ELANG: Journal of Interdisciplinary Research
E-ISSN: XXXX-XXXX || P-ISSN: XXXX-XXXX

CIS Information System Audit Using the COSO Framework (Studi Kasus : CIS)

Rendyka Putra Maulana[1]*, Roni Maher Samuel Siagian[2]
[1)]rendykaputra26@gmail.com || [2)] ronisiagian7@gmail.com

[1,2] *Universitas Merdeka Malang, Teknologi Informasi, Sistem Informasi, Jalan Terusan Dieng, 62-64 Klojen,Pisang Candi, Kec. Sukun, Kota Malang, Jawa Timur 65146, Indonesia*

Kata Kunci
Audit Sistem Informasi, *Campus Information System* (CIS), COSO *Framework*, Keamanan Data, Efisiensi Operasional.

****) Author Korespondensi***
rendykaputra26@gmail.com

Abstrak
Audit Sistem Informasi merupakan langkah penting dalam memastikan efisiensi, keamanan, dan kepatuhan suatu sistem informasi terhadap kebijakan dan regulasi yang berlaku. Penelitian ini menggambarkan implementasi audit menggunakan *framework* COSO pada *Campus Information System* (CIS) di Institut Teknologi Del (IT Del). Audit ini bertujuan untuk mengevaluasi keamanan dan efisiensi pengelolaan informasi dalam CIS IT Del serta mengidentifikasi risiko yang mungkin terkait dengan keamanan data dan akses informasi. Metode penelitian melibatkan identifikasi risiko, penilaian risiko, pengendalian risiko, dan pemangkasan risiko. Dengan fokus pada aspek keamanan data, audit CIS IT Del menggunakan *framework* COSO dari Committee of Sponsoring Organizations of the Treadway Commission (COSO). Penelitian ini mengidentifikasi dua kategori risiko utama, yaitu risiko terkait dengan keamanan data dan risiko terkait dengan akses informasi. Implementasi mitigasi yang efektif diperlukan untuk mengurangi potensi dampak negatif dan memastikan kelancaran operasi CIS serta keamanan data dan informasi secara menyeluruh. Hasil audit ini memberikan rekomendasi perbaikan yang dapat meningkatkan efisiensi operasional IT Del dan mendukung pengambilan keputusan strategis. Selain itu, audit berperan dalam mengidentifikasi dan mencegah potensi masalah terkait dengan etika dan standar dalam lingkungan IT Del. Implementasi *framework* COSO memberikan panduan penting dalam mengelola pengendalian internal, meminimalkan risiko, dan mencapai tujuan organisasi.

1. Pendahuluan

Teknologi Informasi (TI) adalah istilah yang digunakan untuk mengacu pada penggunaan teknologi dalam mengumpulkan, mengolah, menyimpan, dan menyebarkan informasi. Ini mencakup berbagai elemen yang digunakan dalam konteks teknologi dan komunikasi untuk mendukung kebutuhan organisasi, individu, atau masyarakat dalam mengelola dan memproses data, informasi, dan pengetahuan. Oleh sebab itu audit sistem informasi sangat penting, karena memastikan sistem informasi berbasis komputer berfungsi dengan baik, terlindungi dari ancaman, dan sesuai dengan kebijakan organisasi. Selain itu, audit sistem informasi sangat terkait dengan konsep tata kelola teknologi informasi, membantu organisasi memahami bagaimana teknologi informasi digunakan dan dikelola dalam konteks strategi bisnis. Audit sistem informasi dapat memberikan kemampuan mandiri memahami materi tata kelola teknologi informasi, yang menjadi kompetensi kunci dalam dunia profesional yang semakin terkait dengan teknologi informasi [1].

Institut Teknologi Del (IT Del) adalah salah satu perguruan tinggi swasta (PTS) di Sumatera Utara yang dapat menjadi pilihan bagi calon mahasiswa yang ingin melanjutkan pendidikan mereka [2]. IT Del merupakan tempat di mana ilmu pengetahuan, inovasi, dan teknologi berkolaborasi untuk menciptakan pemahaman dalam perkembangan digital, pemecahan masalah, dan penciptaan solusi canggih. Dalam upaya meningkatkan kualitas pembelajaran di kampus, IT Del menyediakan media pembelajaran. Terdapat dua media pembelajaran, yaitu CIS dan E-Course. *Campus Information System* (CIS) adalah sebuah sistem informasi yang dirancang untuk mengelola data terkait dengan suatu universitas atau lembaga pendidikan tinggi. CIS mengumpulkan, menyimpan, mengolah, dan menyajikan berbagai jenis data terkait universitas, seperti materi pembelajaran, data pribadi, KRS, keuangan, artikel, layanan keasramaan, BAAK, SKPI, Informasi, Laboratorium dan Survey. Tujuan utama dari CIS adalah untuk meningkatkan efisiensi dan kemajuan IT Del dengan menyediakan akses yang mudah dan alat analisis yang kuat untuk data yang relevan. Dengan bantuan CIS, universitas dapat mengelola aset fisik mereka, seperti bangunan dan fasilitas, serta melacak data terkait mahasiswa, penerimaan, dan berbagai aspek lain dari operasional kampus.

