JURNAL SISFOTENIKA
Vol. 15 No. 1, Januari 2025
p-ISSN: 2087-7897 ; e-ISSN : 2460-5344
DOI : 10.30700/sisfotenika.v15i1.535

Audit Pengendalian Batasan Sistem Informasi Manajemen Keuangan Menggunakan Kerangka Kerja COSO

Audit of Boundary Control in Financial Management Information Systems Using COSO Framework

Agus Eko Musantono*[1], Yoyon Arie Budi Suprio[2], Rhegysa Alvyanthi Juniartha[3], Arienta Aulia Hapsari[4]
[1,2,3,4]Program Studi Teknik Informatika, STIKOM PGRI Banyuwangi, Banyuwangi
e-mail: *[1]**vizardantoni@gmail.com**, [2]yoyonstikom@gmail.com,
[3]rhegysajuniartha@gmail.com, [4]arientaulia28@gmail.com

Abstrak

Sistem Informasi Manajemen Keuangan merupakan suatu implementasi Teknologi Informasi yang dapat memberikan manfaat juga berpotensi menimbulkan risiko yang dapat merugikan proses bisnis perusahaan. Evaluasi pengendalian batasan sistem informasi manajemen keuangan di PT Lokabyte Digital Innovations perlu dilakukan untuk meminimalisir terjadinya risiko. Pendekatan dilakukan secara langsung pada sistem informasi menggunakan audit through computer dengan berfokus pada tahapan pengendalian batasan (boundary control). Kelemahan utama pada sistem manajemen keuangan PT Lokabyte Digital Innovations meliputi kurangnya pembatasan akses pengguna, pengelolaan umur password, serta otomatisasi sistem saat kesalahan input terjadi. Hasil dari evaluasi sistem informasi manajemen keuangan didapatkan bahwa penerapan boundary control pada PT Lokabyte Digital Innovations memiliki 13 temuan yang terdiri dari 7 temuan positif dan 6 temuan negatif dengan tingkat efektivitas sebesar 58,3% dan berada pada kategori cukup baik. Rekomendasi penelitian yang diberikan mencakup penguatan kebijakan keamanan seperti penerapan otentikasi dua faktor, pembatasan panjang password dan notifikasi masa berlaku password.

Kata kunci*—Sistem Informasi, Manajemen Keuangan, Teknologi Informasi, Pengendalian Batasan, Audit Through The Computer*

Abstract

The Financial Management Information System is an implementation of Information Technology that can provide benefits but also poses risks that may harm a company's business processes. An evaluation of boundary control in the financial management information system at PT Lokabyte Digital Innovations is essential to minimize potential risks. The approach was directly applied to the information system using an audit through the computer method, focusing on boundary control stages. The primary weaknesses identified in PT Lokabyte Digital Innovations' financial management system include inadequate user access restrictions, poor password age management, and a lack of system automation to address input errors. The evaluation results revealed that the implementation of boundary control at PT Lokabyte Digital Innovations identified 13 findings, consisting of 7 positive findings and 6 negative findings, with an effectiveness level of 58.3%, categorized as moderately effective. The study recommends

strengthening security policies, such as implementing two-factor authentication, setting password length restrictions, and introducing password expiration notifications.

Keywords—*Information System, Financial Management, Information Technology, Boundary Control, Audit Through The Computer*

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mendorong perusahaan untuk semakin mengandalkan sistem informasi dalam mengelola aspek-aspek operasionalnya, termasuk manajemen keuangan[1,2]. Dalam lingkungan bisnis yang semakin kompleks, risiko keamanan data dan integritas informasi menjadi perhatian utama[3]. PT Lokabyte Digital Innovations, sebagai perusahaan yang bergerak di bidang jasa optimasi produk bisnis seperti branding dan digital marketing, memerlukan sistem informasi manajemen keuangan yang tidak hanya efisien tetapi juga mampu mengendalikan risiko terkait keamanan dan akurasi data[4]. Pengelolaan sistem informasi keuangan yang tidak memadai dapat mengakibatkan kerugian finansial, gangguan operasional, dan kerentanan terhadap ancaman eksternal maupun internal[5,6].

Framework COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) merupakan salah satu standar yang banyak digunakan dalam pengelolaan pengendalian internal, termasuk pengendalian sistem informasi[7,8]. *Framework* ini terdiri dari lima elemen utama yaitu lingkungan pengendalian, penilaian risiko, aktivitas pengendalian, informasi dan komunikasi, serta pemantauan[9,10,11]. Salah satu implementasi penting dari *framework* COSO adalah *boundary control*, yaitu pengendalian yang memastikan semua aktivitas sistem informasi berada dalam batas yang telah ditetapkan untuk mengurangi risiko kesalahan atau penyalahgunaan[12,13]. Studi sebelumnya yang dilakukan pada Kemkominfo Banyuwangi, menunjukkan efektivitas *framework* COSO dalam memperkuat pengendalian sistem informasi dan meningkatkan keandalan laporan keuangan[1].

