Audit Tingkat Keamanan Sistem Informasi ERP pada PT. POS Indonesia (Persero) Menggunakan Framework Cobit 5

Agesha Diiyah Kamila[1)], I Wayan Ardiyasa[2)], Riza Wulandari[3)]
Teknologi Informasi[1,2)], Sistem Informasi[3)]
Institut Teknologi dan Bisnis STIKOM Bali
Denpasar, Indonesia
e-mail: 200040046@stikom-bali.ac.id[1)],ardi@stikom-bali.ac.id[2)], rizawulandari@stikom-bali.ac.id[3)]

Abstrak

Keamanan sistem informasi menjadi isu krusial bagi perusahaan yang bergantung pada teknologi, seperti PT Pos Indonesia (Persero) yang memanfaatkan sistem Perencanaan Sumber Daya Perusahaan (ERP) dalam menjalankan bisnisnya. Penelitian ini mengeksplorasi implementasi audit sistem ERP menggunakan kerangka kerja COBIT 5, menganalisis hasil audit, dan menelaah dampaknya. Metode penelitian yang digunakan bersifat kuantitatif, dengan pengumpulan data melalui studi literatur, observasi, wawancara, dan kuesioner. Kerangka kerja COBIT 5 diterapkan untuk menilai keamanan sistem melalui domain DSS05 (Pengelolaan Layanan Keamanan), DSS06 (Pengelolaan Pengendalian Proses Bisnis), APO12 (Pengelolaan Risiko), dan MEA02 (Pemantauan, Evaluasi, dan Penilaian Pengendalian Internal). Hasil studi mengungkapkan bahwa sistem ERP PT Pos Indonesia berada pada tingkat kapabilitas Level 2 (Proses yang Dikelola), dengan titik lemah utama pada manajemen akses pengguna, kurangnya otomatisasi pemantauan ancaman, dan minimnya pelatihan keamanan. Dampak positif audit ini terletak pada identifikasi area yang memerlukan perbaikan untuk meningkatkan efektivitas sistem keamanan. Sebagai rekomendasi, perusahaan perlu mengimplementasikan kontrol akses berbasis peran, meningkatkan otomatisasi pemantauan ancaman, dan menyediakan pelatihan keamanan berkala kepada seluruh pengguna sistem ERP. Tindakan ini bertujuan untuk memitigasi risiko keamanan dan memastikan keberlanjutan operasional.

Kata kunci: *Keamanan Sistem Informasi, ERP, COBIT 5, PT. POS Indonesia, Audit IT.*

1. Pendahuluan

Penggunaan teknologi informasi yang sangat pesat saat ini mendorong berbagai sektor dalam mengembangkan sebuah sistem yang dapat membantu memudahkan segala pekerjaan [1]. Perusahaan besar maupun kecil dituntut untuk terus berinovasi dalam memperbarui cara mereka dalam mengelola bisnis [2]. ERP (Enterprise Resource Planning) merupakan salah satu inovasi berbasis teknologi yang dapat digunakan untuk membantu meningkatkan keunggulan bersaing pada suatu perusahaan [3], sebuah sistem informasi terintegrasi yang memungkinkan perusahaan mengelola berbagai fungsi seperti keuangan, logistik, penggajian, pengelolaan inventaris, dan manajemen sumber daya manusia dalam satu *platform* terpadu [4]. *Enterprise Resource Planning* (ERP) tidak hanya dapat membantu perusahaan dalam meningkatkan efisiensi proses bisnis [5], tetapi juga dapat menyajikan data secara *real-time* yang dapat mendukung pengambilan keputusan secara cepat dan akurat [6].

Perusahaan besar seperti PT. Pos Indonesia (Persero), menjadikan ERP sebagai salah satu fondasi penting dalam pengelolaan oprasional yang kompleks, mulai dari pengiriman barang, pengelolaan kantor cabang, hingga layanan pelanggan yang tersebar di seluruh Indonesia [7]. PT. Pos Indonesia (Persero) sebagai salah satu penyelenggara perposan di Indonesia, terus berupaya melakukan pengembangan terhadap sistem pelayanan yang tepat dalam rangka memenuhi kebutuhan masyarakat akan layanan pos yang baik, cepat dan berkualitas, dengan biaya yang terjangkau bagi Masyarakat [8] . Namun, keberhasilan implementasi ERP tidak hanya bergantung pada fungsionalitas sistem, tetapi juga pada tingkat keamanan informasi yang diimplementasikan dalam sistem tersebut. Ketika perusahaan bergantung sepenuhnya pada sistem ERP, terdapat berbagai ancaman keamanan seperti kebocoran data, serangan siber, atau akses tidak sah menjadi risiko yang harus dikelola dengan baik. Sistem teknologi informasi yang terkelola dengan baik merupakan

