghasilkan pengembalian investasi.
3. Aktivitas Pendanaan. Kas yang diterima dari aktivitas pendanaan diperoleh dari pemegang saham atau kreditor seperti hasil dari penerbitan ekuitas atau utang. Menganalisis penerimaan ini membantu menentukan kemampuan perusahaan untuk menarik modal dan mengelola struktur modalnya.

8.6 Mengembangkan Strategi Untuk Mengoptimalkan Pengumpulan Pendapatan dan Manajemen Kas

Mengembangkan strategi untuk mengoptimalkan pengumpulan pendapatan dan manajemen kas sangat penting bagi bisnis untuk menjaga kesehatan keuangan dan profitabilitas. Berikut adalah beberapa strategi dan tips yang terbukti untuk mengoptimalkan pengumpulan pendapatan dan manajemen kas:

1. Lakukan audit sistem saat ini. Cara tercepat untuk mengembangkan rencana kas yang efektif dan dapat dieksekusi adalah dengan mengaudi sistem anda saat ini. Tentukan dulu dan prioritaskan area yang perlu dilakukan perbaikan.

2. Kelola piutang dengan bijak. Manajemen kas yang efektif akan melibatkan pengelolaan pendapatan dan pengeluaran yang mengalir masuk dan keluar dari perusahaan. Salah satu aspek terpenting dalam manajemen kas adalah mengelola piutang. Perusahaan dapat meningkatkan profitabilitas mereka dengan mempersingkat waktu pengumpulan, mengurangi biaya operasional, dan memperlambat pencairan uang tunai.
3. Dapatkan bayaran di muka: Salah satu cara untuk meningkatkan arus kas adalah dengan dibayar di muka. Ini dapat dilakukan dengan menyiapkan punggawa atau memiliki tenaga penjualan yang bertanggung jawab atas proses pengumpulan.
4. Mengotomatiskan koleksi: Mengotomatiskan koleksi dapat membantu bisnis meningkatkan arus kas mereka. Dengan menggunakan perangkat lunak yang mempercepat waktu yang dibutuhkan untuk mengumpulkan uang tunai, bisnis dapat mengumpulkan pembayaran lebih cepat dan lebih efisien.
5. Digitalisasi proses bisnis: Digitalisasi proses bisnis dapat membantu bisnis meningkatkan manajemen kas mereka. Dengan menggunakan pembayaran elektronik untuk pembayaran tagihan, bisnis dapat merampingkan proses pembayaran mereka dan mengurangi waktu yang diperlukan untuk mengumpulkan pembayaran.
6. Meningkatkan budaya kas: Setiap bisnis harus menetapkan praktik terbaik manajemen kas untuk menjaga operasi berjalan lancar dan pelanggan senang. Meningkatkan budaya kas melibatkan menetapkan, berkomunikasi, dan menerapkan kebijakan standar di seluruh organisasi. Kebijakan manajemen kas harus fokus pada penganggaran, peramalan, dan pembiayaan dan menunjukkan bagaimana menangani kegiatan sehari-hari seperti pengumpulan, pengadaan / pemesanan, dan pembayaran.
7. Negosiasikan persyaratan yang lebih baik: Bisnis dapat menegosiasikan persyaratan yang lebih baik dengan vendor mereka untuk meningkatkan arus kas mereka. Ini dapat

dilakukan dengan menegosiasikan persyaratan pembayaran yang lebih lama atau diskon untuk pembayaran awal.

8. Meningkatkan prosedur faktur: Meningkatkan prosedur faktur dapat membantu bisnis mengumpulkan pembayaran lebih cepat. Ini dapat dilakukan dengan mengirimkan faktur segera, menindaklanjuti pembayaran yang terlambat, dan memudahkan pelanggan untuk membayar.
9. Bereksperimen dengan penetapan harga: Bereksperimen dengan penetapan harga dapat membantu bisnis meningkatkan arus kas mereka. Dengan menaikkan harga, bisnis dapat meningkatkan pendapatan mereka dan meningkatkan profitabilitas mereka.
10. Pertahankan saldo kas yang optimal: Mempertahankan saldo kas yang optimal sangat penting bagi bisnis untuk mengelola kas mereka secara efektif. Uang tunai yang tidak memadai dapat memperlambat produksi, sementara uang tunai yang berlebihan dapat berubah menjadi mahal. Oleh karena itu, bisnis harus menekankan pada menjaga keseimbangan kas yang optimal.

