Jurnal Praktik
Keinsinyuran
e-ISSN:3063-7449

Jurnal **Praktik Keinsinyuran** Vol.3 No.5 (September 2026)
journal homepage: http://ejournal.atmajaya.ac.id/index.php/jpk

Implementation of Continuous Auditing to Improve the Effectiveness and Efficiency of Internal Audit: A Practical Study of Telecommunication Company in Indonesia

I Putu Yoga Semadi*[1,2], Hotma Antoni Hutahaean[1], Revelin Anger Saputra[2]

[1]Program Studi Program Profesi Insinyur, Fakultas Biosains, Teknologi, dan Inovasi, Universitas Katolik Indonesia Atma Jaya, Jalan Sudirman 51, Jakarta 12930

[2]Sub Direktorat Internal Audit, PT. Telekomunikasi Selular, Jalan Jenderal Gatot Subroto Kav. 52, Jakarta 12710

Article Info

Article history:

Received
13 June 2026

Accepted
22 June 2026

Keywords:
Continuous Auditing; Internal Audit; User Access Review

Abstract

ABC is the largest digital telecommunications company in Indonesia, providing mobile network services, broadband (including 5G), and integrated digital services. Its operations are supported by backend, middleware, and front-end apps, with access controls defined in the User Access Matrix (UAM). Periodic User Access Reviews (UAR) are conducted to ensure appropriate access rights for employees, vendors, and system users, along with user activity analysis based on prior reconciliation results. Any discrepancies trigger alerts for follow-up. The conventional audit approach requires approximately 90 days and four auditors, making it inefficient. This study aims to improve efficiency through the implementation of continuous auditing based on data analytics using the DMADV Six Sigma methodology. The results show that UAR duration was reduced to 17 days, indicating significant efficiency gains in accelerating review cycles, minimizing data collection bottlenecks, and improving internal audit resource effectiveness.

Info Artikel

Histori Artikel:

Diserahkan:
13 Juni 2026

Diterima:
22 Juni 2026

Kata Kunci:
Audit Berkelanjutan; Audit Internal; Reviu Akses Pengguna

Abstrak

ABC merupakan perusahaan telekomunikasi digital terbesar di Indonesia yang menyediakan layanan jaringan seluler, *broadband* (termasuk 5G), dan layanan digital terintegrasi. Operasionalnya didukung oleh aplikasi *backend*, *middleware*, dan *front-end* dengan pengaturan hak akses dalam *user access matrix* (UAM). Secara berkala, dilakukan *user access review* (UAR) untuk memastikan kesesuaian hak akses bagi karyawan, vendor, dan sistem, serta analisis aktivitas pengguna berdasarkan hasil rekonsiliasi. Ketidaksesuaian akan menghasilkan *alert* untuk tindak lanjut. Metode audit konvensional membutuhkan sekitar 90 hari dan 4 auditor. Penelitian ini bertujuan meningkatkan efisiensi melalui penerapan *continuous auditing* berbasis *data analytics* dengan pendekatan DMADV Six Sigma. Hasil implementasi menunjukkan durasi UAR berhasil ditekan menjadi 17 hari. Hal ini mencerminkan peningkatan efisiensi serta peningkatan efektivitas penggunaan sumber daya Internal Audit.

1. PENDAHULUAN

Perusahaan telekomunikasi beroperasi dalam lingkungan yang sangat padat data, dengan jutaan transaksi dan interaksi pelanggan tercatat setiap hari di berbagai sistem operasional seperti CRM, *billing*, ERP, *payment gateway*, CDR, dan *log* penggunaan

*Corresponding author. I Putu Yoga Semadi
Email address: yoga.semadi@gmail.com

layanan. Pertumbuhan layanan digital dan kanal pembayaran telah meningkatkan volume dan kompleksitas data secara signifikan, sehingga metode audit tradisional yang mengandalkan sampling dan tinjauan berkala sering kali kurang memadai untuk mendeteksi anomali, kebocoran pendapatan, kegagalan pengendalian, maupun indikasi fraud secara tepat waktu.

Data merupakan aset penting yang harus dilindungi untuk menjaga kerahasiaan, integritas, dan ketersediaannya. Meningkatnya volume data, ancaman siber, dan praktik kerja jarak jauh membuat perlindungan data semakin krusial. Selain menerapkan kontrol akses yang kuat, organisasi juga perlu memastikan proses pengelolaan akses tetap efisien dan efektif. Mekanisme kontrol akses harus dirancang untuk meminimalkan penundaan dan mengurangi risiko *false negative*. Dengan memanfaatkan otomatisasi dan menurunkan *false positive*, organisasi dapat menyederhanakan akses pengguna sambil mempertahankan standar keamanan yang kuat (Farhadighalati *et al*., 2025).

Access Control (AC) berperan penting dalam memastikan hanya pihak yang berwenang yang dapat mengakses sumber daya organisasi, sehingga menjadi komponen utama dalam lingkungan sistem yang terhubung dan berbasis data. Sebagai komponen inti dari keamanan data, AC menentukan siapa yang diizinkan untuk mengakses atau melakukan tindakan pada sumber daya sistem dan dalam kondisi apa akses tersebut diberikan. Ia mengelola izin berdasarkan tingkat hak istimewa pengguna, memberikan akses hanya setelah otentikasi berhasil (Farhadighalati *et al*., 2025). Tanpa kontrol akses yang memadai, informasi sensitif berisiko diakses oleh pihak yang tidak berwenang, sehingga meningkatkan risiko pelanggaran privasi, kebocoran data, dan ancaman keamanan organisasi.

