

BAB IV

PEMBAHASAN

4.1 Kronologi Kasus Secara Singkat

Kasus *fraud* terungkap di divisi teknisi, di mana para teknisi yang memiliki tanggung jawab untuk bertemu dengan pelanggan diwajibkan menjalankan kegiatan hiburan, seperti makan bersama, sebagai bagian dari upaya menjaga hubungan baik dengan pelanggan. Perusahaan menyediakan anggaran khusus untuk keperluan ini. Namun, beberapa teknisi memanfaatkan kesempatan tersebut dengan memanipulasi bukti transaksi atau bon. Mereka melaporkan pengeluaran hiburan sesuai dengan anggaran yang ditentukan, meskipun sebenarnya hanya menggunakan separuh dari dana tersebut, sementara sisanya disalahgunakan untuk kepentingan pribadi.

Perusahaan menunjukkan kelemahan dalam pengelolaan anggaran hiburan yang diberikan kepada teknisi. Pertama, jika pertemuan dengan vendor bersifat resmi, seharusnya dapat dilakukan di kantor, sehingga pengeluaran tambahan seperti anggaran hiburan dapat dihindari. Mengadakan pertemuan di luar kantor cenderung menimbulkan biaya yang tidak memiliki pencatatan khususnya, sering kali dimasukkan ke dalam akun "biaya lain-lain" yang rentan terhadap *fraud*. Kedua, jika kegiatan yang dimaksud terkait pengadaan bisnis, seharusnya peran tersebut dijalankan oleh bagian *sales*, bukan teknisi. Dengan demikian, perusahaan tidak perlu mengeluarkan anggaran hiburan untuk pertemuan tersebut, karena pengelolaan hubungan dengan vendor dapat dilakukan oleh bagian yang lebih relevan.

Perusahaan juga menghadapi kelemahan mendasar dalam berbagai aspek sistem pengendalian internal, termasuk lingkungan pengendalian, penilaian risiko, kegiatan pengendalian, pengelolaan informasi, serta pemantauan dan evaluasi. Kekurangan ini disebabkan oleh tidak adanya struktur pengendalian yang memadai, kurangnya identifikasi dan mitigasi risiko, pelaksanaan kegiatan pengendalian yang belum optimal, manajemen informasi yang tidak efisien, serta lemahnya mekanisme pemantauan dan evaluasi. Situasi ini berpotensi mengganggu efisiensi

operasional perusahaan dan meningkatkan risiko baik dalam aspek operasional maupun keuangan.

4.2 Defisiensi *Control Environment*

4.2.1 Integritas dan Nilai Etika

Kasus ini mencerminkan lemahnya penerapan "*Tone at the Top*" dan sistem pengendalian internal yang tidak efektif. Menurut Wells (2004), budaya etika dalam organisasi dimulai dari manajemen senior, dan lemahnya komitmen terhadap nilai-nilai tersebut membuka peluang terjadinya fraud. Hal ini semakin parah arena kurangnya pengawasan ketat pada pengeluaran, sebagaimana dijelaskan oleh Albrecht et al. (2018), yang menyatakan bahwa *fraud* cenderung terjadi di area dengan pengawasan yang lemah. Dalam kasus ini, prosedur pengajuan dana *entertainment* tidak diperiksa secara mendalam, sehingga manipulasi bon oleh teknisi dapat terjadi tanpa deteksi. Selain itu, Kranacher (2020) menekankan bahwa kesenjangan pemahaman terhadap standar internal perusahaan sering kali menciptakan celah yang dapat dieksploitasi, terutama dalam proses pengeluaran.

Kasus ini menyoroti lemahnya pengendalian internal dan kurangnya komitmen terhadap integritas dalam proses pengelolaan anggaran entertain. Albrecht et al. (2018) menjelaskan bahwa *fraud* sering terjadi pada area dengan pengawasan yang minim, di mana laporan pengeluaran teknisi hanya diperiksa secara administratif tanpa verifikasi yang mendalam. Situasi ini diperburuk oleh lemahnya penegakan etika yang memungkinkan manipulasi bon berjalan tanpa konsekuensi yang jelas. ISO 31000 (2018) menyarankan bahwa risiko seperti ini dapat diminimalkan dengan pengawasan ketat dan mekanisme pelaporan transparan yang memastikan setiap pengeluaran sesuai dengan peruntukannya. Lebih jauh, Kranacher (2020) menyatakan bahwa lemahnya pengawasan manajerial dapat memberikan sinyal kepada karyawan bahwa tindakan serupa akan ditoleransi. Kasus ini menjadi refleksi bahwa tanpa penguatan nilai integritas dan implementasi pengendalian yang efektif, potensi *fraud* akan terus berkembang dan merugikan perusahaan secara finansial maupun reputasi.

Sehingga, salah satu problematika yang akan ditinjau dalam elemen ini adalah kurangnya penekanan nilai etika yang mungkin seharusnya telah dilakukan oleh pihak *board of directors*. Belajar dari kasus Enron dan WorldCom, keduanya merupakan skandal keuangan besar yang terjadi akibat lemahnya pengawasan etika di tingkat direksi. Pada 2001, Enron, sebuah perusahaan energi di Amerika Serikat, mengalami kebangkrutan setelah diketahui telah memanipulasi laporan keuangan dengan bantuan akuntan mereka, Arthur Andersen, untuk menyembunyikan utang perusahaan. Kasus ini melibatkan para eksekutif senior seperti Kenneth Lay dan Jeffrey Skilling, yang mengeksploitasi celah akuntansi demi keuntungan pribadi. Sementara itu, pada 2002, WorldCom, salah satu perusahaan telekomunikasi terbesar di AS, juga terlibat dalam skandal *fraud* setelah CEO Bernard Ebbers dan CFO Scott Sullivan memalsukan laporan keuangan dengan menyembunyikan biaya operasional lebih dari \$3,8 miliar. Jones (2011) menyatakan bahwa kedua kasus ini menyoroti bahaya dari ketidakhadiran pengawasan yang efektif oleh *board of directors* terhadap praktik akuntansi yang kreatif dan tidak etis. Kegagalan ini menunjukkan bahwa tanpa pengawasan yang kuat dan konsisten, manipulasi dapat terjadi pada berbagai level organisasi.

