JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 6 November – Desember 2025, Page 2911-2920
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Studi Literatur Audit ISO 27001, COBIT, Dan ITIL Pada Layanan Sistem Informasi

Kristianto Pratama Dessan Putra[1*], Joko Sutopo[2], Suhirman[3]

[1,2,3]Magister Teknologi Informasi, Universitas Teknologi Yogyakarta, Indonesia
Email: [1]kristianto0704@gmail.com, [2]jksutopo@uty.ac.id, [3]suhirman@uty.ac.id
Email Penulis Korespondensi: [1] kristianto0704@gmail.com

Abstrak− Proses audit memegang peranan penting dalam evaluasi suatu layanan informasi. Dengan adanya proses audit, celah-celah kecurangan ataupun kendala-kendala dapat diketahui dan melalui proses audit juga dapat memberikan rekomendasi perbaikan terhadap sistem informasi tersebut. Proses audit dapat memberikan perbaikan pada proses bisnis agar dapat berjalan lebih efektif dan efisien, serta minim dari risiko. Ada berbagai macam kerangka kerja audit sistem informasi, diantaranya ISO 27001, COBIT, dan ITIL dengan fokus dan karakteristik yang berbeda-beda. Menjadi hal penting untuk mengetahui perbedaan dari masing-masing kerangka kerja audit tersebut sehingga proses audit yang dipilih sesuatu dengan kebutuhan dari sistem informasi tersebut. Oleh karena itu, penelitian ini bertujuan untuk memberikan sumber referensi untuk memilih kerangka kerja audit sistem informasi yang tepat sesuai kebutuhan dari masing-masing pengguna.Hasil dari penelitian adalah ISO 27001 memiliki fokus pada keamanan dan perlindungan data sistem informasi, COBIT memiliki fokus pada tata kelola dan manajemen risiko sistem informasi, dan ITIL memiliki fokus pada peningkatan kualitas layanan dan keberlangsungan peningkatan sistem informasi. Selain itu, penelitian ini juga memberikan informasi latar belakang, kelebihan – kekurangan, serta langkah-langkah implementasi dari masing-masing kerangka kerja audit tersebut. Diharapkan penelitian ini dapat menjadi sumber referensi untuk menentukan kebutuhan audit dari masing-masing sistem informasi.

Kata Kunci: Audit Sistem Informasi, COBIT, ISO 27001, ITIL

Abstract− The audit process plays a crucial role in the evaluation of an information service. Through the audit process, loopholes for fraud or obstacles can be identified, and through the audit process, recommendations for improvements to the information system can also be provided. The audit process can provide improvements to business processes so that they can run more effectively and efficiently, with minimal risk. There are various information system audit frameworks, including ISO 27001, COBIT, and ITIL, each with its own focus and characteristics. It is important to understand the differences between these frameworks so that the audit process chosen is in line with the needs of the information system. Therefore, this study aims to provide a reference source for selecting the right information system audit framework according to the needs of each user. The results of the study are that ISO 27001 focuses on the security and protection of information system data, COBIT focuses on the governance and risk management of information systems, and ITIL focuses on improving service quality and the sustainability of information system improvements. In addition, this study also provides background information, advantages and disadvantages, and implementation steps for each audit framework. It is hoped that this research can be a reference source for determining the audit needs of each information system.

Keywords: *Information System Audit*, COBIT, ISO 27001, ITIL

1. PENDAHULUAN

Proses audit memegang peranan penting pada suatu layanan ataupun produk. Dengan adanya proses audit, maka baik buruknya kinerja suatu layanan ataupun produk dapat diketahui dengan tepat, tidak terkecuali suatu layanan sistem informasi. Tahapan teknis dari proses audit dimulai dari menganalisis bukti dan data yang ada, pada proses tersebut sangat penting bagi pemilik layanan untuk bersikap transparan kepada pihak penyelenggara audit agar setiap informasi yang didapatkan bersifat valid, lalu selanjutnya adalah membuat hipotesis, lalu menguji dan menyaringnya menjadi suatu informasi [1], dari situ setiap bentuk penyimpangan ataupun fraud dapat dideteksi. Selain untuk mendeteksi suatu fraud, proses audit juga dapat menjadi alat untuk mendeteksi sedini mungkin potensi-potensi kecurangan yang dapat terjadi ke depannya [2]. Dengan adanya proses audit, maka potensi kerugiaan dari perusahaan yang menjalankan suatu layanan dapat diminimalisir sekecil mungkin, bahkan dapat dicegah. Selain itu, proses audit juga dapat meningkatkan efektivitas, serta kinerja dan tata kelola dari suatu perusahaan [3].

Proses audit tidak hanya berfokus pada kinerja finansial suatu sistem informasi, namun juga berfokus pada keamananan data yang dimiliki oleh sistem informasi tersebut. Banyak perusahaan, salah satunya perbankan, yang melakukan proses audit sistem informasi untuk menjamin keamananan dan kerahasian data nasabahnya [4], hal-hal confidential seperti nama, NIK, password, alamat, hingga nomer HP tidak boleh sembarangan dibagikan. Kebocoran-kebocoran data dari suatu sistem informasi tentunya akan merugikan berbagai pihak, baik penyedia layanan ataupun nasabah dari layanan tersebut, sehingga penting untuk memastikan data confidential hanya dapat diakses oleh pihak-pihak berwenang, dan hasil dari proses audit dapat menjamin hal tersebut. Lebih lanjut lagi, proses audit juga dapat memberikan serangkaian saran perbaikan untuk layanan ataupun cara kerja dari layanan tersebut, sehingga celah-celah keamanan yang berpotensi dieksploitasi dapat ditutup sesegara mungkin [5].