Salah satu tantangan utama dalam kontrol akses adalah merancang model kontrol akses terpadu yang mengintegrasikan fitur dari kerangka kerja yang ada, yang seringkali tidak kompatibel (Farhadighalati *et al*., 2025). Untuk mengatasi risiko-risiko ini, organisasi perlu mengadopsi strategi kontrol akses yang kuat dan juga otomatis. Sistem keamanan informasi yang efektif memainkan peran penting dalam melindungi data dari akses tidak sah dan ancaman berbahaya sekaligus memastikan ketersediaannya. Namun, terlepas dari pentingnya langkah-langkah AC yang kuat, banyak organisasi masih menghadapi tantangan dalam menjaga keamanan data yang memadai.

Salah satu organ Perusahaan yang melakukan monitoring atas AC adalah Internal Audit. Internal Audit adalah aktivitas *assurance*, *continuous auditing* (CA) dan *consulting* yang independen dan objektif, yang dirancang untuk memberi nilai tambah dan meningkatkan efektivitas operasional organisasi. Internal Audit membantu organisasi mencapai tujuannya melalui pendekatan yang sistematis dan teratur dalam mengevaluasi dan meningkatkan efektivitas proses manajemen risiko, pengendalian dan tata kelola (Auditors, 2020).

Continuous auditing merupakan evolusi alami dari audit berbasis teknologi yang mengintegrasikan *automated control testing*, *exception monitoring*, dan *data analytics* ke dalam proses audit harian organisasi. Pendekatan ini menempatkan auditor tidak lagi sebagai pihak yang "datang setelah kejadian", tetapi sebagai fungsi yang terlibat aktif dalam siklus pengendalian internal organisasi. Transformasi ini mengubah peran Internal Audit dari fungsi yang reaktif menjadi proaktif, dari *detective control* menjadi *preventive* dan *predictive control*. Auditor tidak hanya mengidentifikasi temuan setelah kerugian terjadi, tetapi mampu mendeteksi anomali transaksi, pelanggaran kebijakan, dan potensi fraud sejak dini (Chan et al., 2018).

Continuous Auditing menawarkan respons yang relevan terhadap tantangan ini. The Institute of Internal Audit (IIA) mendefinisikan *continuous auditing* sebagai kombinasi

penilaian risiko berkelanjutan yang didukung teknologi dan penilaian pengendalian berkelanjutan yang dirancang untuk memungkinkan auditor internal melaporkan masalah pokok dalam jangka waktu yang jauh lebih singkat daripada pendekatan retrospektif tradisional (The IIA, 2025). Selain itu, konsep *Internal Control Integrated Framework* yang dikeluarkan oleh Committee of Sponsoring Organizations of the Treadway Commission (COSO) mengidentifikasi aktivitas pemantauan sebagai salah satu dari lima komponen penting dari sistem pengendalian internal yang efektif, memperkuat logika bahwa risiko dan pengendalian dalam organisasi yang dinamis harus dinilai secara berkelanjutan daripada hanya melalui tinjauan berkala. (COSO, 2023).

Perkembangan analitik data, AI, dan *machine learning* semakin mendorong penerapan *continuous auditing* melalui deteksi anomali *real-time*, analisis risiko, dan pemantauan tindak lanjut audit secara otomatis. Integrasi teknologi ini dengan sistem seperti ERP, CRM, data *warehouse*, dan Microsoft 365 memungkinkan fungsi internal audit menjadi lebih proaktif, efisien, dan berbasis risiko. Penelitian tentang AI dalam Internal Audit juga menunjukkan bahwa *machine learning* (ML), *natural language processing* (NLP), and *robotic process automation* (RPA) dapat meningkatkan cakupan audit (audit *scope*), identifikasi risiko (*risk identification*), dan efisiensi perencanaan, efektivitas pengujian (*fieldwork*), dan aktivitas tindak lanjut (Andriyanto & Januarti, 2026).

Internal Audit 3.0 adalah model operasi masa depan untuk fungsi Internal Audit yang dirancang oleh Deloitte untuk menjawab tantangan risiko modern melalui inovasi dan teknologi yang berfokus pada tiga pilar utama yaitu *Assure* (memberikan kepastian), *Advise* (memberikan saran), dan *Anticipate* (mengantisipasi risiko), yang didukung oleh teknologi cerdas. Salah satu komponen utama Internal Audit 3.0 yaitu *risk sensing* & *learning* yang mengintegrasikan deteksi risiko dini dan pembelajaran mesin untuk melampaui audit tradisional, membantu organisasi tetap unggul dalam menghadapi risiko yang muncul (Deloitte, 2018).

Meskipun *continuous auditing* semakin banyak dibahas, masih terdapat beberapa kesenjangan penelitian. Sebagian besar studi masih bersifat konseptual dan belum mempertimbangkan kompleksitas industri telekomunikasi yang mengandalkan sistem *real-time* terintegrasi. Penelitian *access control* juga lebih berfokus pada aspek teknis dibandingkan pemanfaatannya sebagai objek *continuous auditing*. Selain itu, masih terdapat kesenjangan antara kerangka kerja audit yang bersifat normatif dengan implementasi praktis akibat tantangan kesiapan data, integrasi sistem, dan koordinasi lintas fungsi. Di Indonesia, penelitian *continuous auditing* juga masih terbatas pada pendekatan konseptual dan minim studi kasus praktis.

Berdasarkan kondisi tersebut, penelitian ini bertujuan mengkaji implementasi continuous auditing untuk meningkatkan efektivitas dan efisiensi fungsi internal audit pada perusahaan telekomunikasi di Indonesia, dengan fokus pada pengujian access control secara berkelanjutan, pemanfaatan AI dalam audit internal, serta penerapan praktik global dalam konteks lokal.

