Jurnal Informatika
Vol. 25, No. 2, Desember 2025, pp.24-34
P-ISSN:1693-3877 / E-ISSN: 2407-1544
DOI:10.30873

Melindungi Integritas Data: Audit Kepatuhan Cobit 5 Untuk Sistem Accurate 5

Aliffia Eka Putri[1], Agus Prasetyo Utomo[2], Novita Mariana[3]

[1,2,3] *Fakultas Teknologi Informasi dan Industri, Universitas Stikubank, Jln Tri Lomba Juang No 1 (Mugas), Kota Semarang, 50241, Indonesia*
E-mail: aliffiaep67@gmail.com[1] , mustagus@edu.unisbank.ac.id[2], novita_mariana@edu.unisbank.ac.id[3]

Abstract — ***This study aims to assess the effectiveness and compliance level of information security controls in the Accurate 5 system using the COBIT 5 framework. The evaluation focuses on data protection mechanisms such as access management, encryption, and activity monitoring, which are aligned with the COBIT 5 domains (APO, BAI, DSS, and MEA). Data were collected through a 13-item questionnaire, interviews, and system documentation analysis. The results indicate that the effectiveness of security controls achieved an average score of 4.18, while compliance with COBIT 5 reached an average score of 4.08. This study contributes by providing a practical compliance audit model for IT-based organizations to enhance data integrity and strengthen information security governance.***

Key word — COBIT 5, Security Controls, Data Compliance, Risk Management, Accurate 5 System

Abstrak — **Penelitian ini bertujuan untuk menilai efektivitas dan tingkat kepatuhan kontrol keamanan informasi pada sistem Accurate 5 menggunakan kerangka kerja COBIT 5. Evaluasi dilakukan terhadap mekanisme perlindungan data seperti manajemen akses, enkripsi, dan pemantauan aktivitas yang dikaitkan dengan domain COBIT 5 (APO, BAI, DSS, MEA). Data diperoleh melalui kuesioner berjumlah 13 item, wawancara, dan dokumentasi sistem. Hasil penelitian menunjukkan bahwa efektivitas keamanan memperoleh nilai rata-rata 4,18 dan tingkat kepatuhan terhadap COBIT 5 sebesar 4,08. Penelitian ini berkontribusi sebagai model audit kepatuhan praktis bagi organisasi berbasis TI dalam meningkatkan integritas data dan tata kelola keamanan informasi.**

Kata kunci— **COBIT 5, Security Controls, Data Compliance, Risk Management, Accurate 5 System**

I. PENDAHULUAN

Grup Hitech adalah perusahaan di sektor perdagangan umum yang berfokus pada produk teknologi informasi, termasuk perangkat keras dan perangkat lunak. Sejak didirikan pada tahun 1988, perusahaan ini telah menjadi entitas terkemuka di bidangnya. Dengan pengalaman operasional selama 36 tahun, Grup Hitech memiliki catatan transaksi yang luas dan terus berkembang. Oleh karena itu, sistem informasi akuntansi yang andal diperlukan untuk mengelola laporan keuangan dengan akurat dan tepat waktu. Grup Hitech menggunakan Accurate 5 sebagai sistem informasi akuntansi dan keuangannya, yang dirancang untuk menyederhanakan proses akuntansi serta memfasilitasi masalah perpajakan sesuai peraturan di Indonesia.

Di era digital ini, data menjadi aset yang sangat berharga bagi organisasi. Menjaga integritas data dan mematuhi peraturan yang semakin kompleks menjadi prioritas utama. Organisasi modern, khususnya yang menggunakan sistem aplikasi penting seperti Accurate 5, harus memastikan bahwa data mereka terlindungi dan bahwa kebijakan serta peraturan keamanan diterapkan dengan baik. Audit sistem informasi menggunakan framework COBIT 5 menjadi langkah penting dalam memastikan data tetap aman, terlindungi, dan sesuai dengan persyaratan yang berlaku. Framework

ini telah banyak digunakan untuk menilai efektivitas kontrol keamanan dan kepatuhan di berbagai organisasi, termasuk institusi pendidikan dan perusahaan swasta [1]-[7].

Sistem aplikasi Accurate 5 telah menjadi tulang punggung operasional bagi berbagai organisasi di berbagai industri. Dengan mengelola aspek seperti akuntansi, penggajian, dan manajemen sumber daya manusia, Accurate 5 menyediakan kemudahan dan efisiensi dalam operasi bisnis. Namun, seiring dengan kompleksitas dan ketergantungannya, muncul risiko terkait keamanan data, privasi, dan integritas informasi [8]. Meskipun COBIT 5 telah banyak diterapkan pada sektor pendidikan dan publik [1][7], penelitian terkait audit kepatuhan pada sistem akuntansi Accurate 5 di perusahaan swasta Indonesia masih terbatas, sehingga diperlukan kajian yang lebih spesifik.