Meski *framework* COSO telah terbukti efektif, penerapannya sering menghadapi tantangan dalam implementasi praktis, khususnya pada perusahaan yang baru memulai integrasi pengendalian berbasis teknologi informasi[14]. PT Lokabyte Digital Innovations menghadapi masalah serupa, dengan beberapa kelemahan pada sistem pengendalian yang dapat mengancam integritas sistem informasi keuangannya. Oleh karena itu, dilakukan observasi menggunakan pendekatan *audit through the computer* untuk mengevaluasi sejauh mana kesesuaian penerapan *framework* COSO pada perusahaan ini dan memberikan rekomendasi yang lebih sistematis dan terstruktur dalam mengelola kontrol di dalam sistem informasi manajemen keuangan. Audit through the computer merupakan pendekatan audit sistem informasi yang berfokus pada proses evaluasi sistem komputer dan aplikasi perangkat lunak yang digunakan untuk memproses data[15]. Pendekatan ini melibatkan pemeriksaan terhadap bagaimana sistem aplikasi bekerja, termasuk input, pemrosesan, dan output data, dengan tujuan untuk menilai apakah kontrol internal sistem tersebut telah berjalan efektif dan data yang dihasilkan dapat dipercaya.

Penelitian ini bertujuan untuk memberikan jawaban atas tiga pertanyaan utama terkait tingkat implementasi *boundary control* dalam sistem informasi manajemen keuangan di PT Lokabyte Digital Innovations. Fokus utama penelitian ini adalah menganalisis sejauh mana mekanisme *boundary control* telah diterapkan sesuai dengan standar yang diharapkan, mengidentifikasi kelemahan atau kekurangan dalam pengendalian yang diterapkan, serta mengeksplorasi solusi yang tepat untuk mengatasi permasalahan tersebut. Selain itu, penelitian ini juga bertujuan untuk mengevaluasi bagaimana *framework* COSO dapat menjadi panduan strategis bagi perusahaan dalam memperkuat aspek keamanan, meningkatkan efisiensi, serta memastikan kepatuhan terhadap pengelolaan sistem informasi manajemen keuangan. Dengan

demikian, hasil penelitian ini diharapkan mampu memberikan kontribusi signifikan dalam pengembangan praktik pengendalian internal yang lebih efektif dan berkelanjutan di PT Lokabyte Digital Innovations

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus untuk menganalisis secara mendalam penerapan *boundary control* dalam sistem informasi manajemen keuangan di PT Lokabyte Digital Innovations. Pendekatan ini dirancang untuk memberikan pemahaman yang mendalam mengenai bagaimana mekanisme *boundary control* diimplementasikan, tantangan apa saja yang dihadapi selama proses tersebut, serta dampak langsung maupun tidak langsung dari implementasi tersebut terhadap efektivitas pengelolaan keuangan perusahaan. Dengan menggunakan metode studi kasus, penelitian ini memungkinkan pengumpulan data yang komprehensif dan kontekstual, sehingga mampu mengungkap hubungan antara pengendalian internal dan keberhasilan sistem informasi. Teknik penelitian yang diterapkan meliputi:

2.1 Pengumpulan Data

2.1.1 Wawancara Mendalam

Wawancara dilakukan dengan pengelola sistem informasi keuangan guna menggali pemahaman yang lebih mendalam mengenai penerapan *boundary control*, termasuk mekanisme pengendalian yang digunakan, tantangan yang dihadapi dalam implementasinya, serta kebijakan strategis yang diterapkan untuk mengatasi hambatan dan memastikan keberlanjutan sistem tersebut.

2.1.2 Kuisioner Terstruktur

Instrumen kuesioner disusun secara sistematis berdasarkan kriteria *boundary control* yang terdapat dalam *framework* COSO, dengan tujuan untuk mengukur secara komprehensif tingkat penerapan pengendalian pada sistem informasi. Desain kuesioner mencakup berbagai indikator utama yang merepresentasikan aspek-aspek pengendalian, sehingga mampu memberikan gambaran yang akurat mengenai efektivitas dan konsistensi implementasi *boundary control* dalam mendukung pengelolaan sistem informasi. Instrumen dapat dilihat pada Tabel 1.