2. METODE PELAKSANAAN

2.1 DMADV Six Sigma

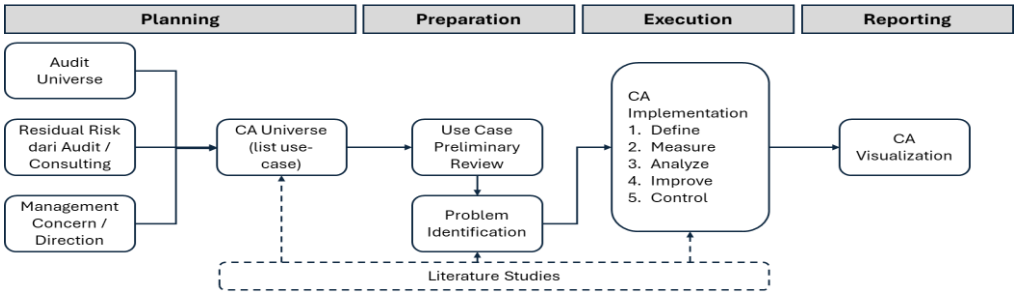
Dalam konteks implementasi continuous auditing, pendekatan DMADV digunakan untuk merancang ulang proses *User Access Review* (UAR) agar lebih efektif, berbasis data, dan mampu berjalan secara berkelanjutan (*continuous*). UAR merupakan proses kritikal dalam memastikan bahwa hak akses pengguna tetap sesuai dengan prinsip *least privilege*

dan *segregation of duties* (SoD). DMADV merupakan singkatan dari lima tahapan utama, yaitu *Define, Measure, Analyze, Design,* dan *Verify* (Alwi, 2023).

1. *Define* (mendefinisikan)
   Tahap *define* berfokus pada identifikasi masalah, tujuan perbaikan, dan pihak yang terlibat. Dalam proses *user access review*, permasalahan utama meliputi pelaksanaan *review* akses yang masih manual dan keterlambatan pencabutan akses bagi karyawan *resign* atau mutasi yang sering menjadi temuan audit. Indikator pada tahap ini mencakup identifikasi sistem prioritas, penetapan SLA pencabutan akses, dan penentuan stakeholder yang terlibat.
2. *Measure* (mengukur)
   Tahap *measure* berfokus pada pengumpulan dan pengukuran data untuk memahami kondisi aktual proses *user access review*. Data yang digunakan meliputi *user list*, *log* aktivitas pengguna, data karyawan (aktif dan terminasi), serta *role & privilege matrix*. Indikator yang diukur mencakup status karyawan organik dan kontrak, data akses pengguna pada aplikasi, serta perubahan status karyawan dari hari sebelumnya untuk mengidentifikasi kebutuhan pencabutan atau penyesuaian akses.
3. *Analyze* (menganalisa)
   Tahap *analyze* berfokus pada analisis data untuk mengidentifikasi akar penyebab masalah. Dalam kasus *user access review*, analisis menunjukkan belum adanya *rule-based monitoring* dan proses UAR yang masih dilakukan secara manual. Indikator pada tahap ini mencakup keselarasan status karyawan dengan hak akses yang dimiliki serta analisis aktivitas pengguna berdasarkan hasil rekonsiliasi sebelumnya.
4. *Design* (merancang)
   Tahap *design* berfokus pada pengembangan solusi yang telah dipilih menjadi rancangan yang siap diimplementasikan. Dalam konteks *user access review*, desain *continuous auditing* mencakup *dashboard* UAR otomatis, *rule-based monitoring*, integrasi data HR dan sistem kritikal, serta pemanfaatan analitik/AI untuk deteksi anomali. Indikator pada tahap ini meliputi persentase sistem yang terintegrasi dan tingkat otomatisasi proses UAR.
5. *Verify* (memverifikasi)
   Tahap *verify* berfokus pada validasi solusi melalui *pilot project* untuk memastikan efektivitas dan kesiapan implementasi. Pada tahap ini dilakukan pengujian akurasi deteksi anomali, perbandingan hasil *review* otomatis dengan manual, serta pengukuran peningkatan efisiensi. Indikator utamanya meliputi penurunan waktu pelaksanaan *user access review* dan berkurangnya temuan audit terkait akses.

2.2 Metodologi Penelitian

Penelitian ini menggunakan desain studi kasus terapan (*applied case study*) pada fungsi Internal Audit di industri telekomunikasi, dengan pendekatan *continuous auditing* berbasis *data analytics*. Desain ini dipilih karena penelitian tidak hanya bertujuan memahami fenomena, tetapi juga mengimplementasikan mekanisme *continuous auditing* secara nyata dalam lingkungan operasional perusahaan.



Gambar 1.
Langkah-langkah penelitian

Penelitian akan mengikuti langkah seperti yang ditunjukkan pada Gambar 1 (Auditor, 2024).