4.2.2 Tanggung Jawab Pengawasan

Kasus *fraud* yang terjadi di divisi teknis mencerminkan kelemahan pada pengawasan internal, khususnya dalam proses pengelolaan dana entertain. COSO (2013) menekankan pentingnya *control environment* yang kuat, di mana kebijakan dan prosedur dirancang untuk mencegah peluang kecurangan. Dalam kasus ini, tidak adanya pengawasan yang memadai memungkinkan teknis memanipulasi bukti transaksi dengan melaporkan pengeluaran entertain yang melebihi realisasi sesungguhnya. Hal ini menunjukkan bahwa sistem kontrol internal yang ada belum diterapkan secara efektif, terutama pada area yang rentan terhadap penyalahgunaan seperti pengelolaan anggaran.

Kurangnya pemisahan tugas atau *segregation of duties* menjadi salah satu penyebab utama dalam kasus ini. Menurut Wells (2004), sistem pengendalian internal yang efektif harus melibatkan pemisahan fungsi antara otorisasi, pencatatan, dan pengawasan. Dalam kasus ini, teknis yang mengajukan dana

entertain tidak diawasi secara ketat oleh pihak yang independen, sehingga mereka dapat memanipulasi laporan pengeluaran tanpa terdeteksi. Hal ini diperburuk dengan lemahnya proses verifikasi dan kurangnya mekanisme pelaporan transparan, sebagaimana dijelaskan oleh Kranacher (2020), bahwa tidak adanya pengawasan independen meningkatkan risiko penyalahgunaan anggaran dan *fraud* dalam organisasi.

Poin penting dalam kasus ini adalah tidak adanya mekanisme kontrol yang memadai untuk memastikan bahwa dana digunakan sesuai dengan peruntukannya. COSO (2017) menyoroti pentingnya pengawasan berbasis risiko dalam *Enterprise Risk Management Framework* untuk mendeteksi dan mencegah kecurangan secara proaktif. Selain itu, Albrecht et al. (2018) menegaskan bahwa *fraud* sering kali terjadi pada area yang kurang diawasi, seperti pengelolaan anggaran entertain ini. Ketidakhadiran pengawasan yang tegas dan independen mengurangi efektivitas kontrol internal, yang dalam kasus ini membuka peluang bagi teknisi untuk menyalahgunakan anggaran. Menurut Arens (2023), pemisahan tugas yang jelas sangat penting dalam pengendalian keuangan untuk meminimalkan risiko manipulasi, dimana setiap proses harus diawasi oleh pihak yang independen untuk menjaga integritas sistem pengelolaan keuangan.

4.2.3 Struktur, Wewenang, dan Tanggung Jawab

Kasus ini menunjukkan kelemahan dalam pengendalian internal perusahaan, meskipun telah mengimplementasikan sistem ERP (SAP) untuk mengelola sumber daya dan transaksi secara digital. Teknisi yang bertugas bertemu dengan pelanggan memanfaatkan celah dalam pengawasan dengan memanipulasi bukti transaksi pengeluaran entertain. Mereka melaporkan penggunaan anggaran sesuai dengan batas yang ditetapkan perusahaan, tetapi kenyataannya hanya setengah dari anggaran tersebut yang digunakan untuk tujuan sebenarnya, sedangkan sisanya disalahgunakan untuk kepentingan pribadi. COSO (2013) menekankan pentingnya pengawasan yang memadai dan pemisahan tanggung jawab dalam sistem pengendalian internal untuk mencegah penyalahgunaan. Hal ini diperkuat oleh Wells (2004), yang menyatakan bahwa pengendalian internal yang lemah dapat menciptakan peluang besar untuk manipulasi transaksi, terutama

ketika sistem tidak dilengkapi dengan proses verifikasi yang ketat. Selain itu, Albrecht et al. (2018) juga menyoroti pentingnya “*segregation of duties*” sebagai kontrol utama dalam menjaga integritas transaksi.

Meskipun ERP dirancang untuk meningkatkan efisiensi, kelemahan implementasi dan kurangnya pengawasan independen memberikan celah bagi kecurangan. Teknisi dapat mengajukan laporan pengeluaran tanpa adanya proses verifikasi yang kuat sehingga manipulasi bon tidak terdeteksi. Hal ini sejalan dengan temuan Kranacher (2020), yang menunjukkan bahwa kurangnya pengawasan independen memungkinkan manipulasi tanpa deteksi. Selain itu, ISO (2018) menegaskan pentingnya pengelolaan risiko yang terintegrasi dengan pengawasan memadai pada setiap tingkat proses. Dalam kasus ini, celah dalam sistem ERP dan ketidaktegasan pengawasan menciptakan situasi di mana laporan pengeluaran entertain dapat dimanipulasi tanpa kontrol yang efektif, seperti ditegaskan Arens (2023), bahwa pemisahan tugas dalam proses transaksi adalah komponen penting untuk meminimalkan risiko *fraud*.