Kerangka kerja COBIT 5 diakui secara global sebagai panduan utama dalam mengelola dan mengendalikan teknologi informasi. Dengan fokus pada manajemen risiko, kontrol, dan kepatuhan peraturan, COBIT 5 menawarkan panduan yang kuat untuk mengevaluasi, merencanakan, dan memantau langkah-langkah keamanan data. Dalam melakukan audit terhadap implementasi kontrol dan kebijakan keamanan dalam sistem aplikasi Accurate 5, langkah-langkah COBIT 5 akan membantu memastikan bahwa data Author. terlindungi, proses berjalan sebagaimana mestinya, dan risiko terkendali dengan baik [9].

Tinjauan ini akan memeriksa apakah kontrol keamanan yang diimplementasikan dalam Accurate 5 sesuai dengan standar COBIT 5 dan memenuhi persyaratan regulasi yang relevan. Ini termasuk penilaian manajemen akses, enkripsi data, pemantauan aktivitas, dan penerapan tindakan korektif yang diperlukan. Audit ini juga akan mengidentifikasi potensi risiko yang mungkin timbul dari kegagalan dalam menerapkan kebijakan dan kontrol yang memadai [10].

Untuk mencapai visi ini, laporan berikut akan membahas temuan audit, merekomendasikan tindakan korektif yang diperlukan, dan menyoroti pentingnya menggunakan COBIT 5 sebagai panduan utama untuk memastikan keamanan data dan kepatuhan peraturan dalam konteks sistem aplikasi Accurate 5. Dengan menggabungkan pengalaman industri, pemahaman teknologi, dan panduan COBIT 5, audit ini bertujuan untuk memberikan pandangan holistik dan solusi yang tepat untuk mengatasi tantangan keamanan data dan kepatuhan peraturan dalam lingkungan bisnis yang berubah dengan cepat saat ini.

Dalam penerapan kontrol dan kebijakan keamanan data dalam sistem Accurate 5, terdapat beberapa tantangan signifikan, termasuk efektivitas kontrol keamanan saat ini, kesesuaian dengan standar COBIT 5, dan kepatuhan terhadap peraturan yang berlaku. Pertanyaan kunci yang perlu dijawab adalah: Apakah kontrol keamanan yang diimplementasikan dalam Accurate 5 memadai dan efektif dalam melindungi data? Ini melibatkan evaluasi kekuatan dan efisiensi langkah-langkah keamanan yang ada. Sejauh mana kontrol dan kebijakan yang diimplementasikan dalam Accurate 5 sesuai dengan standar COBIT 5? Ini melibatkan penilaian rinci tentang kesesuaian sistem dengan praktik tata kelola dan manajemen TI yang telah ditetapkan. Terakhir, bagaimana risiko keamanan data diidentifikasi dan dikelola dalam Accurate 5? Ini melibatkan analisis proses penilaian risiko, pemantauan, dan mitigasi untuk memastikan bahwa ancaman keamanan data ditangani dengan baik.

Secara khusus, penelitian ini bertujuan untuk mengevaluasi efektivitas kontrol keamanan data dalam sistem Accurate 5; menilai tingkat kepatuhan terhadap standar COBIT 5; dan mengidentifikasi kesenjangan serta merumuskan rekomendasi untuk meningkatkan keamanan dan kepatuhan regulasi.

Penelitian ini diharapkan memberikan kontribusi praktis bagi organisasi berbasis TI dalam memperkuat tata kelola keamanan informasi, serta kontribusi akademik melalui pengembangan referensi penerapan COBIT 5 dalam sistem akuntansi perusahaan swasta di Indonesia. [11]

II. METODE PENELITIAN

2. 1. Kerangka Kerja COBIT 5

COBIT 5, yang dikembangkan oleh ISACA (Information Systems Audit and Control Association), adalah kerangka kerja yang diakui secara global untuk mengelola dan mengatur TI di tingkat perusahaan. COBIT 5 menawarkan serangkaian panduan dan prinsip yang komprehensif yang bertujuan untuk membantu organisasi mencapai tujuan strategis mereka melalui praktik tata kelola dan manajemen TI yang efektif [12]. COBIT 5 menyediakan alat untuk mengelola aset informasi dan teknologi guna mendorong nilai dan mencapai tujuan organisasi. Kerangka kerja ini telah berhasil diterapkan di berbagai industri, termasuk keuangan, kesehatan, dan manufaktur, yang menunjukkan fleksibilitas dan efektivitasnya dalam berbagai konteks organisasi.