salah satu sumber daya yang penting, karena dengan teknologi informasi yang terkelola dengan baik memberi kontribusi besar dalam menyediakan layanan sesuai dengan tujuan organisasi [9].

Adanya ketergantungan yang tinggi terhadap teknologi informasi juga membawa risiko kegagalan sistem [10] . Ancaman tersebut dapat berasal dari berbagai sumber, seperti serangan siber oleh peretas, akses tidak sah oleh pihak internal perusahaan, atau kegagalan sistem yang tidak terduga. Dalam konteks PT. Pos Indonesia, yang mengelola data sensitif seperti informasi pelanggan dan transaksi keuangan, ancaman ini bisa menjadi masalah yang sangat serius. Jika data perusahaan atau pelanggan terekspos, tidak hanya bisa merusak kepercayaan publik terhadap perusahaan, tetapi juga berpotensi menyebabkan kerugian finansial yang besar. Oleh karena itu, langkah-langkah pengamanan harus dilakukan dengan optimal, termasuk melakukan audit keamanan untuk memastikan bahwa sistem yang digunakan sudah cukup aman dari berbagai ancaman. Audit keamanan juga penting untuk memastikan sistem ERP berjalan sesuai dengan regulasi yang berlaku, seperti Undang-Undang Perlindungan Data Pribadi di Indonesia [11].

Salah satu pendekatan yang diakui secara luas dalam mengaudit keamanan sistem informasi adalah menggunakan framework COBIT 5 (*Control Objectives for Information and Related Technologies*) [12]. COBIT merupakan kerangka kerja yang menyediakan solusi untuk tata kelola teknologi informasi melalui domain, proses, tujuan, kegiatan, model kematangan dan struktur yang logis dan teratur [13]. Dengan menggunakan COBIT 5, PT. Pos Indonesia dapat mengidentifikasi kelemahan dalam sistem keamanan ERP, mengukur tingkat kepatuhan terhadap standar keamanan, serta memberikan rekomendasi yang sesuai untuk perbaikan. Framework ini berfokus pada pengelolaan risiko, pencapaian tujuan bisnis, dan pemanfaatan optimal dari teknologi informasi dalam mendukung keberlanjutan operasional perusahaan. COBIT 5 menyediakan metode yang terstruktur dan komprehensif dalam melakukan audit keamanan, memastikan semua aspek keamanan diperiksa dengan cermat dan sesuai dengan tujuan bisnis perusahaan.

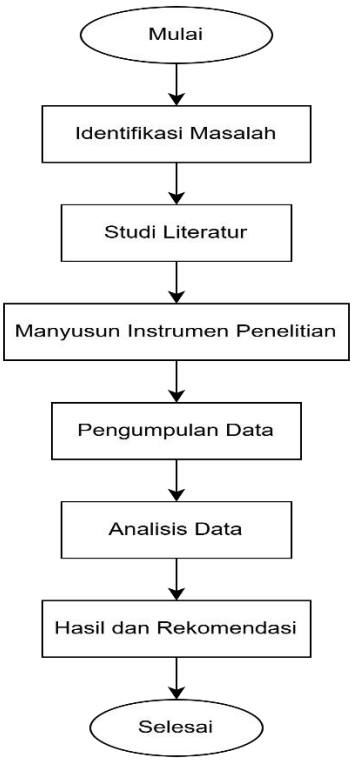
Pos Indonesia merupakan sebuah perusahaan Badan Usaha Milik Negara (BUMN) yang bergerak pada bidang jasa (layanan pos) [14]. Sebagai penyedia layanan yang mengandalkan sistem informasi dalam operasionalnya, perusahaan ini sangat perlu menjaga keamanan dan keandalan sistem ERP yang digunakan. Ancaman terhadap keamanan sistem informasi semakin berkembang seiring kemajuan teknologi, dan kelalaian dalam mengelola keamanan dapat berdampak serius pada operasional dan kepercayaan pelanggan. Audit keamanan menggunakan COBIT 5 tidak hanya akan memberikan gambaran tingkat keamanan sistem saat ini, tetapi juga memberikan rekomendasi untuk pengembangan lebih lanjut. Dengan hasil audit ini, PT. Pos Indonesia diharapkan dapat memperbaiki kerentanan keamanan yang ada, meningkatkan kualitas pengelolaan data, dan memastikan bahwa sistem ERP perusahaan dapat terus mendukung operasional secara aman dan efektif.