Dengan menerapkan strategi ini, bisnis dapat mengoptimalkan pengumpulan pendapatan dan manajemen kas mereka, meningkatkan kesehatan keuangan mereka, dan meningkatkan profitabilitas mereka.

DAFTAR PUSTAKA

Alabdullah, T.T. and Maryanti, E. 2021. 'Internal control mechanisms in accounting, management,

and Economy: A review of the literature and suggestions of new investigations', *International Journal of Business and Management Invention*, 10(9), pp. 8–12. Available at: https://doi.org/10.35629/8028-1009020812.

Hall, J. 2019. *Accounting Information Systems*. Accounting Information Systems.

Karamoy, R. 2013. 'Evaluasi pelaksanaan sistem dan prosedur penerimaan kas di dinas pendapatan

kota Manado', *Jurnal EMBA*, 1(3), pp. 939–948.

Lasmana, Y., Muttaqin, G. and Yunia, D. 2022. 'Cash receipt and disbursement system on micro small

and medium enterprises', *Journal of Applied Business, Taxation and Economics Research*, 1(3), pp. 302–310. Available at: https://doi.org/10.54408/jabter.v1i3.54.

Li, J. *et al.* 2023. 'Tracking down financial statement fraud by analyzing the supplier-customer

relationship network', *Computers & Industrial Engineering*, 178(1).

Needles, B., Powers, M. and Crosson, S. 2017. *Financial and Managerial Accounting (11th ed.)*.

Cengage Learning.

PCAOB. 2007. *Internal Control Components*, *American Institute of Certified Public Accountants, Inc*.

PCAOB. 2016. *An audit of internal control over financial reporting that is integrated with an audit of*

financial statements, *Public Company Accounting*.

Pelealu, D. and Sabijono, H. 2015. 'Analysis of the application of accounting information systems of

cash receipt on the RSIA Kasih Ibu Manado', *Jurnal EMBA*, 3(2), pp. 315–325.

Rittenberg, L. and Johnstone, K. 2017. *Auditing: A Business Risk Approach 10th ed*. Cengage Learning.

Romney, M.B. and Steinbart, P.J. 2018. *Accounting information systems*. New York: Pearson.

Saputra, S., Widagdo, S. and Rachmawati, L. 2023. 'Analysis of accounting information system for
receipt, cash disbursement, purchasing and inventory for internal control', *TGO Journal of Education, Science and Technology*, 1(2), pp. 205–211.
Sitorus, E.T., Setiyawati, H. and Mappanyuki, R. 2019. 'The Effectiveness of The Internal Control
System on The Quality of Financial Statements with The Implementation of Internal Audits as A Moderation Variabel', *International Conference on Rural Development and Entrepreneurship 2019: Enhancing Small Business and Rural Development Toward Industrial Revolution 4.0*, 5.
Sitorus, S. and Rumapea, M. 2017. 'Sistem informasi akuntansi pendapatan dan penerimaan kas
pada PT. Telkom Medan', *Jurnal Manajemen Informatika & Komputerisasi Akuntansi*, 1(1), pp. 1–9.
Vara-miguel, A. *et al.* 2021. 'Funding sustainable online news : sources of revenue in digital-native
and traditional media in Spain', *Sustainability*, 13(1), pp. 1–17. Available at: https://doi.org/https://doi.org/10.3390/su132011328.
Yang, C.-H. and Chang, L.-K. 2020. 'Developing strategy mar for forensic accounting with fraud risk
Management: an integrated balanced scorecard based decision model', *Evaluation and Program Planning*, 80(1), pp. 1–10.

BIODATA PENULIS

Agus Tina,S.Ak.,M.Ak.,CAP.,CTT.,CPTT.,BKP.
Dosen Program Studi Akuntansi
Fakultas Ekonomi Universitas Prima Indonesia

Penulis lahir di Belawan tanggal 28 Agustus 1983. Penulis adalah dosen tetap pada Program Studi Akuntansi Fakultas Ekonomi, Universitas Prima Indonesia. Menyelesaikan pendidikan S1 pada Jurusan Akuntansi dan melanjutkan S2 pada Jurusan Akuntansi. Saat ini penulis juga berprofesi sebagai konsultan pajak dan telah memiliki ijin praktik konsultan pajak.