Dengan adanya proses audit, diharapkan sistem kontrol internal pada suatu perusahaan dapat berjalan dengan baik sebagai mana mestinya tanpa adanya potensi kecurangan yang dapat terjadi [6]. Sebagai contoh, salah satu artikel

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **17/10/2025**; Accepted: **24/10/2025**; Published: **07/11/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 6 November – Desember 2025, Page 2911-2920
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

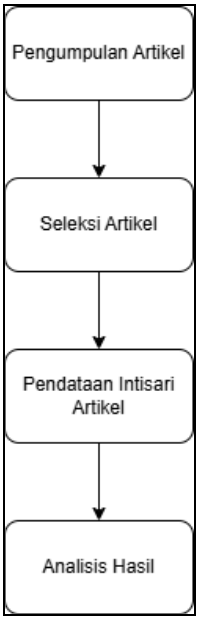
jurnal melakukan proses audit terhadap aplikasi Sirekap dari Komisi Pemilihan Umum (KPU) dan hasil audit menunjukan kerentanan dari sistem informasi tersebut dan memberikan langkah-langkah perbaikan untuk sistem informasi tersebut [7].

Ada berbagai macam kerangka kerja audit terhadap sistem informasi, ada kerangka kerja ISO 27001 yang berfokus pada keamanan data pada sistem informasi [8], ada pula COBIT yang berfokus pada tata kelola dan manajemen risiko sistem informasi [9], dan ada yang berfokus pada peningkatan kualitas layanan teknologi informasi [10]. Setiap kerangka kerja audit sistem informasi memiliki fokus dan fungsi yang berbeda, namun memiliki tujuan yang sama yaitu menjamin peningkatan kualitas dan mutu dari layanan sistem informasi. Penting untuk memahami karakteristik dari masing-masing kerangka kerja agar dapat memilih kerangka kerja audit yang tepat. Penelitian ini akan membahas dan membandingkan 3 kerangka kerja audit sistem informasi, yaitu ISO 27001, COBIT, dan juga ITIL. Cakupan pembahasan akan meliputi latar belakang, tujuan utama dan ruang lingkup, kelebihan dan kekurangan, serta langkah-langkah implementasi proses audit tersebut.

Setiap kerangka kerja audit memiliki karakteristik dan tujuannya masing-masing sehingga harus memastikan terlebih dahulu tujuan utama dari proses audit yang ingin dilakukan sebelum memilih kerangka kerja mana yang akan digunakan. Oleh karena itu, penelitian ini akan membahas mengenai detail dan karakteristik dari masing-masing kerangka kerja audit untuk memberikan gambaran tentang bagaimana tujuan dan hasil akhir dari masing-masing kerangka kerja audit. Penelitian akan memberikan data-data tambahan seperti biaya masing-masing kerangka kerja audit, namun data tersebut tidak menjadi standar ataupun patokan karena bisa terjadi perbedaan biaya pada masing-masing vendor audit. Diharapkan, penelitian ini dapat menjadi sumber referensi bagi pihak-pihak yang ingin melakukan proses audit pada layanan sistem informasinya.

2. METODOLOGI PENELITIAN

Metode penelitian pada artikel ini adalah studi literatur berdasarkan artikel-artikel jurnal terkait mengenai kerangka kerja audit sistem informasi, yaitu ISO 27001, COBIT, dan ITIL. Studi literatur dilakukan dengan mendata tiap-tiap artikel jurnal, dalam kurun waktu 5 tahun ke belakang, secara merinci untuk setiap kerangka kerja audit.
Alur penelitian adalah sebagai berikut :



Gambar 1. Alur Penelitian

1. Pengumpulan Artikel

Pengumpulan artikel dilakukan dengan mencari artikel-artikel jurnal dari google scholar dengan kata kunci audit sistem informasi, ISO 27001, OSBIT, dan ITIL. Artikel yang dipilih adalah artikel yang kurun waktunya adalah 5 tahun terakhir. Preferensi artikel yang dipilih adalah berdasarkan studi case sehingga tergambar tahapan-tahapan proses audit untuk masing-masing kerangka kerja.

2. Seleksi Artikel

Seleksi artikel dilakukan untuk memilah artikel-artikel mana yang akan digunakan dalam penelitian ini. Artikel yang tidak relevan tidak akan digunakan pada penelitian ini supaya terbentuk fokus bahasan pada audit sistem informasi.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **17/10/2025**; Accepted: **24/10/2025**; Published: **07/11/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 6 November – Desember 2025, Page 2911-2920
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

3. Pendataan Intisari Artikel

Pendataan intisari masing-masing artikel ditujukan untuk mendapatkan poin-poin utama dari penelitian ini, yaitu latar belakang, tujuan utama dan ruang lingkup, kelebihan dan kekurangan, serta langkah-langkah implementasi proses audit tersebut. Tiap artikel tidak harus memiliki keseluruhan poin utama karena akan dilengkapi oleh artikel lainnya.

4. Analisis Hasil

Proses analisis dilakukan pada hasil pendataan intisari artikel, tujuannya adalah untuk mendapatkan fokus utama dari masing-masing kerangka kerja audit dan mendapatkan data-data pembanding dari ketiga kerangka kerja audit yang diteliti. Hasil akhir yang diharapkan adalah terbangun informasi lengkap dari model audit ISO 27001, COBIT, dan ITIL, serta didapatkan nilai-nilai pembeda pada ketiga kerangka kerja audit tersebut sehingga dapat menjadi sumber referensi untuk memilih kerangka kerja audit yang tepat untuk sistem informasi yang ingin diaudit.

Dan dari tahapan metodologi tersebut, didapatkan berbagai informasi sebagai berikut :

Audit Sistem Informasi

Audit Sistem Informasi merupakan suatu proses mengumpulkan data dan bukti-bukti untuk mengevaluasi apakah suatu sistem informasi telah menerapkan sistem pengendalian, serta menjaga dan menjamin integritas data, serta memastikan apakah kinerja dari sistem informasi telah efektif dan efisien [11]. Lebih lanjut, proses audit sistem informasi dapat memberikan rekomendasi perbaikan mulai dari tahap input data, proses, hingga kepada outputnya. Proses audit juga penting dilakukan karena dapat mengukur kinerja, keamanan sistem, serta tingkat kemampuan SDM untuk mengelola sistem informasi tersebut [12].