1. Perencanaan (*Planning*)
   Langkah pertama adalah perencanaan *continuous auditing* untuk menyusun CA Universe, yaitu daftar area, proses, risiko, dan objek audit yang dapat dipantau secara berkelanjutan menggunakan teknologi dan analitik data. Secara praktis, CA *Universe* berisi berbagai *use case* yang memiliki risiko tinggi atau merupakan proses inti organisasi. Dalam penyusunan CA *Universe*, beberapa sumber masukan utama yang digunakan meliputi Audit *Universe*, residual risk hasil audit atau konsultasi, *management concern/direction*, serta studi literatur yang mencakup jurnal, penelitian, *benchmarking*, dan referensi terkait industri telekomunikasi. Masukan tersebut membantu memastikan *use case* yang dipilih relevan dengan risiko, prioritas bisnis, dan praktik terbaik yang berlaku.
2. Persiapan (*Preparation*)
   Tahap persiapan merupakan *preliminary review* terhadap *use case* terpilih berdasarkan hasil asesmen risiko. Tahap ini bertujuan mengidentifikasi permasalahan yang akan diselesaikan melalui *continuous auditing*, didukung oleh studi literatur, penelitian, dan *benchmarking* yang relevan dengan *use case* tersebut.
3. Implementasi (*Execution*)
   Permasalahan yang teridentifikasi diselesaikan menggunakan pendekatan DMADV Six Sigma, yang meliputi tahap *Define*, *Measure*, *Analyze*, *Design*, dan *Verify*. Metodologi ini digunakan untuk mengidentifikasi akar penyebab masalah, menentukan kebutuhan bisnis, merancang solusi, serta memvalidasi efektivitas perbaikan yang diusulkan.
4. Pelaporan (*Reporting*)
   Dalam *continuous auditing*, pelaporan dilakukan secara *real-time* atau *near real-time*, bukan lagi secara periodik. Visualisasi melalui *dashboard* dan visual *analytics* menjadi elemen penting untuk menyajikan hasil analisis data secara ringkas, mudah dipahami, dan dapat segera ditindaklanjuti, terutama dalam lingkungan dengan volume data yang besar.

2.3 Kriteria Pengambilan Keputusan

2.3.1 Jenis dan Sumber Data

Penelitian ini menggunakan data primer dan data sekunder. Data primer diperoleh melalui wawancara dengan auditor internal, tim IT security, dan *system owner*, serta observasi proses *user access review*. Sementara itu, data sekunder berasal dari dokumen internal perusahaan, data sistem (*user list*, *log* aktivitas, *role & privilege matrix*), data karyawan, serta literatur akademik dan standar profesional seperti IIA, ISACA, dan COSO.

2.3.2 Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini meliputi wawancara, observasi, dan dokumentasi/data sistem. Wawancara dilakukan dengan pihak yang terlibat dalam audit dan pengelolaan akses untuk memahami proses *user access review*, tantangan pengendalian akses, dan penerapan *continuous auditing*. Observasi digunakan untuk meninjau langsung proses *review* dan pencabutan akses serta penggunaan alat pemantauan. Sementara itu, dokumentasi dan data sistem, seperti *user list*, *log* aktivitas, *role & privilege matrix*, dan laporan audit, digunakan sebagai dasar analisis dan pengukuran indikator penelitian.

2.3.3 Periode Data

Penelitian ini menggunakan data periode 2023–2026 yang mencakup *user list*, aktivitas pengguna, *role & privilege matrix*, temuan audit, dan hasil *user access review* pada sistem kritikal. Periode ini dipilih untuk mengidentifikasi pola anomali serta mengukur perubahan sebelum dan sesudah penerapan *continuous auditing*.

2.3.4 Teknik Analisis Data

Analisis data dilakukan menggunakan pendekatan deskriptif, komparatif, dan data analytics. Analisis deskriptif digunakan untuk menggambarkan kondisi eksisting seperti jumlah pengguna, distribusi hak akses, frekuensi *user access review*, dan temuan akses. Analisis komparatif digunakan untuk membandingkan kondisi sebelum dan sesudah penerapan *continuous auditing* serta efektivitas pemantauan otomatis dibandingkan proses manual. Sementara itu, data *analytics* berbasis aturan (*rule-based*) digunakan untuk mendeteksi anomali, seperti akses aktif milik karyawan nonaktif atau yang telah *resign*/mutasi, dan dapat dikembangkan lebih lanjut dengan *machine learning* untuk deteksi anomali yang lebih canggih.

2.3.5 Validitas dan Reliabilitas Data

Validitas dan reliabilitas data dijaga melalui triangulasi sumber (wawancara, observasi, dan dokumen), triangulasi metode (analisis kualitatif dan kuantitatif), serta *expert judgment* dari praktisi internal audit atau IT *governance*.

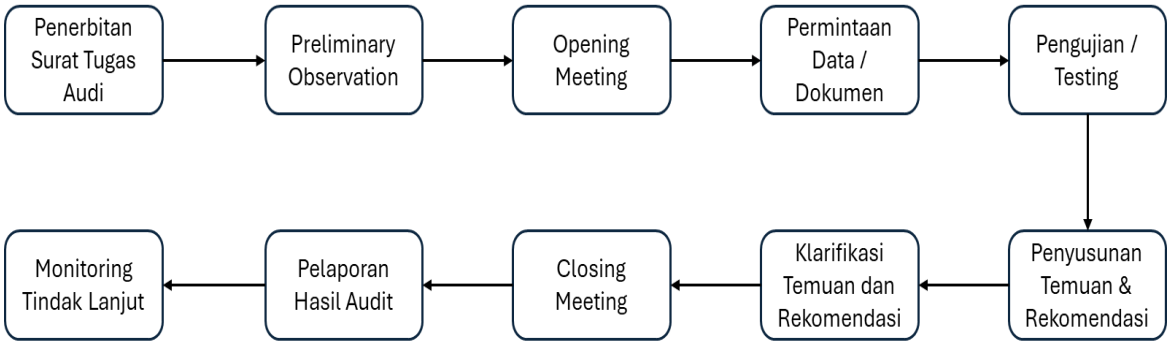
3. HASIL DAN PEMBAHASAN

3.1 Hasil Penelitian

Perusahaan Telekomunikasi ABC merupakan perusahaan telekomunikasi digital yang menyediakan layanan seluler, internet *broadband*, dan berbagai layanan digital yang didukung oleh beragam aplikasi *backend*, *middleware*, dan *front-end*. Setiap aplikasi memiliki pengaturan hak akses yang diatur dalam *User Access Matrix* untuk memastikan pengguna memperoleh akses sesuai fungsi dan perannya.