BIODATA PENULIS

Ade Onny Siagian, M.M., M.H., M.A.P., M.I.Kom.
Dosen Program Studi Akuntansi
Fakultas Ekonomi dan Bisnis, Universitas Bina Sarana Informatika.

Penulis lahir di Mojokerto (1978), Saat ini Jabatan Lektor mengajar di Universitas Swasta, Fakultas Ekonomi, jenjang pendidikan S1 Fakultas Hukum (2003), S2 Magister Manajemen (2010), S2 Magister Ilmu Hukum (2018), Magister Ilmu Administrasi Publik (2019) dan S2 Magister Ilmu Komunikasi (2019) mendapat gelar wisudawan terbaik (Cum Laude), giat melakukan penelitian, dan aktif dalam bidang menulis buku, Google Scholar ID: qyMWX6cAAAAJ; Sinta ID: 6694707; Orcid. ID: https://orcid.org/0000-0002-9701- 9546; dan Scopus ID: 57219985838.

BIODATA PENULIS

Denny Rakhmad Widi Ashari, S.AP, M.E.
Dosen Program Studi Perbankan Syariah dan CTO klikada.com
Fakultas Agama Islam Universitas Nahdlatul Ulama Blitar

Penulis lahir di Tulungagung pada tanggal 13 Juli 1984, saat ini menjalani karier dalam bidang pendidikan dan *digital enterpreneur*. Ia menjabat sebagai dosen tetap di Program Studi Perbankan Syariah, Fakultas Agama Islam, Universitas Nahdlatul Ulama Blitar, dan juga memegang posisi penting sebagai *Chief Technology Officer* di klikada.com, sebuah perusahaan yang bergerak dalam *digital marketing agency*.

Perusahaan ini fokus pada berbagai aspek pembuatan situs web, mulai dari profil perusahaan, toko *online*, sistem manajemen pembelajaran, penjualan *domain*, optimasi *SEO*, pemeliharaan situs *web*, hingga penulisan konten. Selain itu, juga berperan dalam agensi pemasangan iklan di platform seperti *Google Ads*, *Facebook Ads*, dan *Instagram Ads*.

Riwayat pendidikan penulis menunjukkan prestasi yang mengagumkan, dengan menyelesaikan gelar S1 di Jurusan Administrasi Publik, Fakultas Ilmu Administrasi Universitas Brawijaya Malang dalam waktu singkat, hanya 3,5 tahun. Selanjutnya, penulis melanjutkan studi S2 di Jurusan Ekonomi Syariah di Program Pascasarjana Institut Agama Islam Tulungagung, dan berhasil meraih predikat lulusan terbaik.

Tak hanya berperan dalam dunia akademik, penulis juga aktif sebagai juri dalam berbagai kompetisi dan menjadi

narasumber dalam seminar-seminar di berbagai kampus. Tidak hanya itu, penulis juga menjaga hobi sebagai pemrogram ("*kuli koding*") dan tetap terlibat dalam dunia pemrograman web, bahkan ketika mengejar karier sebagai *CTO* di perusahaan *digital marketing agency* di luar dunia kampus.

Penulis mempunyai pengalaman yang luas dalam industri keuangan dan perbankan, dengan karier selama 10 tahun di berbagai sektor keuangan dan perbankan, baik di perbankan konvensional maupun perbankan syariah. Gabungan pengalaman ini memberikan penulis keahlian yang istimewa dalam bidang perbankan, terutama perbankan syariah, yang sesuai dengan pendidikan akademiknya.

Penulis memiliki fokus yang kuat dalam berbagai bidang, seperti perbankan, ekonomi syariah, pemasaran *digital*, pelayanan publik, dan pemrograman web. Jika Anda tertarik untuk berdiskusi atau berbagi pengetahuan seputar topik-topik ini, penulis dapat dihubungi melalui WhatsApp di tautan berikut https://go.klikada.com/e-card (di luar jam kerja), melalui telepon di 082232267100 (selama jam kerja), atau melalui email di masden@klikada.com (di luar jam kerja) dan drwashari@unublitar.ac.id (selama jam kerja). Semangat !!!.