Dengan banyaknya layanan yang diberikan, maka dibutuhkan audit terhadap *Campus Information System* (CIS) agar pengumpulan, pengolahan, penyimpanan, dan penyebaran informasi yang terkait dengan IT Del berjalan dengan baik dan aman. Seiring perkembangannya, banyak permasalahan yang perlu diatasi pada CIS. Salah satu masalah utama adalah keamanan data, seperti pembayaran bursar, kesalahan dalam *generate* kuesioner yang terkadang tidak sesuai dengan program studi. Selain permasalahan dalam dalam keamanan data, CIS juga sering mengalami kegagalan server. Kegagalan server ini berupa, gagalnya mahasiswa untuk mengaksesnya serta lambatnya CIS dalam memberikan respon saat digunakan [3].

Teknologi Informasi berperan penting bagi Campus Sistem Informasi IT DEL, dimana TI berfungsi sebagai penunjang utama pengelolaan data yang efisien dan akurat. TI digunakan sebagai sarana untuk mengoptimalkan proses akademik dan administratif, meningkatkan kualitas layanan pendidikan, dan memperkuat kolaborasi antara fakultas, staf, dan mahasiswa. Dengan fokus pada keamanan informasi, TI bertanggung jawab atas perlindungan data sensitif dan mencegah ancaman keamanan *cyber* yang dapat merugikan institusi. CIS merupakan salah satu implementasi dari teknologi informasi yang digunakan dalam lingkungan kampus. CIS merupakan penerapan kerangka kerja yang dirancang untuk membantu dalam menilai, mengontrol, dan meningkatkan efektivitas sistem informasi di Institut Teknologi Del. Dengan adanya sistem ini, semua bagian penting seperti administrasi akademik, keuangan, dan manajemen sumber daya manusia dapat terintegrasi dengan baik. Sistem ini akan memungkinkan komunikasi yang lancar antara mahasiswa, dosen, dan staf administrasi, memperkuat kerjasama dan pertukaran informasi yang sangat penting. Dengan menggunakan teknologi informasi yang canggih, Institut Teknologi Del dapat meningkatkan kualitas layanan akademik dan administratif, mengoptimalkan penggunaan sumber daya, dan memberikan pengalaman belajar yang lebih terpadu bagi mahasiswa dan staf kampus [10].

Audit terhadap CIS memainkan peran penting dalam memastikan bahwa data dan informasi yang dikumpulkan terkait dengan operasional kampus, termasuk aspek keuangan, akademik, fasilitas, dan sumber daya manusia, dikelola secara efisien dan sesuai dengan standar. Hal ini juga membantu dalam mengidentifikasi risiko yang mungkin terkait dengan keamanan data server. Hasil audit CIS dapat memberikan rekomendasi perbaikan yang dapat meningkatkan efisiensi operasional IT Del, mendukung pengambilan keputusan strategis. Selain itu, audit juga berperan dalam mengidentifikasi dan mencegah potensi masalah terkait dengan etika dan standar yang berlaku dalam lingkungan IT Del. Dalam mengatasi permasalahan yang terjadi pada CIS, dilakukan audit dengan menggunakan *framework* COSO.

Komitmen *Sponsoring Organisasi Treadway Commission (Committee of Sponsoring Organizations of the Treadway Commission*), atau COSO, adalah suatu kerangka kerja yang telah berkembang penting dalam konteks pengendalian internal. Kerangka kerja ini terdiri dari lima komponen yang saling terkait, termasuk lingkungan pengendalian, penilaian risiko, aktivitas pengendalian, informasi dan komunikasi, serta pemantauan. COSO digunakan oleh berbagai jenis organisasi, termasuk organisasi sektor publik, untuk merancang, mengimplementasikan, dan mengelola sistem pengendalian internal yang efektif. Dalam penelitian yang Anda

sebutkan, COSO digunakan sebagai latar belakang untuk menunjukkan pentingnya memiliki kerangka kerja yang komprehensif dan relevan dalam mengelola pengendalian internal, terutama terkait dengan aktivitas pelaporan pelanggaran atau keluhan. COSO memberikan pedoman yang penting untuk membantu organisasi sektor publik dalam meminimalkan risiko, meningkatkan efisiensi, dan mencapai tujuan mereka melalui pengelolaan pengendalian internal yang efektif [4].