Penelitian ini bertujuan untuk melakukan audit terhadap tingkat keamanan sistem informasi ERP pada PT. Pos Indonesia (Persero) menggunakan framework COBIT 5. Audit ini akan membantu mengidentifikasi kelemahan dalam sistem keamanan yang ada, mengevaluasi tingkat kepatuhan terhadap standar keamanan informasi, serta memberikan rekomendasi untuk meningkatkan keamanan sistem ERP yang digunakan oleh perusahaan. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi praktis dalam pengelolaan keamanan informasi PT. Pos Indonesia sekaligus mendukung keberlanjutan operasional perusahaan yang lebih baik.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif untuk menilai kinerja dan efektivitas penerapan sistem ERP di PT. Pos Indonesia (Persero). Pengumpulan data dilakukan melalui survei, pemantauan kinerja sistem, serta analisis *statistic* [15].

Data yang terkumpul kemudian dianalisis dengan menggunakan framework COBIT 5 secara kuantitatif. Tujuan analisis ini adalah untuk memberikan pemahaman lebih mendalam mengenai kinerja sistem ERP di perusahaan, serta untuk mengidentifikasi dan menangani masalah yang berkaitan dengan tata kelola teknologi informasi di PT. Pos Indonesia. Proses analisis ini mengikuti langkah-langkah yang dirancang khusus untuk menangani permasalahan tersebut, yang dijelaskan dalam diagram berikut:



Gambar 1. Alur Penelitian

3. Hasil dan Pembahasan

Penelitian ini dilakukan melalui beberapa tahapan yang sistematis untuk memastikan evaluasi keamanan ERP PT Pos Indonesia dapat dilakukan secara menyeluruh. Tahapan penelitian meliputi:

- **Identifikasi Masalah**: Menentukan titik lemah dalam keamanan ERP, seperti manajemen akses pengguna yang lemah dan kurangnya otomatisasi pemantauan ancaman.
- **Penyusunan Instrumen**: Menyusun instrumen penelitian berdasarkan studi literatur, observasi langsung, wawancara dengan tim IT, dan kuesioner kepada pengguna sistem ERP.
- **Pengumpulan Data**: Data diperoleh dari wawancara, kuesioner, dan hasil observasi terhadap sistem ERP PT Pos Indonesia.
- **Analisis Data**: Menggunakan framework COBIT 5 untuk menilai tingkat kapabilitas keamanan ERP berdasarkan empat domain utama: DSS05, DSS06, APO12, dan MEA02.
- **Hasil dan Rekomendasi**: Menyusun rekomendasi berdasarkan hasil evaluasi masing-masing domain untuk meningkatkan keamanan sistem ERP.

Penelitian ini diharapkan memberikan gambaran mendalam tentang performa dan efektivitas sistem informasi tersebut, serta menyediakan rekomendasi untuk meningkatkan efisiensi dan pengendalian sistem informasi yang ada [16].

3.1 DSS05 Mengelola Layanan Keamanan

Nilai capability level pada subdomain DSS05 berada di ***Level* 2 (*Managed Process*)**. Hal ini menunjukkan bahwa meskipun proses keamanan telah dikelola, implementasinya masih belum sepenuhnya optimal untuk memberikan perlindungan menyeluruh terhadap berbagai ancaman yang ada. PT. Pos Indonesia telah menetapkan beberapa prosedur keamanan penting, seperti pengelolaan akses berbasis peran, enkripsi data, dan pemantauan jaringan. Namun, beberapa area masih memerlukan perbaikan untuk meningkatkan efektivitas sistem keamanan secara keseluruhan. Salah satu kelemahan utama terletak pada kurangnya otomatisasi dalam pemantauan ancaman serta minimnya pelatihan keamanan kepada pengguna sistem ERP.