2. 2. Pengumpulan Data

Instrumen penelitian berjumlah 13 item berdasarkan kontrol COBIT 5 dengan skala Likert 1–5. Pengambilan sampel menggunakan teknik total sampling dengan jumlah responden 51 orang. Instumen kuesioner ini mencakup area kunci berikut:

1. Efektivitas Kontrol Keamanan:
   Mengevaluasi kekuatan dan efisiensi langkah-langkah keamanan yang ada, termasuk manajemen akses, enkripsi data, dan pemantauan aktivitas.
2. Kepatuhan dengan Standar COBIT 5: Menilai kesesuaian kontrol dan kebijakan dengan standar COBIT 5, dengan fokus pada praktik tata kelola dan manajemen TI.
3. Identifikasi dan Manajemen Risiko:
   Memeriksa proses penilaian risiko, pemantauan, dan mitigasi untuk memastikan bahwa ancaman keamanan data ditangani dengan baik.

2. 3. Desain Kuesioner

Kuesioner dirancang untuk mengumpulkan data kuantitatif terkait kinerja dan kepatuhan sistem Accurate 5 Domain-domain tersebut meliputi *Deliver, Service, and Support (DSS); Build, Acquire, and Implement (BAI); Monitor, Evaluate, and Assess (MEA); serta Align, Plan, and Organize (APO*). Kuesioner mencakup item spesifik berikut:

Evaluasi Kontrol Keamanan:

1. Kontrol manajemen akses dalam Accurate 5 efektif (SC1).
2. Metode enkripsi data yang digunakan dalam Accurate 5 kuat (SC2).
3. Pemantauan aktivitas dalam Accurte 5 komprehensif (SC3).
4. Kontrol keamanan dalam Accurate 5 secara teratur diperbarui (SC4).

Kepatuhan terhadap Standar COBIT 5:

1. Accurate 5 selaras dengan prinsip manajemen risiko COBIT 5 (Compl1).
2. Kontrol proses bisnis dalam Accurate 5 mengikuti standar COBIT 5 (Compl2).

Identifikasi dan Manajemen

1) Proses manajemen risiko dalam Accurate 5 efektif (IM1).
2) Kebijakan perlindungan data dalam Accurate 5 komprehensif (IM2).
3) Accurate 5 secara rutin melakukan penilaian risiko (IM3).
4) Pemantauan dan evaluasi kontrol keamanan dalam Accurate 5 menyeluruh (IM4).
5) Strategi mitigasi risiko dalam Accurate 5 memadai (IM5)

Implementasi :

1. Accurate 5 memiliki panduan yang jelas untuk menerapkan peningkatan keamanan (RIG1).

2. Organisasi menyediakan dukungan yang memadai untuk meningkatkan keamanan data dalam Accurate 5 (RIG2).

2. 4. Penilaian Kontrol Keamanan

Dengan menggunakan kerangka kerja COBIT 5, efektivitas kontrol keamanan yang diimplementasikan dievaluasi. Ini melibatkan penilaian kecukupan kontrol akses, kekuatan mekanisme enkripsi data, dan efisiensi proses pemantauan aktivitas. Setiap kontrol diukur berdasarkan standar COBIT 5 untuk mengidentifikasi kesenjangan dan area yang perlu diperbaiki.

2. 5. Evaluasi Kepatuhan

Kepatuhan Accurate 5 terhadap peraturan yang relevan, seperti undang-undang perlindungan data, dievaluasi. Ini mencakup peninjauan sejauh mana sistem ini mematuhi persyaratan hukum dan mengidentifikasi masalah ketidakpatuhan yang dapat menimbulkan risiko bagi organisasi [13].

2. 6. Identifikasi & Manajemen Resiko

Risiko potensial yang terkait dengan kontrol dan kebijakan yang tidak memadai diidentifikasi melalui teknik penilaian risiko. Studi ini menganalisis kemungkinan dan dampak dari risiko-risiko tersebut, memberikan profil risiko yang komprehensif untuk Accurate 5. Berdasarkan risiko yang identifikasi , strategi mitigasi diusulkan [14].

2.7. Rekomendasi dan Panduan Implementasi

Berdasarkan temuan, penelitian ini merumuskan rekomendasi untuk meningkatkan keamanan data dan kepatuhan dalam Accurate 5. Rekomendasi ini mencakup Langkah-langkah praktis untuk memperbaiki manajemen akses, memperkuat enkripsi pemantauan. Panduan implementasi disediakan untuk memastikan bahwa rekomendasi ini dapat diintegrasikan secara efektif ke dalam kerangka kerja keamanan organisasi [15].