Tabel 1. Instrumen Pengendalian Batasan (*Boundary Control*)

No	**Pertanyaan Atas Segmentasi Pengendalian Batasan (*Boundary Control*)**
1.	Apakah Sistem Aplikasi dilengkapi dengan *login* akses seperti *user*name dan *password*?
2.	Apakah sistem menampilkan pesan jika verifikasi *login* tidak valid?
3.	Apakah Sistem Aplikasi membatasi ukuran field (panjang maksimal) terhadap *login* akses (*user*name dan *password*) ?
4.	Apakah *password* yang diketik tidak terlihat (*invisible*)?
5.	Apakah sistem hanya dapat diakses oleh orang orang yang terotorisasi?
6.	Apakah ada pembatasan sistem dalam penginputan *login* akses (*username* dan *password*) dan berapa kali batas salah penginputan *login*?
7.	Jika ya, Apakah sistem memberikan respon dengan menutup secara otomatis sistem aplikasi tersebut (otomatis keluar dari sistem aplikasi tersebut)?
8.	Apakah terdapat batasan kewenangan *user* dalam mengakses aplikasi ? Lakukan

	pengecekan, apakah ada setting menu untuk kewenangan *user* atau management *user*?
9.	Apakah *password* memiliki batasan umur *password* ?
10.	Jika ya, apakah sistem aplikasi menampilkan pesan jika *password* tersebut sudah berakhir (expired) ?
11.	Apakah sistem aplikasi jelas ruang lingkupnya (apa dokumen inputnya, dari mana sumbernya, tujuan pengolahan data, siapa para penggunanya, dan siapa pemegang kewenangan)?
12.	Apakah *login* akses pada Sistem Aplikasi seperti *password* di enkripsi?
13.	Apakah terdapat program untuk merekam semua kegiatan dalam komputer? (semacam *log file*) Jika ya, siapa saja yang mengetahui program tersebut?

2.1.3 Observasi Langsung

Observasi dilakukan dengan menggunakan pendekatan *audit through the computer*, yang difokuskan pada analisis *boundary control* dalam sistem informasi yang sedang berjalan. Pendekatan ini bertujuan untuk mengidentifikasi secara rinci implementasi mekanisme pengendalian yang diterapkan, mengevaluasi efektivitasnya dalam mendukung tujuan organisasi, serta mengungkap potensi kelemahan atau area yang memerlukan perbaikan. Observasi ini mencakup peninjauan langsung terhadap proses, prosedur, dan kebijakan yang berkaitan dengan pengelolaan *boundary control*, sehingga mampu memberikan wawasan yang lebih komprehensif mengenai kinerja sistem informasi tersebut.

2.2 Analisis Data

Proses analisis data dalam penelitian ini dilakukan dengan menggunakan pendekatan deskriptif kualitatif, yang bertujuan untuk memahami penerapan *boundary control* berdasarkan kriteria yang telah ditetapkan dalam *framework* COSO. Kriteria tersebut mencakup beberapa indikator penting sebagai berikut:

a) Sistem aplikasi telah dilengkapi dengan fitur *login* akses sebagai mekanisme utama pengendalian keamanan, yang menjadi pintu awal untuk memastikan hanya pengguna yang berwenang yang dapat mengakses sistem.
b) Sistem dapat menolak akses secara otomatis jika pengguna tidak memiliki otorisasi yang sah, sehingga memastikan bahwa hanya pengguna yang telah diverifikasi yang dapat mengakses data atau fungsi sistem.
c) Terdapat pembatasan jumlah kesalahan input yang dapat dilakukan saat login, di mana pembatasan ini berfungsi untuk mencegah upaya peretasan atau akses ilegal oleh pihak yang tidak berwenang.
d) Sistem memberikan pesan kesalahan atau error message yang informatif kepada pengguna ketika terjadi kesalahan input, sehingga pengguna dapat memahami penyebab kegagalan akses dan melakukan perbaikan yang diperlukan.
e) Sistem Aplikasi dirancang untuk menutup atau keluar secara otomatis setelah jumlah kesalahan input login mencapai batas maksimal, sebagai langkah pengamanan tambahan untuk mencegah eksploitasi sistem.
f) Terdapat pembatasan tingkat kewenangan pengguna dalam mengakses aplikasi, di mana akses ke fitur atau data tertentu dibatasi berdasarkan peran atau tanggung jawab pengguna, untuk memastikan pengelolaan hak akses yang terkontrol dan sesuai dengan kebijakan perusahaan.