Tabel 1. Hasil *Maturity Level* DSS05

Aspek yang Dinilai	Keterangan	Nilai
Kontrol Akses Berbasis Peran	Sudah diterapkan, namun perlu evaluasi lebih mendalam terhadap hak akses kritis.	4
Pemantauan Ancaman Otomatis	Pemantauan ancaman sudah ada, tetapi sistem otomatis masih perlu ditingkatkan.	3
Pelatihan Keamanan untuk Pengguna	Belum diterapkan secara menyeluruh kepada semua pengguna sistem ERP.	2
Enkripsi Data dan Proteksi Data Sensitif	Sudah ada prosedur enkripsi, tetapi perlindungan terhadap data sensitif perlu lebih diperketat.	3
Rata-rata Penilaian	-	**3**

3.2 DSS06 Mengelola Pengendalian Proses Bisnis

Nilai capability level pada subdomain DSS06 mencapai ***Level* 2 (*Managed Process*)**. Proses pengelolaan transaksi bisnis di PT. Pos Indonesia telah dikelola dengan baik melalui penerapan beberapa kontrol, termasuk kontrol akses berbasis peran dan verifikasi transaksi. Proses ini dirancang untuk mengurangi risiko kesalahan atau penyalahgunaan dalam pengelolaan transaksi bisnis. Namun, beberapa kelemahan masih ditemukan, terutama dalam pengelolaan akses ke data dan sistem ERP yang sensitif. Meskipun kontrol berbasis peran telah diterapkan, evaluasi lebih mendalam terkait pembaruan hak akses secara berkala masih kurang optimal. Selain itu, audit data sensitif belum dilakukan secara menyeluruh dan rutin, sehingga ada risiko keamanan yang mungkin terabaikan. Evaluasi proses bisnis juga perlu dilakukan secara lebih sistematis untuk memastikan efektivitasnya terhadap operasional perusahaan secara keseluruhan.

Tabel 2. Hasil *Maturity Level* DSS06

Aspek yang Dinilai	Keterangan	Nilai
Verifikasi Transaksi	Verifikasi transaksi berjalan dengan baik, namun proses verifikasi untuk transaksi kritis masih kurang ketat.	3
Kontrol Akses Sistem ERP Sensitif	Akses ke sistem ERP yang sensitif dikelola, namun masih ada area yang perlu lebih ketat.	3
Audit Data Sensitif	Audit data sensitif perlu diperkuat, dengan lebih banyak pengawasan dan evaluasi rutin.	2
Evaluasi Proses Bisnis	Evaluasi proses bisnis sudah dilakukan, namun kurang sistematis.	3
Rata-rata Penilaian	-	**2.75**

3.3 APO12 Mengelola Resik

Nilai capability level pada subdomain APO12 berada di ***Level* 3 (*Defined Process*)**. Hal ini menunjukkan bahwa PT. Pos Indonesia telah memiliki proses yang terdefinisi dengan baik untuk mengelola risiko, terutama dalam mengidentifikasi ancaman potensial terhadap operasional dan sistem perusahaan. Proses identifikasi risiko dilakukan secara rutin dan mencakup berbagai jenis risiko, termasuk ancaman eksternal seperti serangan siber dan kebocoran data. Meskipun demikian, mitigasi terhadap risiko tertentu, seperti peretasan dan ancaman siber, belum diterapkan secara konsisten. Keamanan terhadap ancaman eksternal ini masih menjadi salah satu area yang membutuhkan perhatian lebih besar. Upaya mitigasi yang lebih efektif, seperti penggunaan firewall tingkat lanjut dan sistem deteksi intrusi (IDS), perlu diterapkan untuk melindungi sistem dari ancaman eksternal. Selain itu, pengawasan terhadap risiko internal dan eksternal perlu dilakukan secara lebih terstruktur dan sistematis untuk mendukung keberlanjutan bisnis.