III. HASIL DAN PEMBAHASAN

3.1. Responden

Kuesioner dalam penelitian ini digunakan sebagai alat utama untuk mengumpulkan data, melibatkan pengawas dan pengguna sistem informasi sebagai responden. Pengawas adalah individu yang bertanggung jawab atas manajemen dan operasional sistem, seringkali dalam peran kepepimpinan, dengan wawasan strategis mengenai keselarasan sistem dengan tujuan bisnis. Pengguna adalah staf atau personel teknis yang berinteraksi langsung dengan sistem sehari-hari, memberikan perspektif praktis mengenai kekuatan dan kelemahan sistem. Menggabungkan pandangan dari kedua kelompok ini memberikan gambaran holistik tentang kinerja sistem informasi, membantu mengidentifikasi area yang perlu perbaikan, dan memastikan sistem memenuhi kebutuhan strategis dan operasional. Data komprehensif yang dikumpulkan melalui kuesioner ini bertujuan untuk memberikan informasi yang dapat ditindaklanjuti guna meningkatkan desain, implementasi, dan manajemen sistem informasi. Jumlah dan distribusi responden dapat dilihat pada Tabel 1.

Tabel 1. Responden

No	Partisipan	Jumlah
1	Manager Operational	4
2	Staff Accounting, Finance, and Purchasing	36
3	Staff IT Operational	6
4	Staff IT Program	5
	Tot	51

3.2. Validitas dan Reliability Instrumen

Validitas kuesioner dievaluasi menggunakan ukuran Kaiser-Meyer-Olkin (KMO) dan uji sphericity Bartlett [16,17]. Nilai KMO sebesar 0.859, yang berada di atas ambang batas 0.6, menunjukkan ukuran sampel yang cukup untuk analisis faktor. Uji Bartlett menghasilkan nilai chi-square signifikan (χ^2 = 675.453, df = 78, p< 0.001), mengindikasikan bahwa korelasi antar item cukup besar untuk analisis faktor. Hasil ini mengonfirmasi validitas instrumen untuk mengukur konstruksi terkait keamanan dan kepatuhan dalam sistem Accurate 5.

Reliabilitas kuesioner dinilai menggunakan Cronbach's Alpha, dengan nilai 0.950 untuk 13 item, jauh di atas ambang batas 0.7 [18]. Ini menunjukkan konsistensi internal yang tinggi dan keandalan dalam mengukur konstruksi yang mendasari. Secara keseluruhan, hasil ini menunjukkan bahwa kuesioner valid dan andal untuk menilai kontrol keamanan, kepatuhan terhadap standar COBIT 5, dan praktik manajemen risiko dalam sistem Accurate 5.

3.3. Analisis data & Hasil Temuan

Berdasarkan Tabel 2 dan 3, hasil temuan memberikan gambaran tentang kondisi saat ini dari kontrol keamanan,kepatuhan,manajemen risiko,dan dukungan untuk peningkatan keamanan dalam sistem Accurate 5. Nilai rata-rata mencerminkan efektivitas dan Tingkat kepuasan keseluruhan dalam area ini, sedangkan standar deviasi menunjukkan variasi dalam tanggapan.

Tabel 2. Evaluasi

Area Evaluasi	Item-Item yang Dievaluasi	Rata-Rata	Std Deviasi
Efektivitas Kontrol Keamanan (*Effectiveness SecurityControls*)	SC1: Kontrol manajemen akses dalam Accurate 5 efektif.	4,45	0,61
	SC2: Metode enkripsi data yang digunakan dalam Accurate 5 kuat	4,39	0,60
	SC3: Pemantauan aktivitas dalam Accurate 5 komprehensif.	4,18	0,62
	SC4: Kontrol keamanan dalam Accurate 5 diperbarui secara berkala.	4,10	0,61
Kepatuhan Terhadap Standar COBIT 5	Compl1: Accurate 5 selaras dengan prinsip manajemen risiko COBIT 5.	4,04	0,89
(*Compliance with COBIT 5 Standards*)	Compl2: Kontrol proses bisnis dalam Accurate 5 mengikuti standar COBIT 5.	4,12	0,89

Identifikasi Manajemen Resiko (Risk Identification and Management)	IM1: Proses manajemen risiko dalam Accurate 5 efektif.	4,10	0,61
	IM2: Kebijakan perlindungan data dalam Accurate 5 komprehensif.	4,08	0,63
	IM3: Accurate 5 secara rutin melakukan penilaian risiko.	4,06	0,79
	IM4: Pemantauan dan evaluasi kontrol keamanan dalam Accurate 5 menyeluruh.	4,00	0,75
	IM5: Strategi mitigasi risiko dalam Accurate 5 memadai.	3,95	0,77
Rekomendasi dan Panduan Implementasi (Recommendations and Implementation Guidance)	RIG1: Accurate 5 memiliki panduan yang jelas untuk menerapkan peningkatan keamanan.	4,12	0,65
	RIG2: Organisasi menyediakan dukungan yang memadai untuk meningkatkan keamanan data dalam Accurate 5.	4,18	0,62