Sesuai kebijakan perusahaan, *User Access Review* dilakukan setiap tiga bulan untuk meninjau kesesuaian hak akses karyawan, tenaga *outsource*, maupun akun sistem. Proses ini bertujuan memastikan akses diberikan sesuai kebutuhan pekerjaan serta meminimalkan risiko kebocoran data, penyalahgunaan akses, dan manipulasi sistem.

Aktivitas audit tradisional dalam pelaksanaan UAR mengikuti alur proses yang ditunjukkan pada Gambar 2 (Auditor, 2024).



Gambar 2.
Aktivitas Audit Tradisional

3.1.1 *Preliminary Review*

Evaluasi awal dilakukan untuk mengidentifikasi kebutuhan sumber daya serta waktu yang dibutuhkan untuk menyelesaikan setiap aktivitas pada proses audit baik audit konvensional maupun *continuous auditing*.

1. Audit Konvensional

   Kebutuhan sumber daya dan waktu dalam pelaksanaan audit konvensional dapat dijelaskan pada Tabel 1.

Tabel 1.
Kebutuhan sumber daya dan waktu dalam pelaksanaan audit konvensional

No	Aktivitas	Jumlah Sumber Daya (auditor)	Rata-rata waktu yang diperlukan (dalam jam)	Kebutuhan waktu (dalam jam)
1	Penerbitan Surat Tugas Audit	1	4	4
2	*Preliminary Observation*	3	40	120
3	*Opening Meeting*	2	1	2
4	Permintaan Data / Dokumen	4	176	704
5	Pengujian / *Testing*	4	192	768
6	Draft Temuan dan Rekomendasi	4	40	160
7	Klarifikasi Temuan	4	40	160
8	*Closing Meeting*	2	1	2
9	Pelaporan Hasil Audit	3	40	120
10	*Monitoring* Tindak Lanjut	3	40	120
Total Waktu yang diperlukan (dalam jam)				2.160

Perhitungan menunjukkan bahwa audit *User Access Review* memerlukan 2.160 jam (90 hari) dengan melibatkan 4 auditor, yang mencerminkan tingginya kompleksitas dan ketergantungan pada proses manual. Sebagian besar waktu terserap pada pengujian (35,6%) dan permintaan data/dokumen (32,6%), yang secara kumulatif mencapai sekitar 68% dari total waktu audit. Kondisi ini menunjukkan ketergantungan pada pengumpulan data dan pengujian manual, serta rendahnya tingkat otomatisasi dan integrasi sistem.

Selain itu, proses validasi dan klarifikasi temuan juga memerlukan waktu yang signifikan, sementara aktivitas rapat hanya memberikan kontribusi kecil terhadap durasi audit. Tingginya keterlibatan auditor pada tahapan utama menunjukkan bahwa audit konvensional kurang efisien dan sulit diskalakan.

Temuan ini memperkuat kebutuhan implementasi *continuous auditing* melalui integrasi data, otomatisasi pengujian dan pemantauan kontrol, serta pemanfaatan analitik data. Dengan pendekatan ini, proses pengumpulan data dan pengujian dapat dilakukan secara otomatis dan *real-time*, sehingga auditor dapat lebih fokus pada penanganan anomali dan area berisiko tinggi.

Memperhatikan waktu penyelesaian 1 proyek audit selama 90 hari dan jumlah auditor sebanyak 20 orang (9 Auditor Utama, 7 Auditor Madya, serta 4 Auditor Pratama/Staff) serta dengan asumsi pekerjaan dilakukan secara matrik (1 auditor dapat dilibatkan dalam beberapa proyek secara bersamaan), maka dapat dihitung jumlah proyek audit yang dapat dilakukan oleh unit Internal Audit seperti ditunjukkan pada Tabel 2.

Tabel 2.
Jumlah proyek audit dan alokasi *resource* periode 1 tahun

No	Tim	Jan	Feb	Mar	Apr	Mei	Jun	Jul	Ags	Sep	Okt	Nov	Des
1	Tim A		Audit 1										
2	Tim B		Audit 2										
3	Tim C		Audit 3										
4	Tim D		Audit 4										
5	Tim A				Audit 5								
6	Tim B				Audit 6								
7	Tim C				Audit 7								
8	Tim D				Audit 8								
9	Tim A					Audit 9							
10	Tim B					Audit 10							
11	Tim C					Audit 11							
12	Tim D					Audit 12							
13	Tim A						Audit 13						
14	Tim B						Audit 14						
15	Tim C						Audit 15						
16	Tim D						Audit 16						
17	Tim A								Audit 17				
18	Tim B								Audit 18				
19	Tim C								Audit 19				
20	Tim D								Audit 20				
21	Tim A									Audit 21			
22	Tim B									Audit 22			
23	Tim C									Audit 23			
24	Tim D									Audit 24			
25	Tim A										Audit 25		
26	Tim B										Audit 26		
27	Tim C										Audit 27		
28	Tim D										Audit 28		

Melihat perhitungan diatas, maka unit Internal Audit dapat melaksanakan sebanyak 28 proyek Audit.

2. *Continuous Auditing*

Kebutuhan sumber daya dan waktu dalam pelaksanaan *continuous auditing* (CA) dijelaskan pada Tabel 3.