Analisis dilakukan melalui dua tahap utama. Pada tahap pertama, elemen-elemen pengendalian yang telah berhasil memenuhi kriteria *framework* COSO dikategorikan sebagai temuan positif. Temuan ini mencerminkan keberhasilan implementasi mekanisme pengendalian yang sesuai dengan standar yang diharapkan. Sebaliknya, elemen-elemen yang menunjukkan

adanya kekurangan, kelemahan, atau potensi risiko yang dapat berdampak pada efektivitas sistem dikategorikan sebagai temuan negatif. Proses klasifikasi ini bertujuan untuk memberikan gambaran awal mengenai aspek-aspek yang telah berfungsi dengan baik dan area-area yang memerlukan perhatian lebih lanjut

Tahap kedua berfokus pada evaluasi tingkat efektivitas pengendalian yang telah diterapkan, dengan menggunakan indikator keberhasilan yang telah ditentukan. Proses ini mencakup analisis mendalam mengenai sejauh mana *boundary control* yang diterapkan dapat mendukung tujuan sistem informasi, baik dari segi keamanan, efisiensi, maupun kepatuhan terhadap kebijakan perusahaan. Evaluasi ini juga mencakup penghitungan tingkat efektivitas secara keseluruhan, yang diharapkan dapat memberikan wawasan berharga bagi manajemen perusahaan. Hasil dari tahap ini tidak hanya membantu dalam mengidentifikasi kesenjangan dalam pengendalian yang ada tetapi juga memberikan rekomendasi strategis untuk perbaikan di masa depan.

$$\left(\frac{\Sigma temuan\ positif}{\Sigma pengujian - \left(\frac{N}{A}\right)}\right) x\ 100\% \quad (1)$$

Keterangan:

∑ temuan positif= jumlah dari data temuan yang bernilai positif

∑ temuan pengujian = jumlah dari instrumen data uji yang dilakukan

N/A = *not applicable*

Tabel 2. Kriteria Penilaian Pengendalian COSO

Nilai	Keterangan
67-100	Baik Sekali
34-66	Cukup Baik
0-33	Kurang Baik

Dapat dilihat pada Tabel 2, hasil evaluasi diklasifikasikan ke dalam tiga kategori berdasarkan tingkat pencapaian efektivitas pengendalian yang diukur menggunakan skala yang telah diadaptasi dari *framework* COSO. Kategori tersebut meliputi baik sekali (dengan rentang nilai 67-100%), yang mencerminkan pengendalian yang telah berjalan secara optimal sesuai standar yang diharapkan; cukup baik (rentang nilai 34-66%), yang menunjukkan adanya pengendalian yang cukup efektif tetapi masih memerlukan beberapa perbaikan; dan kurang baik (rentang nilai 0-33%), yang mengindikasikan kelemahan signifikan dalam implementasi pengendalian yang perlu segera diperbaiki.

2.3 Rekomendasi Hasil Temuan

Berdasarkan hasil analisis yang telah dilakukan, rekomendasi diberikan untuk mengatasi temuan yang diidentifikasi untuk meningkatkan efektivitas pengendalian internal perusahaan. Rekomendasi yang diberikan dirancang secara spesifik untuk memperkuat mekanisme *boundary control* yang saat ini diterapkan oleh PT Lokabyte Digital Innovations. Upaya penguatan ini mencakup penyempurnaan prosedur pengelolaan akses, peningkatan keamanan login, pengaturan kewenangan pengguna yang lebih terstruktur, serta penerapan kebijakan yang lebih ketat terkait pembatasan dan pemantauan aktivitas sistem. Dengan implementasi rekomendasi dari hasil temuan yang ada, diharapkan perusahaan dapat mencapai

standar pengendalian internal yang lebih tinggi, meminimalkan potensi risiko, dan mendukung keberlanjutan operasional sistem informasi secara lebih optimal.

3. HASIL DAN PEMBAHASAN

Hasil analisis terhadap sistem informasi manajemen keuangan PT Lokabyte Digital Innovations dengan menggunakan *framework* COSO mengungkapkan sejumlah temuan penting terkait implementasi *boundary control*. Temuan ini mencakup aspek-aspek utama yang mencerminkan efektivitas pengendalian, potensi kelemahan, serta peluang untuk peningkatan. Data yang disajikan dalam Tabel 3 telah disusun secara sistematis dan logis untuk memberikan gambaran yang komprehensif mengenai kondisi pengendalian saat ini, sehingga memudahkan identifikasi area yang perlu diperbaiki maupun dipertahankan.