Oleh karena itu tujuan dari audit ini adalah untuk mengevaluasi keamanan serta efisiensi pengelolaan informasi dalam *Campus Information System* (CIS) di IT Del dengan menerapkan *framework* COSO dalam proses audit

1.1 COSO

Audit Sistem Informasi adalah proses penilaian independen terhadap sistem informasi suatu organisasi atau perusahaan untuk memastikan bahwa sistem tersebut berfungsi dengan baik, aman, dan sesuai dengan standar keamanan serta regulasi yang berlaku.

Audit ini bertujuan untuk mengevaluasi dan memverifikasi efektivitas dan keamanan sistem informasi, serta memastikan kepatuhan terhadap kebijakan dan prosedur yang telah ditetapkan**.** Audit Sistem Informasi merupakan langkah untuk mengumpulkan dan mengevaluasi yang digunakan untuk menentukan apakah suatu sistem aplikasi terkomputerisasi telah diimplementasikan dengan baik, memastikan pengendalian intern yang memadai, menjaga integritas data, dan memastikan efisiensi operasi sistem informasi berbasis computer [5].

COSO *(Committee of Sponsoring Organizations of the Treadway Commission)* adalah *framework* yang dapat disesuaikan dan digunakan dalam audit teknologi perusahaan. COSO memiliki peran dalam membantu perusahaan mencapai untuk tujuan mereka dalam meningkatkan kinerja perusahaan dengan mengidentifikasi kebijakan, proses, dan sistem kontrol yang sesuai untuk menjaga nilai perusahaan [6]**.** Pengendalian internal dalam kerangka COSO merupakan tindakan yang dijalankan oleh dewan direksi, manajemen, serta karyawan untuk memberikan jaminan yang cukup guna mencapai tujuan operasional yang efisien dan efektif, memastikan keandalan informasi, dan mematuhi peraturan dan perundangan yang berlaku [7]. Pengendalian internal ini bertujuan untuk melindungi aset organisasi, mencegah penipuan, meminimalkan risiko, dan memastikan akuntabilitas. Pengendalian itu bertujuan untuk melindungi aset organisasi, yang mencakup aset finansial, properti, dan sumber daya lainnya, dari berbagai risiko seperti pencurian, penyalahgunaan, atau kerusakan.

2. Metode Penelitian

Adapun tahapan yang dilakukan dalam Risk Management pada *Campus Information System* (CIS) adalah ***Identifying Risks*** **(Identifikasi Risiko),** ***Assessing Risks*** **(Penilaian Risiko),** ***Controlling Risks*** **(Pengendalian Risiko) dan** ***Mitigating Risks*** **(Pemangkasan Risiko).**

Identifying Risks merupakan tahap awal dalam manajemen risiko pada *Campus Information System* (CIS) di IT DEL. Pada tahap ini, dilakukan upaya untuk mengidentifikasi semua potensi risiko yang dapat mempengaruhi keberlanjutan, keamanan, dan kinerja CIS. *Identifying Risks* mencakup pengenalan berbagai ancaman potensial, kerentanan sistem, dan dampak yang mungkin timbul akibat terjadinya risiko.

Setelah risiko diidentifikasi, langkah selanjutnya adalah melakukan *Assessing Risks*. Pada tahap ini, risiko dinilai berdasarkan dua faktor utama: kemungkinan terjadinya risiko dan dampaknya terhadap sistem informasi. *Assessing Risks* dapat menggunakan matriks risiko untuk menentukan tingkat keparahan risiko. Dengan informasi ini, tim manajemen risiko dapat mengidentifikasi risiko-risiko yang memiliki dampak tinggi dan merancang strategi untuk mengelolanya.

Setelah penilaian risiko selesai, langkah selanjutnya adalah merancang dan menerapkan kontrol risiko. *Controlling Risks* melibatkan serangkaian tindakan yang dirancang untuk mengurangi kemungkinan terjadinya risiko atau mengurangi dampaknya jika risiko tersebut terjadi. Contoh *Controlling Risks* meliputi penerapan kebijakan keamanan yang ketat, pembaruan perangkat lunak secara teratur, dan penggunaan teknologi

keamanan seperti *firewall* dan antivirus. Selain itu, tindakan kontrol juga dapat mencakup pelibatan pengguna dan pelatihan keamanan untuk meningkatkan kesadaran terhadap risiko.

Mitigating Risks melibatkan tindakan untuk mengurangi dampak dan kemungkinan terjadinya risiko. Ini dapat mencakup pengembangan rencana pemulihan bencana, pembuatan cadangan data secara teratur, dan implementasi solusi keamanan tambahan. *Mitigating Risks* harus menjadi bagian integral dari strategi manajemen risiko secara keseluruhan.