Tabel 3 Isi Hasil Temuan Utama

Area Evaluasi	Temuan Utama	Hasil
Efektivitas Kontrol Keamanan (*Effectiveness of Security Controls*)	Positif	Kontrol akses, enkripsi data, dan pemantauan aktivitas dinilai efektif berdasarkan umpan balik dari responden. Sistem menunjukkan kemampuan yang baik dalam melindungi data dan mengontrol akses.
Kepatuhan Terhadap Standar COBIT (*Compliance with COBIT 5 Standards*)	Sesuai	Implementasi kontrol dan kebijakan dalam Accurate 5 secara umum sesuai dengan prinsip-prinsip manajemen risiko dan standar tata kelola IT COBIT 5.
Identifikasi dan Manajemen Resiko (*Risk Identification and Management*)	Memadai	Proses penilaian risiko, pemantauan, dan mitigasi dianggap memadai oleh pengguna dan pengawas. Namun, ada ruang untuk perbaikan dalam memperkuat beberapa aspek pengelolaan risiko.
Rekomendasi dan Panduan Implementasi (*Recommendations and Implementation Guidance*)	Konstruktif	Rekomendasi yang diberikan mencakup peningkatan dalam manajemen akses, penguatan enkripsi data, dan pemantauan yang lebih komprehensif. Panduan implementasi jelas dan mendukung penerapan perubahan yang disarankan.

Hasil ini Sejalan dengan temuan penelitian yang menyatakan bahwa efektivitas keamanan data berdampak signifikan terhadap performa operasional [19], kebutuhan automasi pemantauan risiko

semakin kritis [20], penelitian ini menunjukkan bahwa peningkatan pada aspek pemantauan otomatis diperlukan untuk mencapai kapabilitas proses Level 5 (Optimizing).

Efektivitas Kontrol Keamanan

SC1: Kontrol Manajemen Akses - Rata- rata: 4,45, Std Dev: 0,61. Nilai rata-rata yang tinggi menunjukkan bahwa responden umumnya setuju bahwa kontrol manajemen akses efektif. Standar deviasi yang rendah menunjukkan pandangan yang konsisten di antara responden

SC2: Metode Enkripsi Data - Rata-rata: 4,39, Std Dev: 0,60. Skor ini mencerminkan konsensus yang kuat mengenai kekuatan metode enkripsi data, meskipun sedikit lebih rendah dari kontrol manajemen akses.

SC3: Pemantauan Aktivitas - Rata-rata: 4,18, Std Dev: 0,62. Nilai rata-rata menunjukkan persepsi positif terhadap komprehensivitas pemantauan aktivitas, dengan variasi tanggapan yang sedikit lebih besar

SC4: Pembaruan Rutin Kontrol Keamanan - Rata-rata: 4,10, Std Dev: 0,61. Ini menunjukkan bahwa kontrol keamanan umumnya diperbarui secara berkala, meskipun masih ada ruang untuk perbaikan.

Rekomendasi: Pertahankan standar tinggi dalam manajemen akses dan enkripsi data; Tingkatkan proses pemantauan aktivitas untuk memperkuat pengawasan dan keamanan; dan Pastikan pembaruan rutin kontrol keamanan diterapkan secara konsisten dan dikomunikasikan di seluruh organisasi.

Kepatuhan terhadap Standar COBIT

Compl1: Kesesuaian dengan Prinsip Manajemen Risiko - Rata-rata: 4,04, Std Dev: 0,89. Tanggapan kesesuaian yang baik dengan prinsip manajemen risiko COBIT 5, meskipun standar deviasi yang lebih tinggi menunjukkan beberapa variasi dalam persepsi.

Compl2: Kontrol Proses Bisnis - Rata- rata: 4,12, Std Dev: 0,89. Ini mencerminkan pandangan positif terhadap kepatuhan dengan standar COBIT 5, dengan variasi tanggapan yang serupa.

Rekomendasi: Lakukan pelatihan dan sesi kesadaran secara berkala untuk menstandarkan pemahaman dan implementasi prinsip-prinsip COBIT 5 di antara semua pemangku kepentingan; Atasi perbedaan dalam praktik kepatuhan untuk mengurangi variasi dan meningkatkan kesesuaian keseluruhan dengan standar.