Tujuan dari proses audit sistem informasi meliputi beberapa aspek, diantaranya menguji kerahasian, keamananan, dan intergritas data dari sistem informasi tersebut [13]. Selain itu, tujuan dari proses audit sistem informasi adalah mengevaluasi kualitas sistem, meningkatkan keakurasian informasi, dan meningkatkan keamanan data. Secara lebih terperinci berikut adalah tujuan dari proses audit sistem informasi [13].

a. Memastikan adanya pendataan dan pengecekan aset
b. Terjaganya intergritas informasi
c. Evaluasi sistem kerja yang efektif dan efisien
d. Adanya optimalisasi sumber daya yang dimiliki
e. Peningkatan kualitas informasi pada layanan sistem informasi

ISO 27001

ISO 27001 merupakan salah satu kerangka kerja audit pada sistem informasi dan menjadi standar internasional yang digunakan untuk mengevaluasi keamanan sisten dari suatu sistem informasi [14]. Lebih lanjut, ISO 27001 juga berfokus pada perlindungan data-data sensitif yang dimiliki oleh sistem informasi tersebut sehingga hanya pihak-pihak berwenang saja yang dapat mengakses data-data tersebut. Dalam penerapannya, ISO 27001 memiliki beberapa pendekatan, salah satunya yaitu PDCA (Plan, Do, Check, and Act) [15].



Gambar 2. Pendekatan PDCA

Pendekatan tersebut memudahkan proses audit ISO 27001 dikarenakan PDCA telah membagi keseluruhan proses dalam 4 tahapan dan menjamin perbaikan berkelanjutan. Selain pendekatan PDCA, Audit ISO 27001 juga dapat digabungkan dengan analisis SWOT (Strengths, Weaknesses, Opportunities, Threats), analisis SWOT membantu proses audit untuk mendata kekuatan, kelembahan, peluang, dan juga hambatan yang ada pada sistem informasi tersebut [16].

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **17/10/2025**; Accepted: **24/10/2025**; Published: **07/11/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 6 November – Desember 2025, Page 2911-2920
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin



Gambar 3. Pendekatan SWOT

Tujuan utama dari kerangka kerja audit ISO 27001 adalah menjamin keamanana serta integritas data, tata kelola risiko yang optimal, serta kontrol akses yang baik [17] [18]. Selain itu, proses audit ISO 27001 juga memberikan rekomendasi poin-poin perbaikan yang dapat diimplementasikan untuk meningkatkan keamanan sistem informasi [19]. Selain pada aspek teknis sistem informasi, proses audit ISO 27001 juga mengaudit area sumber daya manusia yang mengelola sistem informasi tersebut sehingga sisi "human" juga dapat diperbaiki untuk kinerja yang lebih baik kedepannya.

Salah satu contoh kasus audit ISO 27001 adalah pada PT Citilink dari artikel [16] yang memberikan hasil bahwa PT Citilink memiliki kerentanan terhadap serangan phishing, namun di lain sisi PT Citylink memiliki kekuatan dalam menghadapi serangan siber. Kerentanan terhadap phishing diakibatkan oleh tingkat kesadaran karyawan yang masih rendah terhadap keamanan data sehingga rawan diserang, selain itu hasil audit ISO 27001 juga memberikan rekomendasi perbaikan yang dapat dilakukan oleh perusahaan untuk lebih mengamankan sistem informasinya.

COBIT

COBIT (Control Objectives for Information and Related Technologies) merupakan salah satu kerangka kerja audit pada sistem informasi yang lebih berfokus pada tata kelola dan manajemen risiko sistem informasi [20].
Proses audit COBIT terdiri dari 5 domain utama [21] yaitu :

a. EDM (Evaluate, Direct, and Monitoring)
   Domain ini berfokus pada tata kelola sistem informasi dan terkait pengambilan keputusan. Tujuannya adalah untuk memastikan bahwa kebutuhan tiap stakeholder terpenuhi, meminimalisir risiko, serta efisiensi sumber daya yang dimiliki
b. BAI (Build, Acquire, and Implement)
   Domain ini berfokus pada poin perbaikan dan proses implementasinya. Tujuannya adalah untuk menjamin proses bisnis sistem informasi berjalan secara efektif dan efisien.
c. APO (Align, Plan, and Organize)
   Domain ini berfokus pada strategi-strategi bisnis untuk menjamin keberlangsungan sistem informasi untuk jangka panjang. Domain ini meliputi perencaaan anggaran, sumber daya, hingga pada kebijakan pelaksanaan serta manajemen risiko dari sistem informasi.
d. d. MEA (Monitor, Evaluate, and Assess)
   Domain ini berfokus pada pemantauan dan evaluasi sistem informasi serta kebijakan-kebijakan yang ada pada sistem informasi tersebut. Tujuan dari domain ini adalah memastikan apakah proses bisnis sudah bekerja semestinya atau belum.
e. DSS (Deliver, Service, and Support)
   Domain ini berfokus kepada pengguna akhir dari layanan sistem informasi, tujuannya adalah untuk memastikan bahwa kebutuhan dari user sudah terpenuhi dengan baik and handal. Selain itu, domain ini juga berfokus pada penanganan insiden-insiden, termasuk manajemen risiko.

Selain audit tata kelola dan manajamen risiko, COBIT juga dapat digunakan untuk melakukan audit pada sumber daya manusia (SDM) bidang IT [22]. Proses bisnis yang melibatkan sumber daya manusia yang belum optimal dapat dideteksi dengan proses audit COBIT [23]. Hasil dari audit sumber daya manusia dapat digunakan untuk memastikan bahwa tiap-tiap SDM IT melakukan perannya dengan baik dan handal, hasil akhirnya adalah peningkatan kualitas dan mutu dari sistem informasi tersebut.