2.1 Pengumpulan Data

Adapun penelitian ini menggunakan teknik analisis data kualitatif, dimana analisis kualitatif merupakan analisis yang didasarkan pada penggambaran yang mendukung analisa seperti wawancara, observasi atau analisis dokumen untuk menjalankan analisis untuk menggali informasi yang lengkap untuk memecahkan masalah yang dihadapi. Dan dalam upaya meningkatkan keamanan data, kualitas layanan, serta efisiensi pengumpulan, pengolahan, penyimpanan, dan penyebaran informasi terkait operasional kampus, penelitian ini melibatkan proses analisis data kualitatif seperti menggali, menguraikan, dan merangkum peristiwa dari data yang diperoleh. Selain itu, dengan penerapan *framework* COSO dalam audit Sistem Informasi (CIS) di IT Del juga dimanfaatkan untuk mengevaluasi pengendalian internal dan meningkatkan keamanan serta efisiensi pengelolaan informasi [11].

Tingkat keberhasilan setiap pertanyaan analisis dapat kita asumsikan seperti pada tabel dibawah ini.

Tabel 1. Penilaian Kriteria

Kriteria	Skor
Probability	1-5
Impact	1-5

Untuk menganalisis *Campus Information System* (CIS) yang diperlukan setiap mahasiswa dalam proses pembelajaran yang dilakukan di kampus. Maka, dilakukan desain dengan metode observasi menggunakan *framework* COSO seperti yang ditampilkan pada tabel dibawah ini [12].

Tabel 2.Atribut

Atribut	Keterangan
P	*Probability*
I	*Impact*

3. Hasil dan Pembahasan

Dalam tahap implementasi penelitian ini, proses pengumpulan data dilakukan melalui serangkaian observasi yang menggunakan metode observasi. Pemilihan teknik observasi ini bertujuan untuk memungkinkan peneliti untuk mendapatkan observasi yang lebih mendalam tentang subjek penelitian. Teknik observasi yang digunakan melibatkan pengamatan langsung terhadap berbagai aspek yang relevan dengan kerangka kerja COSO *(Committee of Sponsoring Organizations of the Treadway Commission).* Teknik observasi ini memungkinkan peneliti untuk memahami lebih baik implementasi praktik-praktik yang sesuai dengan standar COSO dalam konteks penelitian, yang pada gilirannya dapat mendukung hasil penelitian yang lebih komprehensif dan relevan.

Pelaksanaan observasi ini dilakukan di lingkungan Kampus IT Del, dengan fokus untuk memperoleh pemahaman yang komprehensif mengenai infrastruktur Teknologi Informasi (TI) yaitu *Campus Information System* yang mendukung sistem informasi kampus. Data yang diperoleh dari hasil observasi kemudian akan dianalisis secara deskriptif. Metode analisis deskriptif digunakan untuk menggambarkan data secara teliti dan objektif tanpa bermaksud untuk membuat kesimpulan yang terlalu umum.

Dari hasil analisis yang dilakukan terhadap infrastruktur Teknologi Informasi *(Campus Information System)*, selanjutnya dapat menyusun laporan hasil audit *Campus Information System*, yang memberikan gambaran menyeluruh tentang tingkat pemanfaatan dan efektivitas penggunaan Teknologi Informasi *(Campus Information System)* di lingkungan IT Del. Laporan hasil audit tersebut diharapkan menjadi landasan untuk pengembangan yang lebih baik di masa mendatang. Dan diharapkan kampus IT Del dapat terus mengoptimalkan penggunaan *Campus Information System* guna mendukung dan meningkatkan efisiensi serta efektivitas dari proses kegiatan bisnis yang berlangsung [13].

Berdasarkan implementasi yang telah dilakukan pada bab sebelumnya, dapat dihasilkan penggunaan COSO *framework* pada CIS IT Del sebagai berikut.

Tabel 3. Hasil

No	*Asset*	*Risk*	P	I	P x I
1.	**Perkuliahan**	Kesulitan dalam mengakses mata kuliah untuk memperoleh materi pembelajaran.	1	2	2
2.	**Data Diri**	Ancaman terhadap keamanan data diri mahasiswa dan kelengkapan informasi mahasiswa.	2	5	10
3.	**KRS (Kartu Rencana Studi)**	Kurangnya kelengkapan mata kuliah, Persyaratan Program Studi dalam pengambilan mata kuliah.	1	3	3
4.	**Keuangan**	Ancaman terhadap informasi keuangan serta keamanan data keuangan.	2	5	10
5.	**Artikel**	Ancaman terhadap kelengkapan informasi dalam artikel serta keamanan informasi kampus seperti peraturan-peraturan yang terdapat pada Kampus IT Del.	1	2	2
6.	**Keasramaan**	Resiko terhadap informasi pelanggaran peraturan keasramaan dan informasi perizinan kepada keasramaan.	1	3	3
7.	**BAAK(Biro Administrasi Akademik dan Kemahasiswaan**	Ancaman terhadap keamanan data seperti data mahasiswa, dosen atau pegawai serta pengelolaan administrasi akademik dan kemahasiswaan.	2	5	10
8.	**Laboratorium**	Ancaman terhadap keamanan dalam penggunaan laboratorium, pengelolaan dalam peminjaman alat-alat laboratorium serta pemesanan dan penggunaan bahan laboratorium yang baik dan benar.	2	4	8
9.	**Informasi**	Ancaman terhadap keamanan data informasi, kebocoran informasi IT Del atau serangan siber.	2	5	10
10.	**Survei**	Resiko pengisian kuesioner serta pelaksanaan polling yang tidak terlaksana dengan baik yang dilakukan oleh seluruh civitas IT Del.	5	2	10