BIODATA PENULIS

Angga Aditya Permana, S.Kom., M.Kom
Dosen Program Studi Informatika
Universitas Multimedia Nusantara

Angga Aditya Permana (lahir pada Desember 1989 di Jakarta) seorang dosen full time di bidang Computer Science pada Universitas Multimedia Nusantara sejak tahun 2021, fokus penelitian pada kriptografi, steganografi serta keamanan computer, namun pada tahun 2021 sedang mendalami topik bioinformatika dan network science. Angga juga memiliki hobi yaitu touring dan juga bermain bulutangkis, saat ini sedang menjadi mahasiswa program doctoral pada IPB University. Memulai karir pertama kali sebagai Network Enginner tahun 2011 dan memulai profesinya sebagai dosen pada 2013 di kampus swasta yang ada di Jakarta, pernah juga mengajar di kampus negri yang berada di Jakarta dan Tangerang, juga pernah di undang menjadi dosen tamu untuk mengenalkan Bioinformatika di kampus negeri di Jakarta. Terimakasih..

BIODATA PENULIS

Ketut Tanti Kustina, SE, MM,Ak,CA,CSRA.
Dosen Program Studi Akuntansi
Fakultas Ekonomi dan Bisnis
Universitas Pendidikan Nasional (Undiknas) Denpasar

Penulis lahir di Bogor tanggal 16 Nopember 1981. Penulis adalah dosen tetap pada Program Akuntansi Fakultas Ekonomi dan Bisnis, Universitas Pendidikan Nasional (Undiknas) Denpasar. Menyelesaikan pendidikan S1 ditempuh pada Jurusan Akuntansi Fakultas Ekonomi Universitas Udayana, lulus pada tahun 2004. Selanjutnya penulis melanjutkan studi pada Program Studi Magister Manajemen Program Pascasarjana Universitas Udayana dan meraih gelar magister pada tahun 2010. Penulis merupakan dosen pada LLDIKTI Wilayah VIII sejak tahun 2005 dpk pada Fakultas Ekonomi Universitas Samawa Sumbawa Besar dan pada Program Studi Akuntansi Fakultas Ekonomi dan Bisnis Universitas Pendidikan Nasional Denpasar sejak tahun 2011 hingga saat ini. Penulis mendapatkan *Certified Sustainability Specialist* (CSRS) dan *Certified Sustainability Assurer* (CSRA) Certificate dari National Center for Sustainability Reporting (NCSR) sejak tahun 2019. Pada tahun 2021 penulis melanjutkan Studi Strata 3 (S3) pada Program Studi Doktor Manajemen di Fakultas Ekonomi dan Bisnis Universitas Udayana.

BIODATA PENULIS

Nano Suyatna,SE.,Ak.,M.E.,M.Kom.,CPA.,ASEAN CPA
Dosen Departemen Komputerisasi Akuntansi
Fakultas Komputer Universitas Ma'soem

Penulis lahir di Sumedang tanggal 03 Desember 1964. Penulis adalah dosen tetap pada Departemen Komputerisasi Akuntansi, Fakultas Komputer, Universitas Ma'soem. Menyelesaikan pendidikan S1 pada Jurusan Akuntansi dan melanjutkan S2 pada Jurusan Magister Komputer dan Magister Ekonomi Islam. Penulis menekuni bidang Akuntansi, Sistem Informasi Akuntansi, Auditing dan Audit Teknologi Informasi. Penulis berprofesi juga sebagai Akuntan Publik dan Pengembang Aplikasi.

BIODATA PENULIS

Ika Prayanthi, SE, MM, Ak
Dosen Program Studi Akuntansi
Fakultas Ekonomi dan Bisnis Universitas Klabat

Lahir di Airmadidi pada tanggal 25 Juni 1986. Profesi pekerjaan penulis adalah sebagai dosen pada program studi akuntansi di Fakultas Ekonomi dan Bisnis Universitas Klabat. Saat penyusunan buku ini, penulis terdaftar sebagai mahasiswa pada Program Studi Doktor Ilmu Manajemen konsentrasi Akuntansi Keuangan di Fakultas Ekonomi dan Bisnis Universitas Sam Ratulangi. Menyelesaikan Pendidikan Magister Manajemen konsentrasi keuangan di Universitas Klabat tahun 2011 serta Pendidikan Sarjana Ekonomi program studi akuntansi di Universitas Klabat tahun 2007. Penulis aktif dalam beberapa penulisan ilmiah yang dipulikasikan baik dalam level nasional maupun internasional sejak tahun 2011 hingga tahun 2022. Penulis juga adalah reviewer aktif untuk artikel penelitian baik nasional maupun internasional.