Tabel 3.
Kebutuhan sumber daya dan waktu dalam pelaksanaan *continuous auditing*

No	Aktivitas	Jumlah Sumber Daya (auditor)	Rata-rata waktu yang diperlukan (dalam jam)	Kebutuhan waktu (dalam jam)
1	Penerbitan Surat Tugas Audit	1	4	4
2	*Preliminary Observation*	3	24	72
3	Permintaan Data	2	40	80
4	*Development* CA	2	40	80
5	*Testing*	3	40	120
6	Pelaporan Hasil CA	3	16	48
Total Waktu yang diperlukan (dalam jam)				404

Perhitungan menunjukkan bahwa *Continuous Auditing* UAR memerlukan 404 jam (17 hari) dengan 3 auditor, jauh lebih efisien dibandingkan audit konvensional. Porsi waktu terbesar dialokasikan untuk testing, permintaan data, dan pengembangan CA, yang mencerminkan pergeseran fokus dari aktivitas manual ke pendekatan berbasis sistem dan data.

Dibandingkan audit konvensional, kebutuhan waktu untuk pengumpulan data menurun signifikan berkat integrasi sistem dan ketersediaan data yang lebih baik. Selain itu, jumlah auditor yang terlibat juga lebih sedikit, sehingga penggunaan sumber daya menjadi lebih efisien dan mudah diskalakan.

Meskipun memerlukan investasi awal untuk pengembangan *rule-based monitoring*, *dashboard*, dan integrasi data, solusi ini dapat digunakan kembali pada siklus berikutnya. Secara keseluruhan, penerapan CA UAR mampu mengurangi waktu audit sekitar 81%, mengotomatisasi proses pengujian, mempercepat identifikasi anomali, dan memungkinkan auditor lebih fokus pada analisis serta penanganan risiko.

3.1.2 *Problem Identification*

Berdasarkan evaluasi awal, audit *User Access Review* memerlukan waktu 90 hari. Dengan sumber daya 20 auditor, unit Internal Audit hanya mampu menyelesaikan 28 proyek audit, sehingga masih terdapat gap 30% terhadap target manajemen. Oleh karena itu, penelitian ini berfokus pada penerapan *continuous auditing* untuk mempercepat proses UAR, meningkatkan efektivitas dan efisiensi penggunaan sumber daya, serta mendukung pencapaian target audit yang ditetapkan.

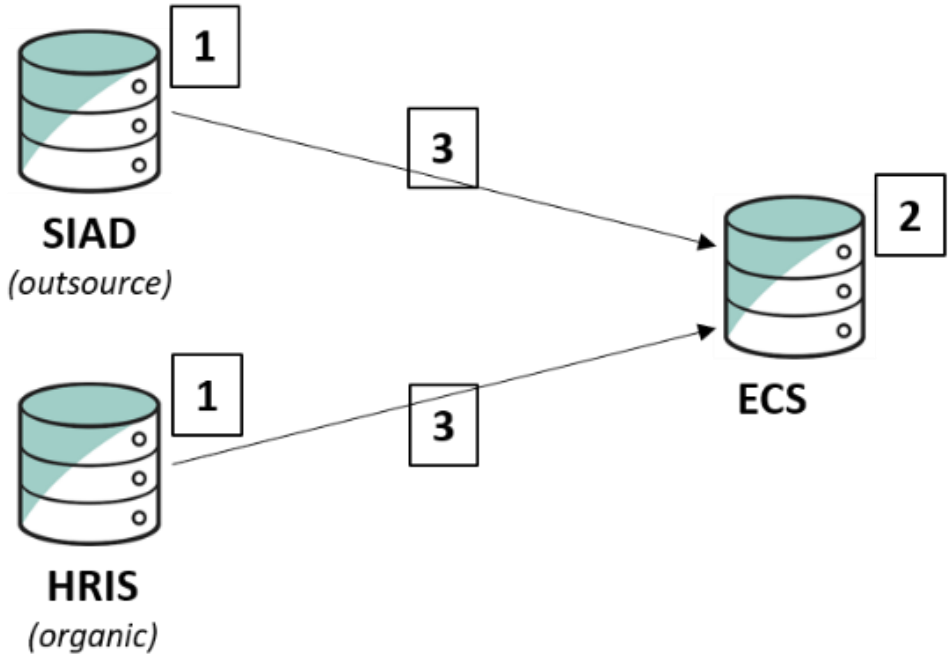
3.1.3 *Problem Solving / Implementation* dengan DMADV Six Sigma

1. *Define*

   Pada tahap Define, permasalahan utama yang diidentifikasi adalah lamanya proses *User Access Review* (90 hari) serta keterlambatan pencabutan akses bagi karyawan *resign* atau mutasi. Fokus perbaikan diarahkan pada sistem prioritas, yaitu SIAD, HRIS, dan *Enterprise Critical Systems* (ECS), dengan target mempercepat SLA pencabutan akses dari 1 hari menjadi *near real-time*. *Stakeholder* yang terlibat meliputi HCM, IT, dan CSM.

2. *Measure*

   Pada tahap ini, dilakukan pengumpulan data-data yang terkait yang berasal dari sistem-sistem utama yang dijelaskan pada gambar 2 dan tabel 4.



Gambar 2.
Gambar Desain Alat Peraga Penyemprotan Bahan Bakar Diesel

Tabel 4.
Pengumpulan data dari sistem terkait per tahun 2023

Jenis Data	HRIS	SIAD	ECS
Jumlah *user* aplikasi			4.739 *records*
Karyawan organik	6.298 *records*		
Karyawan *outsource*		50.935 *records*	
Jumlah *Role*			88 *roles*

Adapun *flow process user access review* dapat dijelaskan sebagai berikut:

a. Analisa karyawan organik (KO) dan karyawan kontrak (KK) dengan status aktif, mutasi, dan *resign*
b. Perbandingan status karyawan antara data KO dan KK pada hari berjalan (D) dengan data hari sebelumnya (D-1)
c. Analisa *user list* dan *role* yang dimiliki
d. Atas status karyawan yang sudah tidak ditemukan pada hari berjalan (D) dibandingkan dengan data hari sebelumnya (D-1), maka akan dilakukan pengecekan ke data *user* pada aplikasi ECS termasuk aktivitas user tersebut selama beberapa waktu kebelakang

3. *Analyze*

Dilakukan analisa lebih mendalam terkait kendala dan penyebab yaitu terkait waktu yang dibutuhkan untuk menyelesaikan *user access review* yang cukup lama serta keterlambatan pencabutan akses untuk karyawan *resign*/mutasi menggunakan referensi berupa hasil reviu terhadap proses audit konvensional, hasil diskusi dengan Tim Audit, serta *benchmarking* dengan organisasi lain. Adapun beberapa kendala dan penyebab yang dihadapi dalam pelaksanaan audit ditunjukkan pada tabel 5.