Tabel 3. Data Temuan

Kategori Pengendalian	**Temuan**
Pengendalian Batasan (*Boundary controls*)	Sistem aplikasi telah dilengkapi dengan fitur *login* akses yang menggunakan *username* dan *password* sebagai mekanisme autentikasi awal.
	Password pada sistem aplikasi dirancang agar tidak terlihat (*invisible*) saat diketik untuk menjaga kerahasiaan pengguna.
	Sistem aplikasi menampilkan pesan yang jelas apabila proses verifikasi login tidak valid, membantu pengguna memahami kesalahan yang terjadi.
	Pengaksesan sistem hanya dapat dilakukan oleh individu yang telah mendapatkan otorisasi resmi dan diberikan wewenang sesuai dengan kebijakan perusahaan.
	Login akses pada sistem telah dilengkapi dengan teknologi enkripsi untuk memastikan keamanan data pengguna.
	Tidak ada kebijakan untuk menampilkan notifikasi kepada pengguna jika *password* telah kedaluwarsa, sehingga pengguna tidak mendapatkan peringatan untuk memperbarui kredensial mereka.
	Tidak terdapat pembatasan pada panjang maksimal *field* untuk *username* dan *password*, sehingga berpotensi membuka celah keamanan.
	Tidak ada batasan jumlah kesalahan saat penginputan login akses, yang dapat membuka peluang percobaan akses tidak sah melalui teknik brute force.
	Sistem aplikasi dilengkapi dengan program log file yang berfungsi untuk merekam aktivitas pengguna dalam sistem, memberikan jejak audit untuk analisis lebih lanjut jika terjadi pelanggaran atau kesalahan.
	Tidak ada kebijakan terkait pembatasan usia password (*password expiration*), yang dapat meningkatkan risiko penggunaan *password* yang tidak aman dalam jangka waktu panjang.
	Sistem tidak dirancang untuk menutup atau keluar secara otomatis setelah jumlah kesalahan login melebihi batas tertentu, yang dapat meningkatkan risiko keamanan.

	Ruang lingkup sistem aplikasi telah didefinisikan dengan jelas sesuai prosedur, termasuk dokumen input, sumber data, tujuan pemrosesan, dan pengguna yang terlibat.
	Tidak terdapat pengaturan yang membatasi kewenangan pengguna dalam mengakses aplikasi sesuai dengan tingkat otorisasi yang ditentukan, yang dapat menyebabkan risiko akses tidak sah ke data atau fitur yang sensitif.

Langkah selanjutnya dalam analisis adalah mengklasifikasikan data temuan berdasarkan kategori *boundary control* untuk mengidentifikasi elemen-elemen pengendalian yang menunjukkan hasil positif maupun negatif. Temuan bernilai positif mencerminkan kelebihan atau keberhasilan sistem aplikasi dalam memenuhi kriteria pengendalian, sedangkan temuan negatif mengindikasikan kelemahan, potensi risiko, atau area yang memerlukan perbaikan lebih lanjut. Proses klasifikasi ini bertujuan untuk memberikan pemahaman yang terperinci mengenai aspek-aspek pengendalian yang telah berjalan dengan baik dan yang masih perlu ditingkatkan. Berikut hasil klasifikasi temuan positif secara lengkap disajikan pada Tabel 4.

Tabel 4. Klasifikasi Temuan Positif

Kategori Pengendalian	**Positif**
Pengendalian Batasan (*Boundary controls*)	Sistem aplikasi telah dilengkapi dengan fitur login akses yang menggunakan *username* dan *password* sebagai mekanisme autentikasi awal.
	Password pada sistem aplikasi dirancang agar tidak terlihat (*invisible*) saat diketik untuk menjaga kerahasiaan pengguna.
	Sistem aplikasi menampilkan pesan yang jelas apabila proses verifikasi login tidak *valid*, membantu pengguna memahami kesalahan yang terjadi.
	Login akses pada sistem telah dilengkapi dengan teknologi enkripsi untuk memastikan keamanan data pengguna.
	Pengaksesan sistem hanya dapat dilakukan oleh individu yang telah mendapatkan otorisasi resmi dan diberikan wewenang sesuai dengan kebijakan perusahaan.
	Sistem aplikasi dilengkapi dengan program *log file* yang berfungsi untuk merekam aktivitas pengguna dalam sistem, memberikan jejak audit untuk analisis lebih lanjut jika terjadi pelanggaran atau kesalahan.
	Ruang lingkup sistem aplikasi telah didefinisikan dengan jelas sesuai prosedur, termasuk dokumen input, sumber data, tujuan pemrosesan, dan pengguna yang terlibat.

Tabel 5 menyajikan klasifikasi temuan negatif yang menunjukkan kelemahan dalam penerapan pengendalian batasan (*boundary controls*), seperti tidak adanya pembatasan kewenangan pengguna, pengaturan umur *password*, batasan kesalahan login, serta mekanisme otomatis untuk menutup aplikasi setelah kesalahan melebihi batas yang ditentukan.