Identifikasi dan Manajemen Risiko

IM1: Efektivitas Proses Manajemen Risiko - Rata-rata: 4,10, Std Dev: 0,61. Skor tinggi menunjukkan proses manajemen risiko yang efektif, dengan kesepakatan yang konsisten di antara responden.

IM2: Kebijakan Perlindungan Data - Rata-rata: 4,08, Std Dev: 0,63. Skor ini menunjukkan bahwa
kebijakan perlindungan data dipandang komprehensif, meskipun ada ruang untuk perbaikan.

IM3: Penilaian Risiko Rutin - Rata- rata: 4,06, Std Dev: 0,79. Menunjukkan praktik baik dalam melakukan penilaian risiko rutin, dengan lebih banyak variasi dalam seberapa sering dan teliti hal ini dianggap dilakukan.

IM4: Pemantauan dan Evaluasi Kontrol Keamanan - Rata-rata: 4,00, Std Dev: 0,75. Meskipun masih positif, skor ini adalah yang terendah dalam kategori ini, menunjukkan perlunya peningkatan dalam proses pemantauan dan evaluasi.

IM5: Strategi Mitigasi Risiko - Rata- rata: 3,95, Std Dev: 0,77. Ini menunjukkan bahwa strategi mitigasi risiko cukup memadai tetapi dapat ditingkatkan lebih lanjut.

Rekomendasi: Perkuat mekanisme pemantauan dan evaluasi untuk memastikan ketelitian dan konsistensi; Tinjau dan tingkatkan strategi mitigasi risiko, terutama di area yang menunjukkan variasi tanggapan yang lebih tinggi.

Rekomendasi dan Panduan Implementasi

RIG1: Panduan untuk Peningkatan Keamanan - Rata-rata: 4,12, Std Dev: 0,65. Ini mencerminkan kejelasan dalam panduan untuk menerapkan peningkatan keamanan, meskipun masih ada ruang untuk standarisasi.

RIG2: Dukungan Organisasi untuk Keamanan Data - Rata-rata: 4,18, Std Dev: 0,62. Menunjukkan dukungan organisasi yang kuat untuk peningkatan keamanan data, dengan tanggapan yang relatif konsisten.

Rekomendasi: Lanjutkan untuk memperbaiki dan mengkomunikasikan panduan untuk peningkatan keamanan untuk memastikan kejelasan dan konsistensi; Pertahankan dan tingkatkan dukungan organisasi untuk inisiatif keamanan data, memastikan bahwa semua staf diberi informasi dan dilengkapi dengan baik.

Hasil ini secara keseluruhan menunjukkan penilaian yang umumnya positif terhadap kontrol keamanan, kepatuhan dengan standar COBIT 5, dan praktik manajemen risiko dalam sistem Accurate 5. Namun, masih ada area yang memerlukan perbaikan, terutama dalam standarisasi proses dan peningkatan pemantauan serta evaluasi. Dengan mengatasi area ini, organisasi dapat memperkuat bentuk keamanannya dan memastikan kepatuhan yang konsisten dengan praktik terbaik dan standar yang berlaku

3.4. Model Kapabilitas Proses COBIT 5

Berdasarkan hasil audit sistem, responden menilai tingkat pencapaian proses menggunakan model kapabilitas COBIT 5. Tingkat kapabilitas ini menunjukkan sejauh mana proses memenuhi tujuan yang diharapkan:

1. Level 0: Incomplete Process - Proses belum diimplementasikan atau tidak mencapai hasil yang diharapkan.
2. Level 1: Performed Process - Proses telah dilaksanakan, namun mungkin tidak terstruktur dengan baik dan kurang terdokumentasi.
3. Level 2: Managed Process - Proses terencana, diatur, dan dipantau dengan baik, memungkinkan evaluasi dan penyesuaian.
4. Level 3: Established Process - Proses distandarisasi di seluruh organisasi dan dilakukan dengan konsistensi.
5. Level 4: Predictable Process - Proses dipantau dan diukur secara rutin, dengan hasil yang dapat diprediksi.
6. Level 5: Optimizing Process - Proses terus ditingkatkan melalui inovasi dan adaptasi untuk efisiensi dan efektivitas yang lebih baik.

Penilaian ini membantu organisasi mengidentifikasi area untuk perbaikan, memastikan pencapaian tujuan proses secara optimal, dan meningkatkan kapabilitas serta kinerja keseluruhan organisasi, hasil penlaian bisa dilihat pada Tabel 4.

Tabel 4 memberikan evaluasi terperinci mengenai kontrol keamanan, kepatuhan terhadap standar COBIT 5, manajemen risiko, dan panduan implementasi dalam sistem Accurate 5. Setiap aspek dinilai menggunakan skala penilaian dan model kapabilitas COBIT 5.