Salah satu contoh kasus proses audit COBIT adalah pada PT Aneka Optimal dari artikel [24] yang hasil akhirnya berhasil menemukan kendala-kendala yang ada pada sistem informasi perusahaan tersebut, mulai dari sistem yang belum optimal, ketergantungan pada 1 sumber daya, integritas data yang belum terjamin, hingga kurangnya pelatihan pada karyawan sehingga sistem informasi kurang optimal penggunaannya. Selain menemukan kendala-kendala pada sistem informasi tersebut, proses audit COBIT juga memberikan rekomendasi perbaikan sistem informasi guna memberikan layanan yang lebih baik kepada konsumen kedepannya.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **17/10/2025**; Accepted: **24/10/2025**; Published: **07/11/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 6 November – Desember 2025, Page 2911-2920
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

ITIL

ITIL (Information Technology Infrastructure Library) merupakan salah satu kerangka kerja audit pada sistem informasi yang lebih berfokus pada peningkatan kualitas layanan dari sistem informasi [25]. Selain itu, fokus dari kerangka audit ITIL adalah pada tingkat kepuasaan pengguna saat menggunakan sistem informasi tersebut [26].
Kerangka kerja ITIL meliputi 5 domain [26] yaitu :

a. Service Strategy
   Domain ini berfokus tentang rencana strategis dalam memenuhi kebutuhan bisnis dari sistem informasi tersebut. Selain itu, domain ini juga berfokus pada memahami kebutuhan pengguna serta memastikan kepuasaan pengguna dari sistem informasi tersebut.
b. Service Design
   Domain ini memastikan bahwa design dari sistem informasi telah mengakomodasi kebutuhan dari pengguna, serta memastikan bahwa proses bisnis berjalan dengan efektif dan efisien.
c. Service Transition
   Domain ini berfungsi untuk memastikan bahwa setiap perubahan yang terjadi, ataupun penambahan fitur, dapat berjalan dengan baik dan meminimalisir risiko kegagalan sekecil mungkin. Selain itu, domain ini juga berfokus pada transfer-knowledge pada saat terjadi proses transisi.
d. d. Service Operation
   Domain ini berfokus pada pengelolaan harian, mulai dari menjamin ketersediaan dan kehandalan dari sistem informasi tersebut. Selain itu, domain ini juga memastikan bahwa setiap kendala yang terjadi dapat diselesaikan dengan sesegera mungkin, seefektif dan seefisien mungkin.
e. Continual Service Improvement
   Domain ini berfokus pada peningkatan layanan yang terus berjalan seiring waktu sehingga sistem informasi terus dapat mengakomodasi kebutuhan dari pengguna. Peningkatan layanan dapat berasal dari feedback pengguna ataupun karena ditemukannya celah-celah perbaikan pada sistem informasi.

Kerangka kerja ITIL terbukti efektif dalam mengintegrasikan berbagai layanan sistem informasi, mulai dari tahap perencaaan hingga ke proses implementasi sistem informasi, selain itu kinerja operasional juga dapat diefisiensikan hingga 35%, serta penurunan kendala-kendala teknis IT hingga 40% [27]. Selain hal teknis, kerangka kerja audit ITIL juga sukses meningkatkan kinerja tim yang tentunya berdampak positif pada layanan sistem informasi tersebut [25].

Salah satu contoh kasus proses audit ITIL adalah pada aplikasi BRI Mobile dari artikel [28] yang hasil akhirnya berhasil mengidentifikasi kendala-kendala yang ada di sistem informasi BRI Mobile. Kendala-kendala meliputi keamanan aplikasi, kualitas layanan, dan ketersediaan fitur dan layanan. Selain mengidentifikasi kendala-kendala yang ada, proses audit juga memberikan rekomendasi perbaikan untuk kendala-kendala yang ditemukan dalam proses audit sehingga kedepannya diharapkan aplikasi BRI Mobile dapat berjalan lebih efektif dan efisien.

3. HASIL DAN PEMBAHASAN

Hasil dari penelitian ini merupakan studi literatur yang kemudian dianalisis untuk menemukan aspek-aspek pembeda, yaitu latar belakang, tujuan utama dan ruang lingkup, kelebihan dan kekurangan, serta langkah-langkah implementasi proses audit tersebut. Berikut adalah hasil dan pembahasan untuk masing-masing kerangka kerja audit sistem informasi.

3.1 ISO 27001



Gambar 4. Logo ISO 27001

ISO 27001 merupakan standar internasional yang digunakan dalam proses audit sistem informasi yang diterbitkan oleh International Organization for Standarization (ISO). ISO 27001 hampir digunakan oleh seluruh lembaga sebagai standarisasi untuk sistem informasi yang dimiliki. Kerangka kerja ini awalnya dikembangkan pada

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **17/10/2025**; Accepted: **24/10/2025**; Published: **07/11/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 6 November – Desember 2025, Page 2911-2920
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

tahun 1995 oleh Departemen Perdagangan dan Industri Inggris (BSI) lalu di tahun 2000 mulai diadopsi oleh ISO untuk menjadi standar audit dengan nama ISO 17799. Kemudian pada tahun 2005 standarisasi audit tersebut diberi nama ISO 27001 dan terus bertahan hingga saat ini dengan pengembangan berkala guna mengikuti perubahan yang terjadi.

Tujuan Utama dan Ruang Lingkup

ISO 27001 memiliki fokus dan tujuan utama dalam hal keamanan informasi dan kerahasiaan data dari sistem informasi. Proses audit dari kerangka kerja ISO 27001 berfokus pada perlindungan data-data sensitif dari sistem informasi tersebut sehingga hanya pihak tertentu saja yang dapat mengaksesnya. Selain itu, ISO 27001 juga berfokus pada integritas data serta tata kelola risiko yang optimal. Dalam hal tersebut, proses audit ISO 27001 memastikan bahwa tidak sembarangan proses dapat mengubah value sebuah data dan untuk setiap perubahan diharuskan menyimpan informasinya dalam log, serta memastikan bahwa tata kelola informasi sudah berjalan secara optimal dan minim dari gangguan.