Setelah melakukan analisis terhadap CIS *(Campus information System),* maka dapat diketahui resiko yang umumnya terjadi risiko yang pada CIS. Untuk mengatasi terjadinya risiko tersebut berikut control yang dapat dilakukan.

Tabel 4. Control

No	*Asset*	Control
1.	**Perkuliahan**	***Mitigation:*** Untuk menghindari resiko tersebut adalah dengan memastikan kelengkapan materi pembelajaran secara online tersedia dengan baik. Dengan begitu mahasiswa dapat mengakses mata kuliah yang dibutuhkan menggunakan jaringan internet yang cepat agar mudah diakses.

2.	**Data Diri**	***Mitigation:*** Untuk menghindari resiko tersebut adalah dengan memberikan kebijakan serta prosedur keamanan data yang ketat dan baik, serta memanfaatkan penggunaan alat keamanan teknologi untuk melindungi data-data mahasiswa.
3.	**KRS (Kartu Rencana Studi)**	***Mitigation:*** Untuk menghindari resiko tersebut adalah memberikan informasi yang akurat kepada mahasiswa terkait persyaratan program studi dalam pengambilan mata kuliah yang sesuai dengan ketentuan, serta memastikan bahwa mata kuliah lengkap dan tersedia.
4.	**Keuangan**	***Mitigation:*** Untuk menghindari resiko tersebut adalah dengan menerapkan kebijakan serta prosedur yang memadai, enkripsi data, pemantauan keamanan yang ketat untuk mengurangi kemungkinan terjadinya pelanggaran keamanan data keuangan dan mengurangi dampak negatif lainnya yang akan terjadi.
5.	**Artikel**	***Mitigation:*** Untuk menghindari resiko tersebut adalah dengan memastikan bahwa artikel dapat diakses oleh seluruh civitas IT Del agar setiap informasi penting seperti peraturan-peraturan yang terdapat di IT Del dapat dilakukan dengan baik. Melakukan pengawasan dan pemantauan terhadap keamanan yang terdapat pada artikel.
6.	**Keasramaan**	***Mitigation:*** Untuk menghindari resiko tersebut adalah dengan memastikan informasi keasramaan tersampaikan kepada mahasiswa sehingga pelaksanaan prosedur perizinan dapat dilakukan dengan tepat untuk meminimalkan kemungkinan pelanggaran dan kerugian terhadap mahasiswa maupun layanan keasramaan.
7.	**BAAK(Biro Administrasi Akademik dan Kemahasiswaan**	***Mitigation:*** Untuk menghindari resiko tersebut adalah dengan menerapkan tindakan keamanan, seperti enkripsi data, penggunaan firewall, pelatihan keamanan, dan langkah-langkah teknis lainnya yang dirancang untuk mencegah atau mengurangi potensi risiko terkait dengan keamanan data dan administrasi akademik pada BAAK.
8.	**Laboratorium**	***Mitigation:*** Untuk menghindari resiko tersebut adalah dengan memastikan keamanan laboratorium, pelatihan pengguna laboratorium, pengawasan yang ketat terhadap alat dan bahan laboratorium, serta pengambilan tindakan pencegahan untuk mengurangi kemungkinan terjadinya insiden keamanan dengan tujuan untuk mengendalikan risiko dan mengurangi potensi kerugian yang dapat timbul akibat ancaman pada laboratorium.
9.	**Informasi**	***Mitigation:*** Untuk menghindari resiko tersebut adalah dengan melakukan pemantauan keamanan, enkripsi data, serta pengelolaan terhadap akses ke sistem untuk mengetahui siapa aja yang mengakses sistem dan melakukan tindakan mencurigakan yang menyebabkan kebocoran informasi kampus.
10.	**Survei**	**Mitigation:** Untuk menghindari resiko tersebut adalah dengan memastikan informasi terkait pengisian kuesioner dan polling tersampaikan kepada mahasiswa agar mahasiswa maupun civitas IT Del tidak lupa untuk mengisinya.