4.2.4 Komitmen Terhadap Kompetensi

Perusahaan telah menyediakan pelatihan untuk meningkatkan kemampuan karyawan, namun pelaksanaan pelatihan tersebut masih terbatas dan tidak merata di seluruh organisasi. Akibatnya, beberapa karyawan tidak sepenuhnya memahami kebijakan dan prosedur yang berlaku, terutama terkait pengelolaan pengeluaran dan pengajuan dana. Seperti dijelaskan oleh Albrecht et al. (2018), lemahnya kesadaran terhadap prosedur pengendalian internal dapat meningkatkan potensi kecurangan jika tidak ada pelatihan yang memadai. Selain itu, COSO (2013) menekankan pentingnya pengendalian berbasis kompetensi sebagai bagian dari sistem internal yang efektif untuk memitigasi risiko. Kurangnya kejelasan dalam proses seleksi dan pengembangan karyawan juga menjadi kelemahan dalam sistem manajemen risiko perusahaan, di mana Arens (2023) menyoroti perlunya pendekatan terstruktur untuk memastikan bahwa individu yang rawan melanggar kebijakan dapat teridentifikasi dan dikelola dengan baik.

Dalam kasus ini, meskipun ada kebijakan dan prosedur yang dirancang untuk menjaga integritas pengelolaan dana, kurangnya pelatihan yang merata mengarah pada pemanfaatan celah oleh teknisi. Mereka memanipulasi pengajuan dana entertain dengan memalsukan bukti transaksi atau bon, melaporkan pengeluaran sesuai anggaran meskipun hanya sebagian yang benar-benar digunakan untuk tujuan yang dimaksud. Ketidakjelasan jalur pelaporan dan lemahnya pengawasan lebih lanjut memperburuk situasi, memungkinkan manipulasi berlangsung tanpa kontrol yang memadai. Hal ini sejalan dengan temuan Skalak (2006), yang menegaskan pentingnya pelatihan yang efektif dan penerapan kebijakan dengan konsisten untuk meminimalkan risiko kecurangan. Selain itu, ISO (2018) menegaskan bahwa pemahaman mendalam terhadap prosedur organisasi adalah elemen kunci dalam menciptakan sistem yang tangguh terhadap potensi penyalahgunaan wewenang.

4.2.5 Akuntabilitas

Penegakan akuntabilitas di perusahaan seharusnya dilakukan dengan sistem pelaporan yang jelas kepada atasan dan evaluasi kinerja berbasis ukuran yang objektif. Meskipun perusahaan memiliki sistem dasar untuk penilaian kinerja, implementasinya sering kali tidak optimal dalam mencegah penyalahgunaan. Albrecht et al. (2018) menekankan bahwa tanpa pengawasan yang memadai, sulit mendeteksi tanda-tanda awal kecurangan. Pada kasus ini, proses evaluasi kinerja lebih mengandalkan kuisioner atau penilaian tidak langsung yang kurang efektif dalam mencerminkan potensi risiko individu. Wells (2004) menyatakan bahwa sistem penilaian yang tidak menyeluruh dapat menciptakan celah bagi karyawan untuk menyalahgunakan wewenang. Sistem pengukuran yang tidak spesifik dan kurangnya pengawasan langsung menurunkan efektivitas akuntabilitas, sehingga sulit bagi organisasi untuk mengidentifikasi kesenjangan antara kinerja yang diharapkan dan yang dicapai. Kaplan dan Norton (1996) menegaskan bahwa pengukuran yang berorientasi pada hasil akan membantu organisasi mengenali masalah lebih dini dan mengambil tindakan korektif dengan cepat.

Dalam praktiknya, hal ini terlihat pada kasus manipulasi pengeluaran entertain oleh teknisi. Ketika evaluasi kinerja hanya bergantung pada kuisioner

tanpa pemantauan langsung, teknisi dapat dengan mudah melaporkan pengeluaran entertain sesuai anggaran meskipun hanya menggunakan setengahnya, dan sisanya disalahgunakan untuk kepentingan pribadi. Kurangnya verifikasi bukti transaksi serta pengawasan terhadap pelaporan menciptakan celah untuk penyalahgunaan. Kranacher (2020) menyoroti bahwa akuntabilitas yang lemah akan mempermudah terjadi kecurangan, sementara ISO 31000 (2018) menegaskan perlu pengelolaan risiko berbasis proses untuk meningkatkan deteksi dan pencegahan penyalahgunaan. Dengan sistem evaluasi dan pengawasan yang tidak memadai, organisasi kehilangan kesempatan untuk mendeteksi manipulasi sejak dini, yang berpotensi menyebabkan kerugian signifikan bagi perusahaan.

4.3 Defisiensi *Risk Assessment*

4.3.1 Tujuan yang Sesuai

Tujuan yang jelas dan terstruktur merupakan elemen kunci dalam pengelolaan perusahaan yang efektif. Dalam konteks ini, perusahaan telah menetapkan tujuan untuk mengelola pengeluaran operasional secara efisien. Namun, seperti yang dijelaskan oleh Wells (2004), tanpa prosedur implementasi yang rinci, tujuan tersebut hanya akan menjadi ambisi tanpa hasil nyata. Albrecht et al. (2018) juga menyoroti bahwa ketidakjelasan dalam prosedur implementasi dan pengawasan dapat membuka peluang bagi penyalahgunaan sumber daya. Dalam kasus ini, meskipun perusahaan memiliki kebijakan yang mengatur alokasi anggaran entertain untuk teknisi, prosedur pengelolaan dan verifikasi biaya yang kurang komprehensif menciptakan celah bagi manipulasi anggaran. Tanpa pengawasan yang rinci dan sistematis, risiko penyalahgunaan dapat meningkat, mengarah pada pemborosan atau penggunaan anggaran yang tidak sesuai tujuan.