Kelebihan dan Kekurangan

Kelebihan dari ISO 27001 tentunya adalah karena standar internasional yang dimiliki oleh kerangka kerja audit tersebut sehingga lebih memiliki kredibilitas dibandingkan kerangka kerja audit lainnya. Dan lagi, fokus utama dari ISO 27001 adalah keamanan informasi sehingga memberikan kepercayaan lebih kepada pengguna jika sistem informasi telah di audit dengan ISO 27001. Lebih lanjut, karena ISO 27001 dikembangkan oleh lembaga international maka isu-isu terkini akan lebih cepat diimplementasikan ke dalam proses audit ISO 27001, dalam hal ini ISO 27001 lebih cepat beradaptasi dengan perubahan kondisi.

Kekurangan dari ISO 27001 tentu yang pertama berkaitan dengan biaya implementasinya, dikarenakan ISO 27001 merupakan standar internasional maka biayanya lebih mahal dibandingkan kerangka kerja audit lainnya seperti COBIT dan ITIL. Selain itu, tahapan proses dalam ISO 27001 juga lebih kompleks dibandingkan kerangka kerja audit lainnya sehingga membutuhkan waktu yang lebih lama. Dan terakhir, dikarenakan ISO 27001 berfokus pada keamanan informasi maka aspek-aspek lain, seperti pengembangan fitur dan kepuasaan pelanggan, tidak masuk ke dalam metriks penilaian ISO 27001.

Langkah-Langkah Implementasi

ISO 27001 adalah sistem audit yang dapat diimplementasikan dengan beberapa pendekatan, salah satunya PDCA yang berfokus pada ISMS (Information Security Management System). Langkah awal dari kerangka kerja audit ISO 27001 adalah perencanaan awal, perlu dipastikan bahwa perusahan atau pemilik dari sistem informasi tersebut berkomitmen penuh dalam proses audit. Hal ini dikarenakan ISO 27001 berfokus pada keamanan informasi, maka pihak yang ingin diaudit perlu terbuka perihal celah-celah keamanan pada sistem informasi tersebut. Selanjutnya, tentukan ruang lingkup audit, mulai dari struktur organiasisi, proses bisnis yang berjalan, hingga kebijakan-kebijakan atau SOP yang digunakan. Setelah itu, lakukan analisis dengan menerapkan SOA (Statement of Applicability) untuk memastikan apakah sistem informasi telah memenuhi standar ISO 27001 atau belum dan lakukan pendokumentasian untuk setiap setiap poin dalam SOA Berdasarkan hasil analisis dan SOA, buat rekomendasi perubahan atau kebijakan yang selaras dengan ISO 27001 dan lakukan pelatihan serta perbaikan internal untuk mengimplementasikan hal tersebut. Setelah berhasil diimplementasikan, perlu dilakukan re-check ulang apakah kebijakan dan perubahan telah diterapkan dengan baik atau belum. Tahapan akhir dari proses audit ISO 27001 adalah melakukan pemeliharan dan evaluasi rutin untuk menjaga kepatuhan terhadap ISO 27001.

3.2 COBIT



Gambar 5. Logo COBIT

COBIT merupakan kerangka kerja audit sistem informasi yang dikembangkan oleh perusahaan ISACA (Information Systems Audit and Control Association) pada tahun 1996. Kemudian terus mengalami perkembangan menjadi COBIT versi 3 dan 4, kemudian pada tahun 2013 berkembang menjadi COBIT 5, dan pada tahun 2019 menjadi COBIT 2019. Pada awalnya, COBIT dikembangkan dengan tujuan memastikan bahwa sektor IT, terutama sistem informasi, berjalan dengan efektif dan memiliki tata kelola yang baik. Hingga akhirnya kini COBIT terus beradaptasi dengan perubahan dan pada COBIT 2019 mengadaptasikan era transformasi digital dengan tetap menjaga fokus audit pada area tata kelola IT.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **17/10/2025**; Accepted: **24/10/2025**; Published: **07/11/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 6 November – Desember 2025, Page 2911-2920
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Tujuan Utama dan Ruang Lingkup

COBIT memiliki fokus dan tujuan utama pada tata kelola dan manajemen risiko pada sistem informasi. Proses audit COBIT memastikan bahwa tata kelola telah berjalan dengan seefektig dan seefisien mungkin. Selain itu, COBIT juga melakukan proses audit pada area pemantuan dan evaluasi sistem informasi, serta kebijakan-kebijakan pada sistem informasi tersebut. Dalam hal tersebut, COBIT memastikan bahwa setiap proses tersebut berjalan dengan baik dan minim risiko. Lebih lanjut, COBIT juga digunakan untuk melakukan audit pada sumber daya manusia. Kendala-kendala pada SDM, seperti minimnya pengalaman, kurangnya pelatiham, ataupun belum optimalnya SDM dapat diketahui melalui proses audit COBIT.

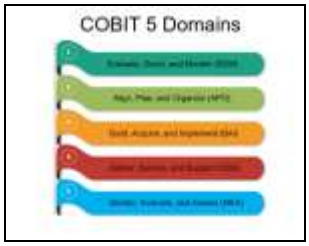
Kelebihan dan Kekurangan

Karena COBIT dirancang untuk melakukan audit agar tata kelola menjadi seefektif dan seefisien mungkin maka implementasi COBIT dapat memberikan dampak finansial yang baik. Dan lagi, dikarenakan COBIT juga berfokus pada manajemen risiko malah implementasi COBIT dapat memberikan informasi kendala-kendala apa saja yang mungkin dan akan terjadi serta memberikan rekomendasi perbaikan sehingga sistem informasi menjadi minim kendala atau risiko. Selain itu, biaya implementasi audit COBIT tidak semahal ISO 27001.