Tabel 3. Hasil *Maturity Level* APO12

Aspek yang Dinilai	Keterangan	Nilai
Identifikasi Risiko	Identifikasi risiko dilakukan secara rutin, mencakup berbagai jenis risiko yang mungkin dihadapi perusahaan.	4
Mitigasi Risiko	Mitigasi risiko terhadap ancaman eksternal, seperti peretasan dan kebocoran data, masih perlu ditingkatkan.	3
PengelolaanRisiko Eksternal	Keamanan terhadap ancaman eksternal masih menjadi risiko utama yang belum sepenuhnya dikelola dengan efektif.	2
Pengawasan dan Evaluasi Risiko	Pengawasan terhadap risiko sudah dilakukan, namun perlu lebih terstruktur dan rutin.	4
Rata-rata Penilaian	-	**3.25**

3.4 MEA02 Memantau, Mengevaluasi, dan Menilai Pengendalian Internal

Nilai capability level pada subdomain MEA02 berada di **Level 2 (*Managed Process*)**. PT. Pos Indonesia telah memiliki prosedur untuk memantau dan mengevaluasi pengendalian internal. Prosedur ini mencakup laporan audit internal yang dilakukan secara berkala untuk menilai efektivitas kontrol internal terhadap sistem dan proses bisnis. Namun, hasil audit seringkali tidak diikuti dengan implementasi perbaikan yang memadai. Proses evaluasi pengendalian internal juga belum sepenuhnya mencakup analisis mendalam terhadap dampak pada kinerja operasional. Evaluasi yang lebih menyeluruh perlu dilakukan untuk meningkatkan keandalan sistem ERP dan memastikan bahwa hasil audit internal menghasilkan tindakan perbaikan yang konkret dan berkelanjutan.

Tabel 4. Hasil *Maturity Level* MEA02

Aspek yang Dinilai	Keterangan	Nilai
Pemantauan Pengendalian Internal	Pemantauan terhadap pengendalian internal sudah dilakukan, tetapi evaluasi terhadap hasil pemantauan perlu diperkuat.	3
Evaluasi Hasil Audit Internal	Laporan audit internal dilakukan, namun implementasi perbaikan berdasarkan audit masih kurang efektif.	2
Analisis Dampak terhadap Kinerja Operasional	Evaluasi harus mencakup analisis yang lebih mendalam terhadap dampak pada kinerja operasional dan sistem ERP.	3
Evaluasi dan Peningkatan Berkelanjutan	Evaluasi terhadap pengendalian internal sudah ada, namun implementasi perbaikan masih belum konsisten.	3
Rata-rata Penilaian	-	**2.75**

4. Kesimpulan

Audit keamanan sistem ERP pada PT. Pos Indonesia menunjukkan bahwa meskipun beberapa prosedur keamanan, seperti kontrol akses berbasis peran dan enkripsi data, telah diterapkan, masih ada kelemahan dalam otomatisasi pemantauan ancaman, pelatihan keamanan, dan audit data sensitif. Hasil audit menunjukkan bahwa beberapa subdomain berada pada level "*Managed Process"* (*Level* 2), dengan perbaikan yang diperlukan di area pemantauan ancaman dan pengelolaan risiko eksternal. Untuk meningkatkan keamanan, disarankan agar PT. Pos Indonesia memperkuat kontrol akses, meningkatkan otomatisasi pemantauan ancaman, serta melakukan pelatihan keamanan lebih menyeluruh bagi pengguna sistem ERP. Langkah-langkah ini akan membantu memperbaiki keamanan sistem dan mendukung operasional yang lebih aman dan efektif.

Daftar Pustaka

[1] R. Handayani and E. Zuraidah, "Audit Sistem Informasi Aplikasi Attendance Manager Menggunakan Framework Cobit 5," *Resolusi: Rekayasa Teknik Informatika ...*, vol. 4, no. 4, pp. 321–333, 2024.

[2] C. B. Suwito, D. Arisanti, Soedarmanto, and N. Widyawati, "Analisa Sistem Informasi Centra pada Manajemen PT. Berkah Industri Mesin Angkat," *Jurnal Administrasi Bisnis (JUTRANIS)*, vol. 01, no. 01, pp. 45–67, 2024.

[3] N. KS, R. Rahayu, and R. Kartika, "Pengaruh Corporate Governance dan Diversifikasi terhadap Kinerja Keuangan Perusahaan yang Menerapkan Enterprise Resource Planning (ERP)," *Ekonomis: Journal of Economics and Business*, vol. 6, no. 1, p. 78, 2022, doi: 10.33087/ekonomis.v6i1.458.