Contoh konkretnya terlihat dalam pengelolaan anggaran entertain di divisi teknisi, *staff* teknisi yang mengajukan dana tidak diwajibkan untuk memberikan bukti transaksi yang valid atau melalui prosedur verifikasi yang jelas.

Hal ini memungkinkan manipulasi laporan pengeluaran, seperti pelaporan biaya entertain penuh meskipun hanya menggunakan sebagian anggaran. Kondisi

ini menunjukkan bahwa meskipun tujuan pengelolaan biaya telah ditetapkan, tanpa tindakan yang terstruktur dan kontrol yang efektif, hasil yang diinginkan sulit tercapai. Jones (2011) mencatat bahwa tujuan tanpa pengawasan yang ketat dan tindakan yang terorganisasi hanya akan menciptakan celah untuk penyalahgunaan sumber daya, yang pada akhirnya dapat merugikan perusahaan.

Secara garis besar, tujuan perusahaan sering tertuang pada dokumen program realisasi rencana strategis manajemen yang disusun setiap awal tahun, yang menjadi tolak ukur kinerja di periode yang akan berjalan. Namun, pencapaian tujuan ini seringkali terhambat oleh kurangnya prosedur yang mendetail dalam implementasi serta ketidakjelasan dalam pengawasan. Tanpa prosedur pengendalian yang jelas, strategi yang baik bisa berakhir dengan kegagalan yang merugikan (Albrecht et al, 2018). Hal ini juga terlihat dalam kasus-kasus besar seperti **Volkswagen (VW)** pada 2015, yang terlibat dalam skandal "*dieseldgate*". Dalam upaya untuk mencapai tujuan penjualan dan pangsa pasar yang lebih besar, perusahaan ini secara sengaja memanipulasi uji emisi untuk mobil diesel mereka. Meskipun perusahaan memiliki tujuan yang jelas dalam hal ekspansi pasar, pengawasan yang tidak cukup ketat dan kebijakan internal yang gagal mencegah tindakan manipulatif ini menyebabkan kerusakan reputasi yang besar dan biaya hukum yang sangat tinggi.

4.3.2 Mengidentifikasi dan Menganalisis Risiko

Perusahaan telah melakukan analisis risiko yang melibatkan berbagai tingkatan manajerial. Namun, analisis tersebut tidak selalu mencakup secara menyeluruh semua risiko yang mungkin muncul, terutama dalam hal pengelolaan pengeluaran eksternal dan pengajuan dana. Wells (2004) menegaskan bahwa tanpa pemahaman yang memadai tentang risiko internal dan eksternal, perusahaan berisiko mengalami kebocoran anggaran dan penyalahgunaan sumber daya. Dalam konteks pengajuan reimbursement, risiko terkait pengelolaan pengeluaran, seperti pengontrolan dana entertain, sering kali tidak teridentifikasi dengan baik.

COSO (2013) menyatakan bahwa pengelolaan risiko yang lemah dapat menyebabkan terjadinya penyalahgunaan, terutama jika proses pengelolaan dana

tidak dilengkapi dengan kontrol yang memadai. Meskipun manajer terlibat dalam pengambilan keputusan, ketidakterlibatan mereka dalam proses pengelolaan eksternal berkontribusi pada celah yang memungkinkan penyalahgunaan terjadi.

Contoh nyata dari masalah ini dapat dilihat pada pengajuan *reimbursement* oleh teknisi tanpa pengawasan yang cukup. Teknisi yang memiliki kebebasan mengundang tamu eksternal tanpa memerlukan laporan transparan kepada manajer meningkatkan risiko penyalahgunaan anggaran. Tanpa pengawasan yang ketat, proses *meeting* yang tidak tercatat ini dapat menyebabkan pengeluaran yang tidak sah dan tidak terkontrol. Albrecht et al. (2018) menegaskan bahwa penyalahgunaan anggaran sering kali dimulai dengan aktivitas kecil yang tampaknya tidak berbahaya namun dapat berkembang menjadi manipulasi yang signifikan. Joseph T. Wells (2004) menambahkan bahwa kurangnya pengawasan yang ketat dalam proses pengelolaan pengeluaran adalah faktor utama dalam terjadinya penyalahgunaan.

4.3.3 Menilai Risiko *Fraud*

Dalam konteks penipuan (*fraud*), perusahaan awalnya tidak mengidentifikasi adanya risiko *fraud* yang signifikan dalam operasionalnya, khususnya dalam pengelolaan keuangan. Namun, salah satu penyebab utama terjadinya *fraud* dalam organisasi adalah pengawasan yang tidak memadai terhadap pengelolaan keuangan dan pengeluaran. Menurut Wells (2004), kurangnya pengawasan yang ketat dapat memberikan ruang bagi individu untuk memanipulasi laporan keuangan dan pengeluaran demi kepentingan pribadi. Kranacher (2020) menegaskan bahwa pengelolaan pengeluaran yang buruk dapat meningkatkan peluang terjadinya penyalahgunaan anggaran, yang sering kali disebabkan oleh kurangnya pengawasan dan kontrol yang memadai. Lebih lanjut, COSO (2017) menggarisbawahi bahwa pengendalian internal yang lemah dapat menyebabkan pengambilan keputusan yang tidak akurat serta meningkatkan risiko penyalahgunaan sumber daya. Oleh karena itu, pengawasan yang tidak memadai dari manajer terhadap pengeluaran yang diajukan dapat menciptakan celah bagi manipulasi angka dalam laporan pengeluaran yang tidak terdeteksi.