Efektivitas Kontrol Keamanan:

SC1(Manajemen Akses): Skor rata-rata 4,45 (Kapabilitas 4 - Predictable), menunjukkan proses yang konsisten dan dapat diprediksi.

SC2 (Enkripsi Data): Skor rata- rata 4,39, menunjukkan efektivitas yang kuat.

SC3 (Pemantauan Aktivitas) & SC4 (Pembaruan Rutin): Skor rata-rata masing-masing 4,18 dan 4,10, mengindikasikan manajemen yang baik dengan ruang untuk perbaikan

Kepatuhan dengan Standar COBIT 5:

Compl1 & Compl2**:** Skor rata-rata 4,04 dan 4,12 (Kapabilitas 4 -Predictable), menunjukkan kesesuaian yang baik dengan beberapa variabilitas yang memerlukan standarisasi.

Identifikasi dan Manajemen Risiko:

IM1-IM5: Skor rata-rata 3,95 hingga 4,10, dengan IM5 pada Kapabilitas 3 Established), mengindikasikan kebutuhan untuk memperkuat strategi mitigasi risiko dan konsistensi dalam pemantauan.

Rekomendasi dan Panduan Implementasi:

RIG1 & RG2**:** Skor rata-rata 4,12 dan 4,18, menunjukkan panduan yang jelas dan dukungan organisasi yang kuat. Penting untuk memastikan panduan tersebut diimplementasikan secara konsisten di seluruh organisasi.

Kesimpulan**:** Meskipun Accurate 5 umumnya memiliki kontrol keamanan yang kuat dan kepatuhan terhadap standar COBIT 5, perbaikan diperlukan dalam standarisasi kepatuhan, strategi mitigasi risiko, serta pemantauan dan evaluasi kontrol keamanan. Dengan perbaikan ini, sistem Accurate 5 dapat lebih baik dalam menjamin keamanan data dan keselarasan dengan standar industry.

Tabel 4. Penilaian Model Kapabilitas Proses

Area Evaluasi	Items	Hasil	Rating Scale	Capability Level	Target	Gap
	SC1.	4,45	F	4	5	1
Efektivitas Kontrol Keamanan (*Effectiveness of Security Controls*)	SC2	4,39	F	4	5	1
	SC3	4,18	F	4	5	1
	SC4	4,10	F	4	5	1
Kepatuhan Terhadap Standar COBIT 5 (*Compliance with COBIT 5 Standards*)	Compl1	4,04	F	4	5	1
	Compl2	4,12	F	4	5	1
Identifikasi dan Manajemen Resiko (*Risk Identification and Management*)	IM1	4,10	F	4	5	1
	IM2	4,08	F	4	5	1
	IM3	4,06	F	4	5	1
	IM4	4,00	F	4	5	1
	IM5	3,95	L	3	5	2
Rekomendasi dan Panduan	RIG1	4,12	F	4	5	1

Implementasi R*ecommendations and Implementation Guidance*)	RIG2	4,18	F	4	5	1

Keterangan: Rating Scale F=Fully Achieved, L=Largely Achieved

IV. SIMPULAN

Penelitian ini berhasil mengevaluasi efektivitas kontrol keamanan data pada sistem Accurate 5 menggunakan kerangka kerja COBIT 5, dengan hasil menunjukkan bahwa kontrol keamanan berada pada kategori efektif dengan skor rata-rata 4,18 dan tingkat kepatuhan terhadap COBIT 5 mencapai skor rata-rata 4,08. Meskipun demikian, aspek pemantauan aktivitas dan mitigasi risiko masih memerlukan peningkatan untuk mencapai level kapabilitas yang lebih tinggi. Secara praktis, temuan ini memberikan dasar strategis bagi manajemen dalam memperkuat efektivitas kontrol keamanan, meningkatkan mekanisme pemantauan sistem, serta mengimplementasikan kebijakan tata kelola keamanan data secara berkelanjutan. Selain itu, beberapa penelitian terbaru menunjukkan bahwa pendekatan audit berbasis COBIT 2019 mampu meningkatkan kapabilitas tata kelola TI secara signifikan [21], [22], sehingga penelitian selanjutnya disarankan untuk mengadopsi kerangka COBIT 2019 dan memperluas objek penelitian pada organisasi multi-unit guna memperoleh hasil yang lebih komprehensif dan relevan terhadap tantangan keamanan data modern..

DAFTAR PUSTAKA

[1] T. Handayani and B. V. Christioko, "Audit sistem informasi menggunakan framework COBIT 5 pada LPPM Universitas Semarang," *IJCIT (Indonesian Journal on Computer and Information Technology)*, vol. 8, no. 1, pp. 49–54, 2023.