Tabel 5. Klasifikasi Temuan Negatif

Kategori Pengendalian	**Negatif**
Pengendalian	Tidak terdapat pengaturan yang membatasi kewenangan pengguna

Batasan (*Boundary controls*)	dalam mengakses aplikasi sesuai dengan tingkat otorisasi yang ditentukan, yang dapat menyebabkan risiko akses tidak sah ke data atau fitur yang sensitif.
	Tidak terdapat pembatasan pada panjang maksimal *field* untuk *username* dan *password*, sehingga berpotensi membuka celah keamanan.
	Tidak ada kebijakan terkait pembatasan usia password (*password expiration*), yang dapat meningkatkan risiko penggunaan *password* yang tidak aman dalam jangka waktu panjang.
	Tidak ada batasan jumlah kesalahan saat penginputan *login* akses, yang dapat membuka peluang percobaan akses tidak sah melalui teknik *brute force*.
	Tidak ada kebijakan untuk menampilkan notifikasi kepada pengguna jika *password* telah kedaluwarsa, sehingga pengguna tidak mendapatkan peringatan untuk memperbarui kredensial mereka.
	Sistem tidak dirancang untuk menutup atau keluar secara otomatis setelah jumlah kesalahan login melebihi batas tertentu, yang dapat meningkatkan risiko keamanan.

Berdasarkan data temuan yang disajikan pada Tabel 4 dan Tabel 5, langkah selanjutnya adalah melakukan penilaian untuk mengukur tingkat efektivitas pengendalian yang diterapkan. Penilaian ini dilakukan dengan menggunakan rumus yang telah diadaptasi dari framework COSO(1), yang dirancang untuk memberikan evaluasi kuantitatif terhadap implementasi pengendalian. Proses perhitungan mencakup analisis terhadap elemen-elemen positif dan negatif, yang kemudian diintegrasikan untuk memberikan skor keseluruhan mengenai efektivitas sistem. Perhitungan dilakukan sebagai berikut:

$$\frac{7}{13}\ x\ 100\% = 53{,}85\% \quad (2)$$

Commented [UC1]: Angka 7 dan 13 dari mana harus dimunculkan perhitungannya sehingga kelihatan bahwa angka 7 dan 13 asalnya

Adapun hasil akhir dari penilaian yang diperoleh melalui perhitungan yang telah dilakukan(2) dirangkum secara sistematis dan disajikan dalam Tabel 6. Tabel ini memberikan gambaran yang jelas mengenai tingkat efektivitas pengendalian yang diukur, sekaligus mengidentifikasi elemen-elemen yang memerlukan perhatian lebih lanjut untuk meningkatkan kinerja sistem.

Tabel 6. Hasil Penilaian Pengendalian Batasan

Kategori Pengendalian	Jumlah Pengujian	Temuan Positif	Nilai	Kriteria
Pengendalian batasan (*Boundary control*)	13	7	53,8	Cukup Baik

Hasil menunjukkan bahwa validasi login telah diterapkan dengan baik melalui enkripsi *password* dan notifikasi error untuk verifikasi yang tidak valid. Namun, pengaturan panjang maksimal *username* dan *password* belum diterapkan, sehingga berpotensi meningkatkan risiko keamanan terhadap serangan *brute force*. Kemudian untuk pengelolaan akses menggunakan manajemen user sudah cukup memadai. Namun, kurangnya kebijakan umur *password* dan notifikasi *expired password* menciptakan celah keamanan, terutama jika *password* lama tetap

digunakan tanpa pembaruan. Berikutnya tentang kesalahan input login dan otomatisasi sistem, tidak adanya batasan jumlah kesalahan login dan fitur otomatis keluar berpotensi meningkatkan risiko akses tidak sah. Otomatisasi sistem ini penting untuk mencegah eksploitasi sistem oleh pihak yang tidak berwenang. Dan yang terakhir, ketersediaan *log file* memberikan catatan aktivitas yang dapat digunakan untuk audit dan pemantauan. Namun, pengelola sistem perlu memastikan bahwa *log file* dilindungi dan tidak mudah diakses oleh pihak yang tidak berwenang.

Berdasarkan hasil penelitian, implementasi *boundary control* di PT Lokabyte menunjukkan efektivitas pada beberapa aspek dasar, tetapi masih terdapat kekurangan yang signifikan. Untuk itu, diberikan rekomendasi tindak lanjut untuk meminimalisir kekurangan yang signifikan tersebut. Rekomendasi dapat dilihat pada Tabel 7.