3.2 Pembahasan

Aset merupakan komponen yang mencakup berbagai elemen, mulai dari perangkat keras yang mencakup server, komputer, dan perangkat jaringan, hingga perangkat lunak seperti aplikasi dan sistem operasi yang menjadi fondasi dari sistem informasi tersebut. Selain itu, aset juga melibatkan elemen data dan basis data yang merupakan harta berharga bagi organisasi. Namun, tidak hanya terbatas pada komponen teknis, aset juga mencakup sumber daya manusia yang terlibat dalam manajemen dan penggunaan sistem informasi. Auditor dalam proses audit sistem informasi akan menjalankan serangkaian evaluasi yang mencakup penilaian nilai aset ini, pemantauan perlindungan yang diberikan, serta manajemen dan pemeliharaan yang diterima. Selain itu, auditor akan memeriksa apakah organisasi telah menetapkan kebijakan dan prosedur yang sesuai untuk mengelola aset ini, dan sejauh mana aset-aset ini mendukung tujuan bisnis organisasi.

Selain itu, auditor akan melakukan penelusuran terhadap kepemilikan dan pemeliharaan aset. Dalam hal ini, auditor akan mengidentifikasi potensi risiko dan ancaman yang mungkin dapat mengancam keberlangsungan aset-aset tersebut. Risiko ini dapat berasal dari serangan siber, kegagalan perangkat keras, kerentanan perangkat lunak, hingga kesalahan manusia. Hasil audit ini kemudian akan didokumentasikan secara lengkap dan dilaporkan kepada manajemen organisasi. Laporan ini tidak hanya mengungkapkan temuan-temuan dari audit, melainkan juga memberikan pandangan yang sangat berharga bagi organisasi dalam hal bagaimana aset-aset mereka dikelola. Dengan demikian, organisasi dapat mengambil langkah-langkah konkret untuk memperbaiki manajemen aset, meningkatkan keamanan, serta meningkatkan efisiensi dalam penggunaan aset dalam konteks sistem informasi. Dengan aset yang dikelola dengan baik, organisasi akan dapat mengoptimalkan kinerja sistem informasi mereka dan meminimalkan risiko yang dapat terjadi.

Risk dalam konteks audit sistem informasi merujuk pada potensi ancaman atau ketidakpastian yang dapat mempengaruhi keberhasilan atau efektivitas audit tersebut. Audit sistem informasi adalah proses yang dirancang untuk mengevaluasi dan memeriksa sistem informasi suatu organisasi, termasuk infrastruktur teknologi, prosedur, dan kontrol yang ada. Risiko dalam audit sistem nformasi dapat berasal dari berbagai sumber dan memiliki dampak yang beragam.

Dalam audit sistem informasi, auditor harus mengidentifikasi, mengevaluasi, dan mengelola risiko-risiko ini agar dapat menyusun rencana audit yang efektif. Hal ini melibatkan pemahaman yang mendalam tentang sistem yang akan diaudit, pemahaman tentang potensi ancaman, dan langkah-langkah pengendalian yang telah diimplementasikan. Sebagai bagian dari proses audit, auditor juga harus menentukan tingkat risiko yang dapat diterima dan menyusun strategi audit yang sesuai. Penanganan risiko yang efektif dalam audit sistem informasi sangat penting untuk memastikan bahwa audit berjalan dengan baik dan memberikan nilai tambah bagi organisasi.

Probability (probabilitas) merupakan faktor penting dalam mengevaluasi risiko dan merencanakan audit. Probabilitas digunakan oleh auditor untuk mengukur sejauh mana suatu peristiwa atau kondisi yang berpotensi merugikan sistem informasi dapat terjadi. Sebagai contoh, auditor mungkin akan menilai probabilitas terjadinya serangan siber berdasarkan sejarah serangan sebelumnya, tingkat keamanan yang diterapkan, dan kerentanannya terhadap serangan. Dengan pemahaman yang baik mengenai probabilitas, auditor dapat mengidentifikasi risiko yang lebih tinggi dan fokus pada pengujian dan pemeriksaan yang lebih mendalam pada area tersebut, memastikan bahwa masalah yang paling berpotensi berdampak besar diperhatikan.

Setelah audit dilakukan, probabilitas juga digunakan untuk mengevaluasi temuan atau hasil audit. Auditor akan mempertimbangkan probabilitas terjadinya masalah yang ditemukan dan tingkat dampaknya pada sistem informasi. Hasil yang memiliki probabilitas tinggi dan dampak yang signifikan akan mendapatkan prioritas lebih tinggi dalam perencanaan tindakan korektif. Dengan demikian, probabilitas menjadi alat penting dalam pengelolaan risiko dan perbaikan sistem informasi untuk organisasi.