Hal ini menunjukkan bahwa meskipun prosedur pengajuan biaya telah ada, pengelolaan yang longgar dan tanpa pengawasan ketat membuka peluang bagi individu untuk memanfaatkan celah tersebut. Dalam kasus ini, pengajuan biaya yang tidak transparan dan tidak diperiksa dengan baik dapat berkontribusi pada kecurangan. Wells (2017) menyebutkan bahwa kurangnya pengawasan yang ketat dapat memberikan ruang bagi individu untuk memanipulasi laporan keuangan dan pengeluaran demi kepentingan pribadi. Albrecht et al. (2018) menambahkan bahwa implementasi pengawasan yang tidak memadai dapat memungkinkan penggelapan dana, bahkan ketika perusahaan telah memiliki pedoman untuk mencegah kecurangan. Oleh karena itu, sistem audit yang lebih sering dan pengawasan yang lebih ketat perlu diterapkan guna mengurangi risiko *fraud*. Kranacher (2020) juga menekankan pentingnya pengawasan yang ketat terhadap transaksi keuangan, karena pengelolaan yang lemah dapat menyebabkan individu menyalahgunakan anggaran dan melakukan manipulasi yang merugikan perusahaan.

4.3.4 Mengidentifikasi dan Menganalisis Perubahan Signifikan

Perubahan eksternal yang mempengaruhi operasional perusahaan, baik berupa regulasi atau kebijakan internal yang berubah, harus diantisipasi dengan baik. Ketika perusahaan gagal mengenali perubahan kecil yang dapat mengubah prosedur operasional, ini dapat membuka celah risiko yang lebih besar, seperti yang dijelaskan oleh Albrecht et al. (2018). Menurut Albrecht et al. (2018), kegagalan organisasi dalam merespons perubahan eksternal dapat menciptakan celah yang dieksploitasi oleh individu untuk kepentingan pribadi. Wells (2004) juga menegaskan bahwa perubahan lingkungan yang tidak diperhitungkan dapat menyebabkan kebijakan yang lemah, yang pada gilirannya menciptakan peluang bagi tindakan penipuan. Kotter (1996) menambahkan bahwa organisasi yang gagal untuk menyesuaikan diri dengan perubahan lingkungan eksternal atau internal cenderung menghadapi kesulitan dalam mempertahankan kinerja yang baik. Oleh karena itu, perusahaan perlu proaktif dalam menyesuaikan kebijakan dan prosedur internal untuk menanggapi dinamika yang berkembang baik dari sisi eksternal maupun internal.

Dalam konteks perusahaan yang gagal mengantisipasi perubahan ini, kasus penyelewengan dana melalui pengajuan biaya yang tidak terkontrol menjadi lebih nyata. Ketika regulasi atau prosedur internal yang baru diterapkan tidak sepenuhnya dipahami atau tidak diikuti dengan ketat, individu-individu di dalam organisasi mungkin memanfaatkan ketidaktahuan ini untuk kepentingan pribadi mereka. Skalak (2006) mencatat bahwa kurangnya perhatian terhadap perubahan kebijakan dan prosedur dapat menyebabkan kelonggaran dalam pengawasan, yang seringkali berujung pada penipuan. Sebagai contoh, jika teknisi tidak diawasi secara ketat dalam mengajukan biaya untuk kegiatan seperti entertain dengan pelanggan, celah ini dapat disalahgunakan untuk menciptakan pengeluaran fiktif atau tidak sah, seperti yang dijelaskan oleh Jones (2011). Dalam situasi ini, kebijakan internal yang lemah dan kurangnya pengawasan yang memadai membuka peluang bagi manipulasi laporan keuangan, yang pada akhirnya merugikan perusahaan.

4.4 Defisiensi *Control Activity*

4.4.1 Mengembangkan Kegiatan Pengendalian

Dalam kasus ini, meskipun perusahaan telah merancang sistem kontrol untuk memantau operasional, mekanisme yang ada belum cukup efektif dalam mencegah atau mendeteksi penyelewengan yang dilakukan oleh teknisi. Salah satu kelemahannya adalah pengajuan *reimbursement* yang dilakukan tanpa adanya pengawasan ketat atau otorisasi formal dari manajer. Menurut Wells (2004), fraud sering kali terjadi ketika ada kelemahan signifikan dalam pengawasan atau kontrol internal. Albrecht et al. (2018) menegaskan bahwa sistem otorisasi yang lemah menjadi pintu masuk utama bagi pengeluaran yang tidak sah. Ketidakterlibatan langsung atasan dalam memverifikasi pengajuan anggaran menciptakan celah yang dapat dimanfaatkan untuk penyalahgunaan. Dalam konteks ini, kurangnya prosedur pengawasan yang ketat dan sistematis, sebagaimana dijelaskan oleh COSO (2013), membuka peluang bagi kecurangan yang tidak terdeteksi.

Contoh nyata dari kelemahan ini terlihat pada pengajuan dana untuk acara entertain teknisi dengan tamu eksternal. Dalam proses ini, teknisi diberi kebebasan untuk melaporkan biaya yang digunakan tanpa perlu menyertakan dokumentasi

pendukung yang cukup, seperti laporan detail kegiatan. Akibatnya, dana operasional sering kali digunakan untuk tujuan yang tidak relevan atau bahkan dimanipulasi untuk kepentingan pribadi. Analisis oleh Kranacher (2020) menyoroti bahwa kurangnya prosedur validasi transaksi mengakibatkan peningkatan risiko penyalahgunaan anggaran. Jones (2011) menambahkan bahwa pengelolaan anggaran yang lemah, tanpa kontrol yang memadai, dapat menciptakan ruang bagi manipulasi yang tidak terdeteksi. Dalam konteks ini, perusahaan tidak hanya menghadapi kerugian finansial tetapi juga potensi hilangnya kepercayaan dari para pemangku kepentingan, yang dapat berdampak negatif pada reputasi perusahaan secara keseluruhan.