Tabel 7. Rekomendasi Hasil Temuan

Temuan	**Rekomendasi Hasil Temuan**
Tidak ada batasan-batasan terhadap kewenangan *user* dalam mengakses aplikasi.	Gunakan otentikasi dua faktor, untuk melindungi akun pengguna agar batasan-batasan terhadap kewenangan pengguna dalam mengakses aplikasi tetap terjaga.
*User*name dan *password* pada sistem aplikasi tidak membatasi *field* atau ukuran panjang maksimal.	Tetapkan panjang karakter minimal dan maksimal untuk *user*name. Misalnya, minimal 6 karakter dan maksimal 20 karakter. Pastikan *password* mengandung kombinasi huruf, angka, dan simbol.
Tidak ada kebijakan dalam pembatasan sistem umur *password*.	Tentukan jangka waktu tertentu (misalnya, setiap 90 hari) untuk mengganti *password*. Jangan izinkan pengguna untuk menggunakan kembali *password* lama dalam beberapa siklus penggantian.
Tidak ada pembatasan kesalahan dalam penginputan *login* akses berupa *user*name dan *password*.	Batasi jumlah percobaan *login* menjadi maksimal 3–5 kali berturut-turut. Tambahkan lapisan keamanan berupa kode OTP (*One-Time Password*) yang dikirimkan melalui email atau SMS setelah *login* berhasil dilakukan.
Tidak ada kebijakan dalam menampilkan pesan jika *password* telah berakhir (*expired*).	Kirimkan notifikasi kepada pengguna secara otomatis beberapa hari sebelum masa berlaku password berakhir, sehingga dapat mencegah potensi gangguan akses dan memastikan keamanan sistem tetap terjaga.
Sistem aplikasi tidak akan menutup secara otomatis karena sistem aplikasi tidak ada pembatasan sistem kesalahan.	Atur agar aplikasi dapat menutup diri secara otomatis ketika terjadi kesalahan yang kritis atau ketika kondisi tertentu terpenuhi (misalnya, kehabisan memori). Sebelum menutup, pastikan data yang sedang diproses disimpan dengan aman untuk menghindari kehilangan data.

4. KESIMPULAN

Hasil yang didapatkan dalam penelitian ini menunjukkan bahwa penerapan *boundary control* dalam sistem informasi manajemen keuangan PT Lokabyte Digital Innovations memiliki sebanyak 13 temuan yang terdiri dari 7 temuan positif dan 6 temuan negatif. Dengan tingkat efektivitas sebesar 58,3% dan berada pada kategori cukup baik. Hasil ini mengindikasikan perlunya peningkatan dalam implementasi *boundary control* untuk memperkuat keamanan data, mengurangi risiko akses tidak sah, dan memastikan kepatuhan

Commented [UC2]: Dari mana angka 58.3% ini.kalau sudah jelas maka munculkan juga di abstraknya

terhadap regulasi yang berlaku. Penggunaan *framework* COSO dalam penelitian ini telah memberikan panduan yang relevan untuk meningkatkan efektivitas pengendalian sistem informasi, khususnya pada aspek pengelolaan akses pengguna, pembaruan *password*, dan otomatisasi sistem. Rekomendasi hasil temuan yang telah diberikan diharapkan mampu memberikan hasil yang lebih signifikan dalam mendukung keamanan dan efisiensi sistem informasi manajemen keuangan PT Lokabyte Digital Innovations.

5. SARAN

Pada penelitian selanjutnya dapat dikembangkan dengan mengkombinasikan *framework* COSO dengan *framework* lain guna memperoleh pendekatan yang lebih komprehensif. Metode audit sistem informasi yang digunakan dalam penelitian ini dapat dimodifikasi dengan mengadopsi pendekatan *Audit Around the Computer* atau *Audit With the Computer*. Pendekatan *Audit Around the Computer* memungkinkan auditor untuk memfokuskan evaluasi pada input dan output sistem tanpa perlu menganalisis logika internal program, sementara *Audit With the Computer* melibatkan penggunaan alat bantu audit untuk memeriksa proses dan logika sistem secara lebih rinci. Modifikasi ini diharapkan tidak hanya memberikan sudut pandang yang lebih luas tetapi juga menghasilkan temuan yang lebih mendalam, yang dapat digunakan sebagai landasan untuk meningkatkan keamanan dan efektivitas sistem informasi manajemen keuangan dimasa depan.

DAFTAR PUSTAKA

[1] A. E. Musantono, B. S. W. A. Soedijono, and A. Nasiri, "Evaluasi Pengendalian Aplikasi Pada Sistem Informasi Manajemen Keuangan Menggunakan Framework COSO," vol. 5, pp. 1–6, 2019.