Tabel 5.
Kendala dalam *user access review*

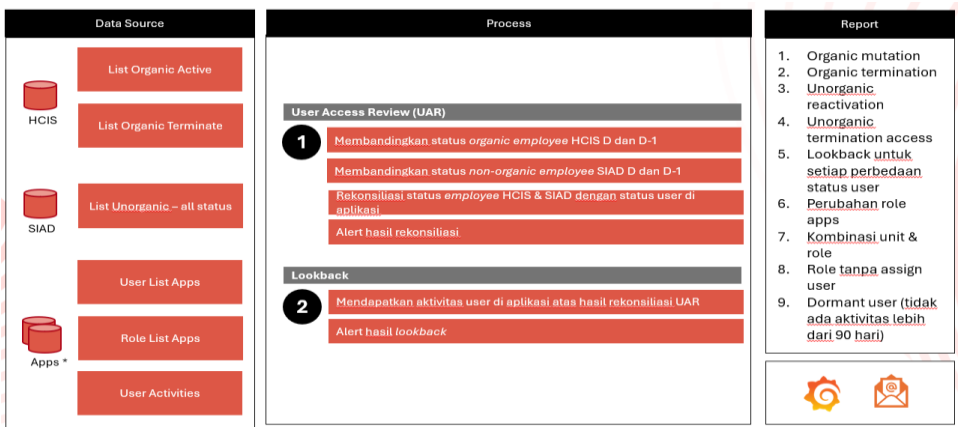
No.	Kendala	Penyebab
1	Pengumpulan data membutuhkan waktu yang lama	• Kompleksitas data yang dianalisa cukup tinggi • Auditee kurang kooperatif (lambat merespon permintaan data, tidak kooperatif, adanya pergantian staff/tim yang membuat pelacakan dokumen menjadi sulit) • Data yang dikirimkan oleh Auditee telah diolah sebelumnya, disisi lain Auditor membutuhkan data asli • Manajemen data disisi Auditee tidak memadai/buruk • Data yang diminta memiliki ukuran yang besar
2	Pengolahan dan analisa data yang membutuhkan waktu lama	• Keterbatasan kemampuan auditor dalam proses pengolahan dan analisa data khususnya data yang komplek dan ukuran data yang besar • Keterbatasan *tool* pengolahan dan analisa data yang digunakan oleh Auditor • Kompleksitas dan ukuran data yang diproses dan dianalisa
3	Kesalahan / *error* pada saat penarikan data	• Perbedaan spesifikasi data yang diminta oleh Auditor dan yang dipahami oleh Auditee • *Error* pada data yang ditarik/*download* karena kesalahan sistem
4	Kesalahan / *error* pada saat pemrosesan data	• Kesalahan *query* pada saat pemrosesan data • Kesalahan/ketidaksesuaian format data • Data kosong (*missing value*)
5	Kesalahan / *error* pada saat analisa data	• Kualitas data yang tidak bagus • Kesalahan memilih metode analisa • Tidak memperhatikan konteks analisa yang diinginkan

Berdasarkan analisis yang dilakukan, kendala utama dalam *User Access Review* terdapat pada proses pengumpulan, pengolahan, serta analisis data. Selain itu, efektivitas proses juga dipengaruhi oleh perbedaan tingkat pemahaman dan kemampuan auditor. Untuk mengatasi kendala tersebut, diperlukan dukungan teknologi melalui penerapan continuous auditing guna meningkatkan efisiensi, konsistensi, dan kecepatan pelaksanaan audit.

4. *Design*

Pada penelitian ini dilakukan otomasi rekonsiliasi dan *monitoring* guna mendeteksi ketidaksesuaian status user secara harian.

a. Model *Architecture*



Gambar 3.
Proses *Continuous Auditing User Access*

Gambar 3 diatas menjelaskan proses penyusunan *continuous auditing* terkait *user access* yang bertujuan untuk memastikan keselarasan antara status karyawan dan hak akses sistem, sekaligus mengidentifikasi potensi risiko akses yang tidak sesuai melalui pendekatan *User Access Review* (UAR) dan *lookback* aktivitas user (melihat aktivitas user pada aplikasi pada periode kebelakang).

i. *Data Source*
   Pada tahap awal, data dikumpulkan dari beberapa sumber utama, yaitu data karyawan organik (KO) baik yang masih aktif maupun terminasi, data karyawan kontrak (KK), serta data dari aplikasi yang mencakup *user list*, *role*, dan aktivitas *user*.
ii. *Process*
   Selanjutnya, dilakukan rekonsiliasi data karyawan dan data pengguna aplikasi untuk memastikan kesesuaian status karyawan dengan hak akses yang dimiliki. Ketidaksesuaian yang ditemukan akan menghasilkan *alert* untuk tindak lanjut. Setelah itu, dilakukan proses *lookback* terhadap aktivitas pengguna guna mengidentifikasi pola penggunaan dan potensi aktivitas yang tidak wajar, yang juga akan menghasilkan alert tambahan.
iii. *Report / Dashboard*
   Hasil analisa perbandingan status karyawan organik dan karyawan kontrak pada hari berjalan (D) dengan data hari sebelumnya (D-1) dan analisa *lookback* terkait aktivitas user pada aplikasi selama periode terakhir ditampilkan pada *dashboard* berupa tampilan visual hasil analisa secara harian serta *alert* atas ketidakwajaran/ketidaksesuaian yang teridentifikasi akan dikirimkan kepada pihak terkait melalui email.