Dalam kerangka kerja COSO, *impact* atau dampak mengacu pada hasil atau konsekuensi yang dapat terjadi jika risiko-risiko yang terkait dengan sistem informasi CIS IT Del tidak dikelola dengan baik. Impact memiliki jenis yang beragam, termasuk kerugian finansial, kerusakan reputasi, gangguan operasional, atau bahkan pelanggaran hukum. COSO dapat membantu auditor untuk mengidentifikasi, mengevaluasi, dan mengelola risiko-risiko ini dengan cara yang efektif. Hal Ini termasuk mengembangkan kebijakan dan prosedur yang tepat, mengimplementasikan kontrol internal, serta melakukan pemantauan dan penilaian terhadap risiko-risiko tersebut. Dengan memahami dan mengelola dampak dari risiko-risiko dalam sistem informasi CIS. organisasi dapat menjaga keberlanjutan operasional, meminimalkan kerugian potensial, dan memastikan kepatuhan terhadap regulasi yang berlaku.

Dalam manajemen risiko, "P x I" (*Probability* x *Impact*) adalah metode yang berguna untuk mengukur sejauh mana risiko yang mungkin terjadi akan mempengaruhi Sistem Informasi CIS IT Del. Probabilitas (*Probability*) merujuk pada seberapa mungkin suatu risiko ak6an terjadi, sementara dampak (Impact) mengukur sejauh mana konsekuensi risiko tersebut akan Sistem Informasi CIS IT Del. Dengan mengalikan *probability* dengan *impact*, akan mendapatkan nilai numerik yang mengidentifikasikan tingkat risiko. Nilai ini membantu auditor dalam menentukan prioritas pengelolaan risiko.

Hasil dari "P x I" memungkinkan auditor untuk mengklasifikasikan risiko menjadi beberapa kategori. Risiko dengan hasil rendah umumnya dianggap kurang mendesak dan memerlukan perhatian yang lebih rendah, sedangkan risiko dengan hasil sedang memerlukan perencanaan pengelolaan risiko yang lebih rinci. Risiko dengan hasil tinggi, di sisi lain, dianggap sangat serius dan memerlukan tindakan segera dan strategi pengelolaan risiko yang kuat. Dengan menggunakan "P x I," auditor dapat dengan lebih efektif mengidentifikasi, mengevaluasi, dan mengelola risiko-risiko yang paling signifikan, memastikan bahwa sumber daya dialokasikan secara bijaksana untuk mengurangi dampak negatif potensial dan mencapai tujuan mereka.

Control dalam konteks CIS IT DEL adalah serangkaian langkah dan mekanisme yang sangat penting dalam mengelola risiko dan menjaga keamanan serta kinerja sistem informasi. Dalam lingkungan ini, *control* merujuk pada sejumlah tindakan, prosedur, dan kebijakan yang dirancang untuk meminimalkan potensi ancaman atau kerentanannya, melindungi integritas dan kerahasiaan data, serta memastikan bahwa sistem informasi beroperasi sesuai dengan standar yang ditetapkan oleh organisasi. Salah satu contoh *contro*l mencakup pengendalian akses, yang memastikan bahwa hanya individu yang berwenang memiliki akses ke data dan sistem; penggunaan enkripsi untuk melindungi data yang dipindahkan atau disimpan dalam sistem; pemantauan dan audit rutin untuk mendeteksi insiden dan memastikan kepatuhan terhadap kebijakan keamanan; serta perencanaan pemulihan bencana, yang memungkinkan organisasi untuk menghadapi gangguan serius dan memulihkan operasional dengan cepat.

4. Kesimpulan

Berdasarkan penilaian terhadap berbagai aspek operasional di Institut Teknologi Del mengungkap beberapa kesimpulan yang sangat penting. Audit yang telah dilakukan mencakup sejumlah aspek yang mencakup perbaikan layanan dalam *Campus Information System* (CIS), pengelolaan data pribadi mahasiswa, pengendalian internal, hingga keamanan dan kualitas fasilitas seperti asrama dan laboratorium.

Secara umum, IT Del telah menunjukkan komitmen yang kuat dalam menjaga keamanan data pada *Campus Information System* (CIS). Keseluruhan risiko yang telah diidentifikasi dalam konteks *Campus Information System* (CIS) di IT Del dapat dikelompokkan menjadi dua kategori utama. Pertama, ada risiko-risiko yang berkaitan erat dengan keamanan data dan informasi, termasuk ancaman terhadap data mahasiswa, data keuangan, dan keamanan dalam penggunaan laboratorium. Risiko-risiko dalam kategori ini memiliki tingkat keparahan dan dampak yang signifikan, mengingat potensi kerugian yang dapat ditimbulkan. Oleh karena itu, tindakan pencegahan dan perlindungan yang ketat sangat penting, seperti penerapan kebijakan keamanan yang kuat, penggunaan teknologi keamanan, dan pemantauan intensif.