[2] Sontri and D. Antoni, "Analisis Pengukuran Tingkat Kematangan Tata Kelola Sistem Informasi Manajemen Keuangan Daerah (SIMDA Keuangan) Menggunakan Cobit 5 (Studi Kasus : Badan Pengelola Keuangan Dan Aset Daerah Kabupaten Musi Banyuasin)," *J. Ilm. Inform. Glob.*, vol. 14, no. 2, pp. 1–7, 2023.

[3] S. H. Sugiarto and S. Ratih, "Analisis Sistem Pengendalian Internal Terhadap Penjualan di Cv Depo Jaya Stationery Surabaya Berdasarkan Komponen Coso – Integrated Framework," *J. Syntax Imp. J. Ilmu Sos. dan Pendidik.*, vol. 4, no. 3, pp. 301–310, 2023, doi: 10.36418/syntax-imperatif.v4i3.263.

[4] D. Fitriani and H. Hwihanus, "Pengaruh Sistem Informasi Akuntansi Dalam Penerapan Siklus Produksi Dan Pengendalian Internal Untuk Meningkatkan Efektivitas Kinerja UMKM," *J. Kaji. dan Penal. Ilmu Manaj.*, vol. 1, no. 1, 2023.

[5] R. I. Fanani, I. Aknuranda, and Y. T. Mursityo, "Pengembangan Sistem Informasi Manajemen Keuangan Peternakan Kambing (Studi Kasus: Yoga's Farm Kabupaten Tulungagung)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 4, pp. 4033–4039, 2019, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/download/5110/2447/

[6] F. O. Voets, J. J. Sondakh, and A. Wangkar, "Analisis Sistem Informasi Akuntansi Siklus Penjualan dan Penerimaan Kas Untuk Meningkatkan Pengendalian Interen Pada PT. Sumber Alfaria Trijaya, Tbk (Alfamrat) Cabang Manado," *J. Berk. Ilm. Efisiensi*, vol. 16, no. 4, pp. 194–195, 2016.

[7] T. H. Thabit, A. Solaimanzadah, and M. T. Al-Abood, "The Effectiveness of COSO Framework to Evaluate Internal Control System: The Case of Kurdistan Companies," *Cihan Int. J. Soc. Sci.*, vol. 1, no. 1, pp. 44–54, 2017.

[8] Z. Aini, N. Nurwijayanti, S. Supriyanto, and H. E. Susanto, "Strategi Pengembangan Transformasi Sistem Informasi Manajemen Rumah Sakit (SIM-RS) di RSUD dr. Iskak Tulungagung," *J. Community Engagem. Heal.*, vol. 5, no. 2, pp. 128–139, 2022, doi:

10.30994/jceh.v5i22.383.

[9] Oluwaseun Oladeji Olaniyi and Dagogo Sopriala Omubo, "The Importance of COSO Framework Compliance in Information Technology Auditing and Enterprise Resource Management," *Int. J. Innov. Res. Dev.*, vol. 12, no. 5, pp. 1–6, 2023, doi: 10.24940/ijird/2023/v12/i5/may23001.

[10] 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.

[11] S. Mudzalifah and A. Subandoro., "Analisis Sistem Informasi Akuntansi Piutang dan Sistem Pengendalian Internal Piutang Pada Perusahaan Kontruksi Di Surabaya (Studi kasus PT. Sarana Remaja Mandiri)," *J. Ekon. Manajemen, Bisnis dan Sos. E-ISSN 2747-0938*, vol. 2, no. 3, pp. 303–310, 2022, [Online]. Available: https://www.embiss.com/index.php/embiss/article/view/95/73

[12] S. Susilawati, "Pengaruh Profesionalisme Dan Independensi Auditor Internal Terhadap Kualitas Audit: Studi Pada Inspektorat Propinsi Jawa Barat," *Etikonomi*, vol. 13, no. 2, pp. 190–210, 2015, doi: 10.15408/etk.v13i2.1886.

[13] T. Amani, E. D. Vidiyastutik, and K. Hudzafidah, "Dampak Teknologi Informasi Terhadap Audit," *Pros. Semin. Nas. dan Call Pap. Ekon. dan Bisnis*, vol. 2017, pp. 27–28, 2017.

[14] M. A. Saputra and Novita, "Sistem_Pengendalian_Internal_Berdasarkan_Coso_Fram," *J. Ris. Akunt. Politala*, vol. 6, no. 1, pp. 197–210, 2023.

[15] Gondodiyoto, S., 2007, *Audit Sistem Informasi + Pendekatan CobIT*, Mitra Wacana Media, Jakarta.