Kekurangan dari COBIT adalah mengenai kerahasiaan dan integritas informasi, hal ini dikarenakan COBIT berfokus pada tata kelola IT. Selain itu, implementasi audit COBIT juga tidak memiliki sertifikasi internasional seperti ISO 27001 sehingga kurang memberikan rasa percaya kepada pengguna sistem informasi tersebut.

Langkah-Langkah Implementasi

Implementasi dari COBIT berfokus pada tata kelola sehingga bagian yang akan banyak diaudit adalah berkaitan dengan kebijakan dan proses bisnis. Langkah pertama adalah memastikan dukungan dari pihak yang ingin diaudit, memastikan bahwa adanya keterbukaan dalam hal kebijakan dan proses bisnis. Selanjutnya, tentukan ruang lingkup yang akan menjadi fokus audit. Setelah itu, implementasikan 5 domain itu dari COBIT untuk mengalisis ruang lingkup tersebut, guna menemukan kendala-kendala serta rekomendasi perbaikan. Berikut adalah domain-domain dari COBIT yang tersaji pada Gambar 6.



Gambar 6. Domain COBIT

Setelah didapatkan hasil dari implementasi 5 domain tersebut, maka tahapan selanjutnya adalah proses evaluasi. Tahapan evaluasi bertujuan untuk memastikan apakah implementasi telah berjalan dengan baik dan apakah tata kelola IT sudah berjalan dengan efektif dan efisien, serta memastikan tenaga SDM menjalankan kepatuhan terhadap hasil audit COBIT.

3.3 ITIL



Gambar 7. Logo ITIL

Latar Belakang

Awal pengembangan ITIL dimulai pada 1980 oleh pemerintah Inggris guna melakukan audit pada pengelolaan IT di zaman itu. ITIL versi 1 berhasil dirilis pada tahun 1989, dilanjutkan dengan ITIL versi 2, ITIL versi 3, ITIL 2011, dan kini ITIL versi 4 yang dirilis pada tahun 2019. Kini banyak perusahaan mengimplementasikan audit ITIL pada sistem informasinya dikarenakan cakupan auditnya yang berfokus pada peningkatan layanan kepada pengguna.

Tujuan Utama dan Ruang Lingkup

ITIL merupakan kerangka kerja audit yang berfokus pada peningkatan kualitas layanan dari sistem informasi. Tujuan utama dari proses audit ITIL adalah memastikan bahwa kebutuhan dari pengguna terakomodasi dengan baik

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **17/10/2025**; Accepted: **24/10/2025**; Published: **07/11/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 6 November – Desember 2025, Page 2911-2920
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

serta memastikan proses bisnis berjalan dengan efektif dan efisien. Proses audit dari ITIL juga berfokus pada minimalisir risiko dari sistem informasi tersebut sehingga pengguna dapat menggunakan sistem informasi dengan optimal. Lebih lanjut, ITIL juga melakukan audit pada proses monitoring harian dan memastikan bahwa setiap kendala yang terjadi dapat diselesaikan sesegera mungkin dengan minim risiko.

Kelebihan dan Kekurangan

Kelebihan ITIL dibandingan 2 kerangka kerja audit lainnya adalah biaya implementasi yang paling murah sehingga lebih terjangkau untuk berbagai organisasi. Selain itu, karena fokus utama dari kerangka kerja audit ITIL adalah pada peningkatan kualitas layanan maka implementasi dari ITIL dapat meningkatkan user experience dari sistem informasi tersebut. Lebih lanjut, kelebihan dari audit ITIl adalah keberlanjutan peningkatan layanan sehingga layanan sistem informasi terus mengalami peningkatan layanan setiap waktunya.

Kekurangan dari ITIL adalah tidak adanya sertifikasi internasional seperti halnya ISO 27001. Selain itu, karena fokusnya adalah pada peningkatan layanan maka durasi dari implementasi bisa menjadi proses panjang. Selain itu, karena proses audit ITIL sangat berkaitan dengan SDM (Sumber Daya Manusia) maka peruibahan yang terjadi bisa jadi memerlukan masa-masa penyesuaian jika perubahan yang terjadi cukup besar dan membutuhkan beberapa pelatihan-pelatihan untuk mengikuti standar ITIL.

Langkah-Langkah Implementasi

ITIL merupakan kerangka kerja audit yang berfokus pada peningkatan kualitas layanan sehingga sangat berkaitan dengan SDM dan proses bisnis. Langkah implementasi dari ITIL dimulai dari identifikasi awal untuk mengetahui kualitas layanan dan proses bisnis yang berjalan saat ini. Setelah itu, dilakukan analisis berdasarkan hasil identifikasi awal untuk menemukan kendala-kendala dalam sistem informasi tersebut. Proses analisis dapat diproses dengan menggunakan KPI (Key Performance Index) dari kerangka kerja ITIL untuk mempermudah identifikasi kendala yang ada. Setelah itu, dilanjutkan dengan melakukan implementasi dengan memperhatikan domain dari ITIL.



Gambar 8. Domain ITIL

Setelah dilakukan implementasi sesuai dengan domain dari ITIL maka tahap selanjutnya adalah memastikan bahwa SDM mampu dan terlatih untuk menerapkan rekomendasi-rekomendasi perbaikan, maka disarankan untuk mengadakan pelatihan-pelatihan bagi SDM. Lalu, perlu dilakukan evaluasi untuk memastikan kepatuhan terhadap hasil audit ITIL dan untuk meninjau ulang apakah ada kendala-kendala baru yang ditemukan karena ITIL berfokus pada keberlanjutan perbaikan setiap waktunya.