Kedua, terdapat risiko-risiko yang lebih berfokus pada akses dan kelengkapan informasi, seperti kesulitan dalam mengakses materi pembelajaran, persyaratan program studi, dan pengisian kuesioner. Meskipun risiko-

risiko ini memiliki dampak yang lebih rendah, namun tetap memerlukan upaya dalam memberikan informasi yang lebih baik kepada mahasiswa, sehingga mereka dapat mengakses sumber daya dengan lebih mudah dan efisien. Dalam kedua kategori risiko ini, implementasi mitigasi yang efektif dan komprehensif akan memungkinkan IT Del untuk mengurangi potensi dampak negatif dan memastikan kelancaran operasi CIS serta keamanan data dan informasi secara menyeluruh. Dengan demikian, langkah-langkah ini akan membantu IT Del menjaga reputasinya sebagai lembaga pendidikan yang berfokus pada keamanan dan akses informasi yang baik.

5. Referensi

[1] Y. Rahmanto, F. Ulum, and B. Priyopradono, "Aplikasi Pembelajaran Audit Sistem Informasi Dan Tata Kelola Teknologi Informasi Berbasis Mobile," *J. Tekno Kompak*, vol. 14, no. 2, p. 62, 2020, doi: 10.33365/jtk.v14i2.723.

[2] T. E. Barus and N. S. P. Simamora, "Analisis Persebaran Pendaftar di Institut Teknologi Del Berdasarkan Asal Wilayah," *Pros. Ind. Res. ...*, pp. 26–27, 2020.

[3] A. C. Aydinoglu and T. Yomralioglu, "Web based *Campus Information System*," *Proc. Int. Symp. GIS Istanbul, ISBN 975-395-664-9*, vol. 6, no. November 2014, pp. 56–61, 2002.

[4] M. R. M. Dangi, A. Nawawi, and A. S. A. P. Salin, "Application of COSO *framework* in whistle-blowing activities of public higher-learning institutions," *Int. J. Law Manag.*, vol. 62, no. 2, pp. 193–211, 2020, doi: 10.1108/IJLMA-06-2017-0145.

[5] A. P. Rabhani *et al.*, "Audit Sistem Informasi Absensi Pada Kejaksaan Negeri Kota Bandung Menggunakan *Framework* Cobit 5," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 2, pp. 275–280, 2020, doi: 10.32736/sisfokom.v9i2.890.

[6] Y. Heningtyas, L. Fauziah, and A. Junaidi, "Audit Teknologi Informasi Pada Pt Xyz Menggunakan *Framework* Committee of Sponsoring Organizations of the Treadway Commission (Coso)," *Explor. J. Sist. Inf. dan Telemat.*, vol. 10, no. 1, 2019, doi: 10.36448/jsit.v10i1.1213.

[7] M. A. Saputra and N. Novita, "Sistem Pengendalian Internal Berdasarkan Coso *Framework* Pada Perusahaan Konstruksi," *J. Ris. Akunt. Politala*, vol. 6, no. 1, pp. 197–210, 2023, doi: 10.34128/jra.v6i1.148.

[8] R. P. Kusuma, "Audit Teknologi Informasi Menggunakan *Framework* Cobit 5 Pada Domain Dss (Deliver,Service, and Support) (Studi Kasus : Konsultan Manajemen Pusat)," *J. Digit*, vol. 9, no. 1, p. 97, 2020, doi: 10.51920/jd.v9i1.137.

[9] D. Stoel, D. Havelka, and J. W. Merhout, "An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners," *Int. J. Account. Inf. Syst.*, vol. 13, no. 1, pp. 60–79, 2012, doi: 10.1016/j.accinf.2011.11.001.

[10] Amalia Yunia Rahmawati, "**済無**No Title No Title No Title," no. July, pp. 1–23, 2020.

[11] M. K. N. Sengari, M. N. Dince, and Y. D. P. Rangga, "Evaluasi Penerapan Sistem Pengendalianinternal Persediaan Barang Dagang Dengan Coso *Framework* Pada Pintu Air Swalayan Maumere," *J. Ris. Manaj. dan Akunt.*, vol. 3, no. 2, pp. 54–66, 2023, doi: 10.55606/jurima.v3i2.2175.

[12] V. N. Sia, "Penerapan Model Coso Untuk Peningkatan Fungsi Pengendalian Internal: Studi Pada Agency Administração De Aeroporto E Navegação Aérea De Timor-Leste," *J. Ekon. dan Bisnis Airlangga*, vol. 29, no. 2, pp. 142–169, 2019, doi: 10.20473/jeba.V29I22019.6220.

[13] X. D. Crystallography, "AUDIT TEKNOLOGI INFORMASI PADA PT TUNAS DWIPA MATRA MENGGUNAKAN *FRAMEWORK* COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO)," pp. 1–23, 2016