[4] Sri Febri Mayona and N. Sunaryo, "Perancangan Sistem Informasi Logistik Pada PT. Sembilan Cipta Karya," *JEKIN - Jurnal Teknik Informatika*, vol. 4, no. 2, pp. 107–119, 2024, doi: 10.58794/jekin.v4i2.707.

[5] L. Juliani and G. Masitoh, "Pengaruh Implementasi Sistem Berbasis (Erp) Untuk Peningkatan Kinerja Operasional Pada Pt Laju Perdana Indah," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 2, pp. 2399–2404, 2024, doi: 10.36040/jati.v8i2.9493.

[6] G. Bodnar, W. H.-B. Satu, S. Empat, undefined Jakarta, and undefined 2000, *Sistem informasi akuntansi*.

[7] B. D. Anggoro and E. S. Hartatik, "Dari Perum Pos dan Giro menjadi PT Pos Indonesia : Dinamika Perusahaan Jasa Pos Indonesia," vol. 3, no. 2, pp. 150–160, 2022.

[8] Siti Wahyuningsih, "Pengembangan Layanan Jasa Pengiriman PT. POS Indonesia untuk Kebutuhan Masyarakat di Kota Bandung," *Jurnal Penelitian Pos dan Informatika*, vol. 3, no. 1, pp. 19–49, 2013.

[9] E. Zuraidah, "Audit Sistem Informasi Management Project Pada Pt. Rikaryatama Menggunakan Framework Cobit 5," *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, vol. 10, no. 2, pp. 146–151, 2023, doi: 10.30656/prosisko.v10i2.6935.

[10] Beno Jange, Dorce Idie, Ade Taufan, Muhamad Pattiran, and Jalmijn Tindage, "Peran Inovasi Teknologi Dalam Meningkatkan Efisiensi Operasional Dalam Manajemen Ekonomi: Sebuah Kajian Kritis Literatur," *Jurnal Review Pendidikan dan Pengajaran*, vol. 7, no. 1, pp. 216–221, 2023, [Online]. Available: http://journal.universitaspahlawan.ac.id/index.php/jrpp/article/view/24063%0Ahttp://journal.universitaspahlawan.ac.id/index.php/jrpp/article/download/24063/16957

[11] M. Ilham and M. Akbar, "Pertanggungjawaban Hukum Bagi Pelaku Penyebaran Data Pribadi Yang Tersimpan Pada Barcode Ditinjau Dari Undang-Undang Informasi Transaksi Elektronik (Uu Ite)," *Indonesia Journal of Business Law*, vol. 3, no. 1, pp. 43–52, 2024, doi: 10.47709/ijbl.v3i1.4281.

[12] W. Priyadi, "Audit Sistem Informasi Presensi Guru Menggunakan Framework Cobit 5.0 Pada SMK Industri Kreatif Kota Bekasi," *Bina Insani Ict Journal*, vol. 11, no. 1, p. 100, 2024, doi: 10.51211/biict.v11i1.2980.

[13] P. P. G. P. Pertama and I. W. Ardiyasa, "Audit Keamanan Sistem Informasi Perpustakaan Stmik Stikom Bali Menggunakan Kerangka Kerja Cobit," *Jurnal Sistem dan Informatika*, vol. 13, no. 2, pp. 1–4, 2019, [Online]. Available: https://jsi.stikom-bali.ac.id/index.php/jsi/article/view/215

[14] A. M. I. Astuti and S. Ratnawati, "Analisis SWOT Dalam Menentukan Strategi Pemasaran (Studi Kasus di Kantor Pos Kota Magelang 56100)," *Jurnal Ilmu Manajemen*, vol. 17, no. 2, pp. 58–70, 2020.

[15] A. A. A. Bintang, K. Dewi, P. Putu, G. Putra, and R. Wulandari, "Audit Sistem Informasi Tata Kelola E-Krs ITB Stikom Bali Menggunakan Framework Cobit 5 . 0," vol. 1, no. 3, pp. 386–391, 2024.

[16] I. Putra, A. Syukur, S. Hanief, and P. Dewanti, "Audit Sistem Informasi Front Office di G ' sign Style Hotel dengan Pendekatan Framework Cobit 4 . 1," vol. 1, no. 3, pp. 108–113, 2024.