4. KESIMPULAN

Hasil dari penelitian menunjukan karakteristik dari masing-masing metode audit sistem informasi, yaitu ISO 27001, COBIT, dan ITIL. Fokus dari masing-masing kerangka kerja audit tersebut adalah ISO 27001 berfokus pada keamanan informasi sistem informasi, COBIT berfokus pada tata kelola sistem informasi dan manajemen risiko, sedangkan ITIL berfokus pada peningkatan layanan kualitas sistem informasi dan keberlanjutan peningkatan layanan. Selain itu, kelebihan dari ISO 27001 adalah standarisasi Internasional serta jaminan keamanan informasi, sedangkan kelemahannya ada pada biaya implementasi yang mahal serta proses yang kompleks. Untuk COBIT, kelebihannya adalah jaminan tata kelola yang efektif dan efisien, serta minim risiko, sedangkan kelemahannya adalah tidak termasuk standarisasi Internasional dan tidak menjamin keamanan informasi. Untuk ITIL, kelebihannya adalah jaminan peningkatan kualitas layanan dan keberlangsungan peningkatan setiap waktunya, sedangkan kekurangannya adalah tidak termasuk standarisasi Internasional dan proses auditnya dalam berlangsung dalam kurun waktu yang cukup panjang. Saran dari penulis, penelitian lebih lanjut mengenai perbandingan dari masing-masing kerangka kerja audit dapat membahas area yang berbeda, selain latar belakang, ruang lingkup, kelebihan – kekurangan, dan langkah-langkah implementasi. Bahkan, penelitian selanjutnya dapat membahas kerangka kerja audit lainnya.

REFERENCES

[1] A. Ulfani and Ernawati, “Studi Literatur : Pengaruh Audit Investigatif Terhadap Pengungkapan Fraud Pada Perusahaan Waskita Karya Tbk DanWijaya Karya Tbk,” *Fusion A Multidiscipinary J.*, vol. 1, no. 1, pp. 158–

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **17/10/2025**; Accepted: **24/10/2025**; Published: **07/11/2025**

172, 2024.
[2] A. P. N. Fadila, A. Yuniasari, I. K. Nisa, and ..., "Studi Literatur Tentang Peranan Audit Internal Dalam Upaya Pencegahan Dan Pendeteksian Kecenderungan Kecurangan," *Triwikrama J. Multidisiplin Ilmu Sos.*, vol. 2, no. 4, 2023, [Online]. Available: http://ejournal.warunayama.org/index.php/triwikrama/article/view/1008%0Ahttps://ejournal.warunayama.org/index.php/triwikrama/article/download/1008/971
[3] A. Ulfani and T. Meutia, "Studi Literatur: Tinjauan Mendalam Terhadap Efektivitas Audit Internal Lensa Organisasi, Pengendalian Risiko, Dan Peningkatan Kinerja," *Fusion*, vol. 1, no. 1, pp. 139–151, 2024, [Online]. Available: https://yasyahikamatzu.com/index.php/FSN/article/view/44%0Ahttps://yasyahikamatzu.com/index.php/FSN/article/download/44/37
[4] J. Angelo, S. Tania, F. Loren, and Angeline, "Kajian Literatur terhadap Audit Sistem Informasi pada Perusahaan Perbankan," *JDMIS J. Data Min. Inf. Syst.*, vol. 2, no. 2, pp. 82–89, 2024, doi: 10.54259/jdmis.v2i2.2216.
[5] F. Komala, M. Sari, and C. Meiden, "Audit Operasional : Studi Literatur Perkembangan Saat Ini," *J. Ekobistek*, vol. 12, no. 4, pp. 773–776, 2023, doi: 10.35134/ekobistek.v12i4.773.
[6] S. A. Ramadhanti and G. F. A. Susilo, "STUDI LITERATUR: PERAN AUDIT INTERNAL DALAM UPAYA MENCEGAH DAN MENDETEKSI KECURANGAN (FRAUD)," *J. Cakrawala Ilm.*, vol. 20, no. 1, pp. 105–123, 2022.
[7] A. Yoga Lestari and J. Nashar Utamajaya, "Audit Sistem Informasi Aplikasi Sirekap KPU: Analisis Keamanan dan Efisiensi," *Switch J. Sains dan Teknol. Inf.*, vol. 2, no. 4, pp. 23–32, 2024.
[8] Muhamad Sidik, "Audit Sistem Informasi Berbasis Cobit 2019 Menggunakan Standar Iso 27001 : 2005," *J. Ilm. Sains Teknol. Dan Inf.*, vol. 1, no. 3, pp. 1–13, 2023, doi: 10.59024/jiti.v1i3.192.
[9] M. Jannah and B. Maula Sulthon, "Analisa Audit Sistem Informasi Barang atau Jasa Menggunakan COBIT 5.0," *KLIK Kaji. Ilm. Inform. dan Komput.*, vol. 2, no. 6, pp. 242–250, 2022, doi: 10.30865/klik.v2i6.400.
[10] L. Oktiviana and R. Jayadi, "Evaluation of It Service Management Implementation Related To Incident Management With Itil Framework in Pt. Xyz," *J. Cahaya Mandalika*, vol. 3, no. 3, pp. 758–771, 2022.
[11] S. Elpitasari, V. D. Andrean, P. Zulfa, and N. Khoiriwati, "Utilization Of Audit On Accounting Information Systems Pemanfaatan Audit Terhadap Sistem Informasi Akuntansi," *Res. Account. J.*, vol. 2, no. 3, pp. 420–425, 2022, [Online]. Available: http://journal.yrpipku.com/index.php/raj%7C
[12] A. W. Salam and D. K. Sari, "ANALISIS AUDIT SISTEM INFORMASI AKADEMIK (SIAKAD) MENGGUNAKAN METODE COBIT FRAMEWORK 4.1 STUDI KASUS DI UNIVERSITAS ISLAM INDRAGIRI," *J. Sist. Inf.*, vol. 2, pp. 824–832, 2024, doi: 10.1134/s0514749219040037.
[13] M. Erfandi and R. Herlianto, "MANFAAT AUDIT DALAM PENGELOLAAN SISTEM INFORMASI AKUNTANSI Mhd," *J. Sist. Inf.*, vol. 2, pp. 677–682, 2024, doi: 10.1134/s0514749219040037.
[14] A. P. Damanik, A. Zaki, S. Fiddarain, and A. B. Nasution, "Implementasi ISO 27001:2013 Dalam Pengamanan Sistem Informasi Pada Yayasan Pendidikan Islam ANNUR PRIMA," *J. Sains dan Teknol.*, vol. 3, no. 1, pp. 68–73, 2023, doi: 10.47233/jsit.v3i1.488.
[15] J. Jevelin and A. Faza, "Evaluation the Information Security Management System: A Path Towards ISO 27001 Certification," *J. Inf. Syst. Informatics*, vol. 5, no. 4, pp. 1240–1256, 2023, doi: 10.51519/journalisi.v5i4.572.
[16] Fatihana Nur Salsabillah, A. Wicaksono, S. Gustina, and L. Sudarmana, "ANALISIS ANCAMAN KEAMANAN CYBER DI PT. CITILINK INDONESIA DAN SOLUSI UNTUK MENGAMANKAN OBJEK VITAL," *J. Sci. Res. Dev.*, vol. 3, no. 1, pp. 24–32, 2024, [Online]. Available: https://idm.or.id/JSCR/index.php/JSCR/article/view/14
[17] E. Soesanto, F. Kurniasih, P. Mutiara, and S. T. Afifi, "Sistem manajemen keamanan informasi dengan standar ISO/IEC 27001 dan ISO/ICE 27002 pada PT Jasa Marga," *Co-Creation J. Ilm. Ekon. Manaj. Akunt. dan Bisnis*, vol. 1, no. 4, pp. 155–164, 2023, doi: 10.55904/cocreation.v1i4.700.
[18] E. Soesanto, M. Rivki Adrian, N. Syifaa Azzahra Suwandi, N. Safitri, and S. Maisa Zahara, "Analisis Keamanan Sistem Informasi di PT.Telkom Menggunakan Indeks KAMI," *IJM Indones. J. Multidiscip.*, vol. 1, pp. 169–175, 2023, [Online]. Available: https://journal.csspublishing/index.php/ijm
[19] M. Nawir, I. AP, and F. Wajidi, "INTEGRASI FRAMEWORK ISO 27001 DAN COBIT 2019 PADA KEAMANAN INFORMASI SMART TOURISM PT. YoY MANAJEMEN INTERNASIONAL," *J-ICON*, vol. 10, no. 2, pp. 122–128, 2022, doi: 10.35508/jicon.v10i2.7985.
[20] M. R. A. Ahadis, G. F. Nama, R. Annisa, and M. A. Muda, "AUDIT TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 5 PADA PT BANK RAKYAT INDONESIA UNIT 1 PRINGSEWU," *J. Inform. dan Tek. Elektro Terap.*, vol. 13, no. 2, pp. 1454–1462, 2025, doi: 10.23960/jitet.v13i2.6474.
[21] K. Wabang, Y. Rahma, A. P. Widodo, and F. Nugraha, "Tata Kelola Teknologi Informasi Menggunakan Cobit 2019 Pada PSI Universitas Muria Kudus," *J. Teknol. dan Sist. Inf.*, vol. 3, no. 3, pp. 2407–1811, 2021.
[22] M. A. Aziz, K. Kusrini, and A. Nasiri, "Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 2019 Domain Align Plan and Organize Studi Kasus: Akademi Komunitas Darussalam Blokagung Banyuwangi," *Tek. Teknol. Inf. dan Multimed.*, vol. 4, no. 2, pp. 132–138, 2023, doi: 10.46764/teknimedia.v4i2.112.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **17/10/2025**; Accepted: **24/10/2025**; Published: **07/11/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 6 November – Desember 2025, Page 2911-2920
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