Kasus Enron Corporation merupakan salah satu contoh penyelewengan yang terjadi akibat lemahnya sistem pengawasan internal dan manipulasi pelaporan keuangan. Enron menggunakan praktik *creative accounting* untuk menyembunyikan hutang perusahaan melalui skema perusahaan cangkang (*special purpose entities*) guna menjaga laporan keuangan terlihat sehat. Menurut Jones (2011), manipulasi laporan keuangan seringkali dilakukan dengan menciptakan struktur yang kompleks dan kurang transparan untuk mengaburkan realitas keuangan organisasi.

4.4.2 Mengembangkan Kontrol Umum Atas Teknologi

Kontrol atas teknologi informasi dalam organisasi sangat penting untuk memastikan integritas sistem dan data yang digunakan dalam operasional bisnis. Namun, perusahaan ini tampaknya belum sepenuhnya menerapkan pengendalian yang kuat terhadap sistem teknologi informasi yang ada. Menurut Albrecht et al. (2018), pengendalian umum atas teknologi melibatkan tidak hanya pemeliharaan sistem, tetapi juga manajemen akses, integritas data, dan perlindungan terhadap risiko manipulasi informasi. Jones (2011) menegaskan bahwa kegagalan dalam mengelola kontrol teknologi dapat membuka peluang besar untuk manipulasi sistem yang dapat merusak kredibilitas laporan keuangan. Dalam kasus ini, teknisi yang bertugas melakukan pengajuan reimbursement memiliki akses ke sistem ERP tanpa pengawasan yang memadai. Teknisi memanfaatkan kelonggaran kontrol dengan mengajukan biaya entertainment yang sebenarnya tidak pernah dilakukan.

Pengajuan tersebut disetujui oleh sistem karena tidak adanya prosedur verifikasi berlapis seperti pengecekan manual oleh manajer atau otorisasi tambahan dari departemen keuangan. Skalak (2006) menambahkan bahwa pengendalian sistem yang lemah menciptakan celah bagi penyalahgunaan, yang akhirnya dapat merusak integritas informasi dan laporan keuangan.

Dalam konteks ini, risiko yang muncul terkait dengan pengajuan biaya entertain yang tidak diawasi secara ketat semakin jelas. Kranacher (2020) menjelaskan bahwa kontrol akses yang lemah terhadap sistem memungkinkan individu untuk memanipulasi data transaksi dengan mudah. Ketidakhadiran verifikasi berlapis mempersulit deteksi penyimpangan, dan hal ini memberikan ruang bagi teknisi untuk memanipulasi data pengeluaran. Proses otorisasi yang longgar membuka celah bagi pengeluaran yang tidak sah, yang berpotensi merugikan perusahaan secara finansial dan merusak reputasi. Menurut COSO (2017), lemahnya kontrol teknologi informasi meningkatkan potensi risiko operasional, yang pada gilirannya dapat menimbulkan penyalahgunaan anggaran.

4.4.3 Mengembangkan Kebijakan dan Prosedur

Dalam kasus penyelewengan dana, terlihat bahwa kelemahan dalam pelaksanaan kebijakan menjadi faktor kunci. Kebijakan yang dirancang untuk memastikan akuntabilitas dalam pengajuan *reimbursement* ternyata tidak didukung oleh prosedur otorisasi yang memadai. Tidak adanya pengawasan ketat dari pihak manajerial menciptakan celah yang dapat dimanfaatkan untuk manipulasi data pengeluaran. Seperti yang dijelaskan oleh Albrecht et al. (2018), *fraud* cenderung terjadi ketika kombinasi kelemahan kontrol internal dan kurangnya pengawasan langsung tidak diperhatikan. Wells (2004) menambahkan bahwa otorisasi pengeluaran tanpa tinjauan rinci oleh pihak berwenang meningkatkan risiko *fraud*, karena tidak adanya kontrol yang ketat mempermudah individu untuk memanfaatkan celah tersebut. Oleh karena itu, penting bagi perusahaan untuk memperkuat mekanisme pengawasan dan pengendalian, terutama dalam hal otorisasi pengeluaran, guna mencegah terjadinya kecurangan.

Sebagai ilustrasi, seorang teknisi di perusahaan diberikan kewenangan untuk mengajukan biaya terkait operasional tanpa memerlukan persetujuan langsung dari supervisornya. Dalam salah satu insiden, teknisi mengajukan *reimbursement* untuk acara entertain bersama klien yang ternyata biaya yang diajukan lebih besar dari yang sebenarnya dikeluarkan untuk acara tersebut. Sistem ERP yang digunakan perusahaan tidak memiliki mekanisme validasi otomatis yang cukup, sehingga pengajuan tersebut lolos tanpa tinjauan lebih lanjut. Kranacher (2020) menegaskan bahwa kontrol teknologi yang lemah memungkinkan individu memanfaatkan celah dalam sistem untuk melakukan manipulasi data. Kejadian ini menunjukkan bahwa kebijakan pengendalian yang tidak diterapkan secara ketat dapat membuka peluang bagi individu untuk memanfaatkan kelemahan sistem, yang pada akhirnya mengakibatkan kerugian finansial bagi perusahaan.