[2] E. Zuraidah and B. M. Sulthon, "Audit sistem informasi movable fixed asset dan inventory management dengan framework COBIT 5," *KLIK: Kajian Ilmiah Informatika dan Komputer*, vol. 3, no. 6, pp. 1088–1099, Jun. 2023.

[3] D. M. Efendi, S. Mintoro, and I. Septiana, "Audit sistem informasi pelayanan perpustakaan menggunakan framework COBIT 5.0," *Jurnal Informasi dan Komputer*, vol. 7, no. 2, 2019.

[4] M. N. Amalia, F. Akbar, I. Risdiani, A. Islaha, and N. Srilena, "Audit sistem informasi pada perpustakaan ARS University menggunakan framework COBIT 5," *Jurnal Sains dan Informatika*, vol. 6, no. 2, Nov. 2020.

[5] B. A. Saputra, F. N. K. Illahi, and S. Mukaromah, "Audit sistem informasi akademik Stikes Salsabila menggunakan COBIT 5 domain DSS," *Jurnal Ilmiah Ilmu Komputer Fakultas Ilmu Komputer Universitas Al Asyariah Mandar*, vol. 8, no. 1, Apr. 2022.

[6] R. W. Witjaksono, "Audit sistem informasi akademik Universitas Telkom menggunakan framework COBIT 5 domain DSS untuk optimasi proses service delivery," *Jurnal Rekayasa Sistem dan Industri*, vol. 6, no. 1, 2019.

[7] P. Octaviyanti and J. F. Andry, "Audit sistem enterprise asset management menggunakan framework COBIT 5," *IKRAITH-INFORMATIKA*, vol. 2, no. 1, Mar. 2018.

[8] S. V. Grabski, S. A. Leech, and P. J. Schmidt, "A review of ERP research: A future agenda for accounting information systems," *Journal of Information Systems*, vol. 34, no. 1, pp. 157–202, 2020.

[9] A. Gunasekaran, S. Subramanian, and T. Papadopoulos, "Information technology for competitive advantage within logistics and supply chains: A review," *Transportation Research Part E: Logistics and Transportation Review*, vol. 114, pp. 91–114, 2018.

[10] T. Davenport and J. Dyché, *Big Data in Big Companies*. Portland, OR: International Institute for Analytics, 2018.
[11] J. Liu, Y. Liu, and H. Xu, "Security risk assessment in cyber-physical systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 101–111, 2021.
[12] ISACA, *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Schaumburg, IL: ISACA, 2012.
[13] M. Jans, M. Alles, and M. Vasarhelyi, "The case for process mining in auditing: Sources of value added and areas of application," *International Journal of Accounting Information Systems*, vol. 14, no. 1, pp. 1–20, 2013.
[14] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers," *International Journal of Electronic Commerce*, vol. 29, no. 1, pp. 67–104, 2019.
[15] J. J. A. van Doorn, "Developing and implementing COBIT 5 for information security," *ISACA Journal*, vol. 4, pp. 1–44, 2019.
[16] M. D. Goni *et al.*, "Development and validation of knowledge, attitude and practice questionnaire for prevention of respiratory tract infections among Malaysian Hajj pilgrims," *BMC Public Health*, vol. 20, pp. 1–10, 2020.
[17] B. Odoi, S. Twumasi-Ankrah, S. Samita, and S. Al-Hassan, "The efficiency of Bartlett's test using different forms of residuals for testing homogeneity of variance in single and factorial experiments: A simulation study," *Scientific African*, vol. 17, e01323, 2022.
[18] R. B. Toma and N. G. Lederman, "A comprehensive review of instruments measuring attitudes toward science," *Research in Science Education*, vol. 52, no. 2, pp. 567–582, 2022.
[19] A. Putra and I. Nugroho, "Audit keamanan sistem informasi menggunakan framework COBIT 5 pada perusahaan distribusi digital," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 10, no. 3, pp. 245–256, 2023.
[20] R. Pratama and W. Santoso, "Tingkat kepatuhan tata kelola teknologi informasi berbasis COBIT 2019 pada sistem ERP," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 7, no. 4, pp. 560–568, 2023.
[21] J. Alkhaldi, M. Almahmeed, and H. Alshammari, "Risk-based information security strategies: balancing compliance and resilience," *Journal of Cybersecurity*, vol. 10, pp. 1–17, 2024.
[22] S. Rahman and I. Abdillah, "Governance maturity assessment for accounting information systems using COBIT framework," *International Journal of Accounting Information Systems*, vol. 30, pp. 1–14, 2024.