[23] R. L. V. Nyoto and N. Nyoto, "Analisis Kapabilitas Tata Kelola Teknologi Informasi Perguruan Tinggi XYZ Menggunakan Cobit 2019," *JOISIE (Journal Inf. Syst. Informatics Eng.*, vol. 7, no. 1, pp. 25–34, 2023.
[24] E. Zuraidah and B. M. Sulthon, "Audit Sistem Informasi Perkreditan Pada PT. Aneka Optimal Menggunakan Framework Cobit 4.0," *PROSISKO J. Pengemb. Ris. dan Obs. Sist. Komput.*, vol. 9, no. 1, pp. 67–75, 2022, doi: 10.30656/prosisko.v9i1.4731.
[25] H. Setiawan and Sfenrianto, "Pengukuran Kinerja Menggunakan ITIL V3 Divisi IT Operation PT XYZ," *J. Inf. dan Teknol.*, vol. 5, pp. 102–111, 2023, doi: 10.37034/jidt.v5i1.281.
[26] R. W. P. Pamungkas, A. Najib, B. D. Nuansyah, F. Sukaesih, J. Setiawan, and W. Syafriadi, "Maturity Level Framework ITIL V3 Dalam Mengukur Kepuasan Mahasiswa terhadap Sistem Informasi Akademik," *J. Int. Multidiscip. Res.*, vol. 1, no. 2, pp. 783–788, 2023, [Online]. Available: https://journal.banjaresepacific.com/index.php/jimr
[27] S. N. Amirah, K. Umam, and A. U. Choirunnisa, "IMPLEMENTASI IT INFRASTRUCTURE LIBRARY (ITIL) DALAM PERENCANAAN STRATEGIS TI PADA PT DEF," *J. Pendidik. Sos. dan Hum.*, vol. 4, no. 2, pp. 58–63, 2025.
[28] N. Rachmatullah and T. Sutabri, "Analisis Manajemen Pelayanan Perbankan pada Aplikasi Bri Mobile berbasis TI menggunakan Framework ITIL V3," *Indones. J. Multidiscip. Soc. Technol.*, vol. 1, no. 2, pp. 69–73, 2023, doi: 10.31004/ijmst.v1i2.119.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **17/10/2025**; Accepted: **24/10/2025**; Published: **07/11/2025**