4.5 Defisiensi Information & Communication

4.5.1 Informasi Relevan

Penyelewengan dana melalui pengajuan *reimbursement* dalam kasus ini mengungkapkan kelemahan signifikan dalam sistem pengelolaan informasi perusahaan. Prosedur pengumpulan data yang hanya mengandalkan formulir pengajuan tanpa mekanisme validasi ketat menciptakan celah besar untuk manipulasi laporan pengeluaran. Menurut Albrecht et al. (2018), tanpa pengawasan langsung dan alat deteksi anomali, organisasi cenderung rentan terhadap tindakan fraud. Wells (2004) menambahkan bahwa sistem kontrol internal yang lemah, terutama yang tidak mengintegrasikan proses verifikasi yang memadai, menjadi pintu masuk bagi manipulasi data pengeluaran. Oleh karena itu, penting bagi perusahaan untuk mengimplementasikan sistem kontrol internal yang lebih ketat dan sistem pengawasan yang lebih efektif guna memastikan transparansi dan akurasi pengelolaan keuangan.

Dalam salah satu insiden, seorang teknisi berhasil mengajukan *reimbursement* untuk pengeluaran yang sebenarnya tidak sesuai dengan yang dilakukan. Sistem ERP perusahaan hanya mencatat pengajuan berdasarkan data yang diinput tanpa validasi dokumen atau kelayakan biaya. Skalak (2006)

menegaskan bahwa ketergantungan pada teknologi tanpa mekanisme validasi yang memadai meningkatkan risiko *fraud*. Selain itu, Kranacher (2020) menyoroti bahwa manajer yang tidak memiliki alat atau prosedur untuk mendeteksi ketidakwajaran dalam laporan pengeluaran juga berkontribusi pada hilangnya dana perusahaan.

Kasus kebocoran data Equifax pada 2017 menjadi contoh nyata kelemahan pada aspek *information and communication*, yang melibatkan data sensitif milik lebih dari 147 juta konsumen. Masalah utamanya adalah kegagalan dalam menyampaikan informasi kritis terkait kerentanan perangkat lunak (*Apache Struts*) kepada pihak yang bertanggung jawab untuk memperbaikinya, meskipun peringatan telah diberikan beberapa bulan sebelumnya. COSO (2017) menekankan bahwa proses komunikasi harus mencakup penyampaian informasi yang relevan dan tepat waktu kepada pihak yang memiliki wewenang untuk bertindak, namun, dalam kasus ini, komunikasi internal yang tidak efektif memperbesar dampak serangan tersebut. Wells (2004) juga menegaskan pentingnya komunikasi transparan untuk mencegah risiko, sementara Kranacher (2020) menyatakan bahwa kegagalan dalam menyampaikan informasi kritis dapat meningkatkan risiko organisasi terhadap ancaman eksternal. Akibatnya, kelemahan komunikasi ini membuka celah besar bagi manipulasi data yang berujung pada kerugian besar bagi organisasi.

4.5.2 Berkomunikasi Secara Internal

Komunikasi internal yang lemah, terutama dalam pelaksanaan pengawasan langsung oleh manajer atas verifikasi pengeluaran, menciptakan peluang untuk terjadinya penyalahgunaan anggaran entertain yang disediakan perusahaan. Ketidakhadiran proses validasi yang ketat memungkinkan teknisi untuk melaporkan pengeluaran yang tidak sesuai dengan kenyataan. COSO (2017) menekankan pentingnya komunikasi yang efektif dalam kerangka kontrol internal untuk memastikan transparansi dan akuntabilitas. Selain itu, Kranacher (2020) mengungkapkan bahwa kurangnya prosedur komunikasi yang terstruktur dapat meningkatkan risiko manipulasi, terutama ketika informasi yang diteruskan ke departemen keuangan tidak divalidasi dengan baik. Hal ini menyoroti bagaimana

kurangnya komunikasi dapat menciptakan celah yang memungkinkan individu memanfaatkan kelemahan sistem.

Kasus ini menunjukkan bagaimana teknisi memanfaatkan celah dalam proses pengajuan biaya entertain. Mereka menyampaikan pengeluaran yang dilaporkan sesuai dengan anggaran, tetapi pada kenyataannya, hanya sebagian kecil dari anggaran tersebut digunakan. Tanpa pengawasan langsung dari manajer atau pihak keuangan, laporan tersebut lolos dari pemeriksaan. Wells (2004) menyoroti bahwa fraud sering terjadi dalam sistem kontrol internal yang lemah, di mana otorisasi pengeluaran dilakukan tanpa pengawasan ketat. Situasi ini mencerminkan perlunya proses verifikasi yang lebih komprehensif untuk memastikan bahwa setiap pengeluaran yang diajukan sesuai dengan kenyataan dan tidak ada potensi penyalahgunaan dana.

4.5.3 Berkomunikasi Secara Eksternal

Komunikasi eksternal perusahaan yang melibatkan kegiatan entertain bersama pelanggan, seperti makan bersama, tidak disertai dengan langkah pengawasan dan verifikasi yang memadai terhadap penggunaan anggaran. Dalam kasus fraud yang teridentifikasi, teknisi memanfaatkan kelemahan pengelolaan ini dengan melaporkan pengeluaran entertain yang sesuai dengan anggaran, meskipun kenyataannya hanya sebagian dana yang digunakan sesuai peruntukan. Skalak (2006) menekankan bahwa kesenjangan dalam pengelolaan informasi keuangan, khususnya terkait kegiatan yang melibatkan pihak eksternal, dapat meningkatkan risiko manipulasi dan kesalahan dalam pelaporan. Albrecht et al. (2018) juga menyoroti pentingnya pengendalian internal yang terintegrasi pada setiap proses, termasuk pengajuan anggaran, untuk memastikan akuntabilitas dan mencegah potensi penyalahgunaan dana. Sayangnya, perusahaan tidak mengimplementasikan mekanisme pengawasan yang memadai pada proses pengajuan *reimbursement* ini, sehingga menciptakan celah yang dieksploitasi oleh oknum teknisi.

Sebagai contoh, teknisi yang bertanggung jawab untuk menjalin hubungan baik dengan pelanggan mengajukan *reimbursement* untuk kegiatan entertain yang dilaporkan sesuai dengan anggaran yang diberikan perusahaan. Namun,

kenyataannya, teknisi hanya menggunakan setengah dari dana tersebut, sementara sisanya disalahgunakan untuk kepentingan pribadi. Sistem perusahaan tidak memiliki mekanisme verifikasi yang memadai untuk mengecek bukti transaksi atau kelayakan pengeluaran tersebut. Wells (2004) menjelaskan bahwa kurangnya kontrol verifikasi berlapis dapat membuka peluang bagi individu untuk melakukan manipulasi demi keuntungan pribadi.

4.6 Defisiensi *Monitoring & Evaluation*

4.6.1 Evaluasi Berkelanjutan Dan Terpisah

Dalam kasus penyelewengan dana oleh sekelompok teknisi, kelemahan dalam mekanisme evaluasi menjadi faktor utama yang memungkinkan manipulasi ini terjadi. Idealnya, perusahaan harus mengintegrasikan evaluasi berkelanjutan dengan evaluasi terpisah yang lebih mendalam. Evaluasi berkelanjutan, seperti monitoring rutin atas pengajuan dan persetujuan pengeluaran, dapat membantu mengidentifikasi penyimpangan secara *real-time* (Arens, 2023). Di sisi lain, evaluasi terpisah, misalnya melalui audit internal atau tinjauan spesifik terhadap laporan keuangan, memungkinkan perusahaan mendalami pola pengeluaran yang mencurigakan (Kranacher, 2020). Tanpa kedua pendekatan ini, prosedur pengawasan tidak mampu memastikan bahwa seluruh pengajuan dana telah diverifikasi dengan benar oleh otoritas yang berwenang, sebagaimana disarankan oleh COSO (2017).

Kasus ini menyoroti bagaimana lemahnya pengawasan terhadap pengajuan *reimbursement* menciptakan celah bagi penyimpangan. Contohnya, teknisi yang bertugas menghadiri pertemuan eksternal diberi kebebasan untuk mengajukan klaim tanpa ada verifikasi mendetail dari pihak keuangan. Dalam satu kasus spesifik, pengeluaran untuk acara eksternal ternyata mengandung elemen fiktif, seperti biaya transportasi atau konsumsi yang tidak sesuai dengan yang terjadi. Hal ini menunjukkan betapa pentingnya kombinasi monitoring dan evaluasi terpisah dalam mencegah risiko *fraud*, sesuai dengan prinsip yang ditegaskan oleh Skalak (2006) bahwa pengendalian internal harus dirancang untuk mendeteksi dan mencegah manipulasi sejak awal.

Lehman Brothers, sebuah bank investasi besar di AS, terlibat dalam praktik manipulasi laporan keuangan yang digunakan untuk menyembunyikan kewajiban utang mereka melalui mekanisme yang dikenal sebagai *Repo 105* untuk memberikan gambaran yang lebih sehat tentang stabilitas finansial mereka. Kegagalan pengawasan internal yang tepat, di mana manajer dan auditor internal tidak dapat mendeteksi manipulasi laporan ini, menjadi faktor utama dalam krisis tersebut. Seperti yang dijelaskan oleh Wells (2004), pengawasan yang lemah terhadap pengelolaan risiko sering kali menyebabkan kerugian besar, sementara oleh Albrecht et al. (2018) menekankan pentingnya evaluasi risiko yang menyeluruh dan verifikasi yang ketat untuk menghindari penipuan dan kerugian besar.

4.6.2 Mengevaluasi dan Mengkomunikasikan Kelemahan

Dalam kasus manipulasi pengajuan *reimbursement* oleh teknisi, kelemahan dalam sistem pengendalian internal dan pengawasan menjadi faktor utama yang memungkinkan terjadinya penyelewengan. Teknisi melaporkan pengeluaran entertain yang seolah-olah sesuai dengan anggaran, tetapi kenyataannya hanya menggunakan sebagian dari dana tersebut. COSO (2013) menekankan pentingnya proses evaluasi yang mencakup pengawasan berkelanjutan dan evaluasi terpisah untuk mengidentifikasi ketidaksesuaian yang memerlukan perhatian mendalam. Kurangnya pengawasan langsung dan audit berkala terhadap laporan pengeluaran menciptakan peluang bagi manipulasi data, sebagaimana diuraikan oleh Arens (2023), bahwa audit yang tidak dirancang dengan menyeluruh akan gagal mendeteksi penyimpangan dalam aktivitas operasional perusahaan.

Sebagai ilustrasi, dalam satu kasus teknisi mengajukan *reimbursement* untuk acara makan bersama pelanggan, di mana dokumen pendukung berupa bon makan telah dimanipulasi agar sesuai dengan total anggaran yang diberikan perusahaan. Namun, hasil audit mendalam kemudian mengungkapkan bahwa separuh dari anggaran tersebut tidak digunakan sesuai peruntukannya dan disalahgunakan untuk kepentingan pribadi. Hal ini terjadi karena proses pengajuan dan persetujuan *reimbursement* tidak melibatkan otorisasi berjenjang dari manajer, yang sesuai dengan peringatan Albrecht et al. (2018) bahwa kelemahan dalam

sistem kontrol otorisasi dapat memberikan celah signifikan untuk *fraud*. Temuan ini menekankan pentingnya desain mekanisme pengawasan yang lebih terintegrasi, termasuk audit rutin dan validasi bukti transaksi secara menyeluruh, sebagaimana disarankan oleh Kranacher (2020).