b. *Operating System*

Dashboard continuous auditing dikembangkan menggunakan sistem operasi Linux karena stabil, aman, dan mampu mengelola beban kerja server secara efisien, termasuk untuk layanan backend, database, web server, dan pemrosesan data terjadwal.Selain itu, Linux mendukung berbagai *tools open-source* yang umum digunakan dalam pengembangan sistem berbasis data, sehingga memberikan fleksibilitas dalam integrasi dan pengembangan lanjutan (VandenBrink, 2021).

Linux mendukung pengelolaan sumber daya, keamanan, dan otomatisasi yang dibutuhkan dalam *continuous auditing*. Fitur seperti manajemen hak akses, kontrol jaringan, dan *scheduler* memungkinkan pemrosesan data audit berjalan secara aman, otomatis, dan berkelanjutan, sehingga menjadi fondasi yang andal bagi dashboard *continuous auditing*.

c. *Application Supporting*

Pengembangan *dashboard continuous auditing* memanfaatkan SQL untuk pengelolaan dan analisis data serta Grafana untuk visualisasi dan pemantauan hasil audit. Integrasi keduanya memungkinkan penyajian data secara *real-time*, penyediaan *dashboard* interaktif, serta notifikasi otomatis atas anomali, sehingga mendukung proses continuous auditing yang lebih efektif dan efisien.

d. *Technical Steps*

Implementasi *continuous auditing* dilakukan melalui empat langkah utama: (1) ekstraksi data harian dari data *warehouse* ke server CA, (2) analisis otomatis berdasarkan skenario dan aturan yang telah ditetapkan, (3) penyajian hasil analisis

melalui *dashboard* CA secara harian, dan (4) pengiriman notifikasi otomatis kepada pihak terkait apabila terdeteksi ketidaksesuaian atau anomali yang memerlukan tindak lanjut.

Berdasarkan implementasi CA diatas, diketahui bahwa beberapa proses audit yang sebelumnya dilakukan secara konvensional dapat dilakukan secara otomatis melalui sistem CA.

5. *Verify*

Berdasarkan hasil implementasi *User Access Review*, dilakukan pengukuran terhadap berbagai indikator kinerja selama periode 2023–2026 untuk menilai efektivitas perbaikan proses. Evaluasi ini berfokus pada peningkatan efisiensi waktu penyelesaian, pencapaian target, serta nilai manfaat yang dihasilkan dalam mendukung tata kelola dan pengendalian akses pengguna yang dapat dilihat pada tabel 6.

Tabel 6.
Pengukuran *Outcome Driver* Tahun 2023–2026

Indikator	2023	2024	2025	2026	Satuan
Baseline of Outcome Driver	90	17	17	17	*Days*
Incremental of Outcome Driver	(73)	0	0	0	*Days*
Target of Outcome Driver	17	0	0	0	*Days*
Value per Outcome Driver	83%	0	0	0	%
Overall Outcome Value	17%	0	0	0	%
SLA for revoke access	1	*near real time*	*near real time*	*near real time*	Day

Hasil pengukuran menunjukkan bahwa implementasi *User Access Review* berhasil menurunkan waktu penyelesaian dari 90 hari menjadi 17 hari pada tahun 2023, atau meningkat sekitar 83% dari kondisi awal. Target waktu penyelesaian 17 hari berhasil dicapai dan dipertahankan secara konsisten hingga 2026, menunjukkan bahwa proses telah mencapai tingkat efisiensi yang optimal dan stabil. Meskipun tidak terdapat peningkatan tambahan pada periode berikutnya, implementasi UAR tetap memberikan kontribusi penting terhadap penguatan tata kelola dan pengendalian internal organisasi.

3.2 Pembahasan

Hasil pengukuran menunjukkan bahwa *continuous auditing* pada proses *User Access Review* secara signifikan meningkatkan efisiensi dengan mengurangi aktivitas manual melalui digitalisasi, otomatisasi pengumpulan data, dan standardisasi proses. Implementasi ini juga didukung oleh koordinasi antar unit yang lebih baik, sehingga mempercepat identifikasi dan penyelesaian masalah. Setelah peningkatan besar pada tahap awal, kinerja proses dapat dipertahankan secara stabil melalui pemantauan berkelanjutan.

Meski demikian, penerapan *continuous auditing* memiliki sejumlah tantangan, seperti risiko kualitas data, ketergantungan pada teknologi, resistensi terhadap perubahan, ketergantungan berlebihan pada otomatisasi, serta keterbatasan cakupan deteksi berbasis aturan. Keberhasilan implementasi sangat bergantung pada kesiapan data dan sistem, dukungan manajemen, tata kelola yang jelas, serta kompetensi auditor dalam analitik data.

Penelitian ini juga memiliki keterbatasan karena hanya dilakukan pada satu organisasi dan berfokus pada proses UAR, sehingga hasilnya belum dapat digeneralisasi secara luas. Penelitian selanjutnya disarankan untuk memperluas objek dan sektor penelitian, serta mengeksplorasi penggunaan teknologi yang lebih maju seperti machine learning, anomaly detection, dan predictive analytics guna meningkatkan efektivitas continuous auditing.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Penelitian ini menunjukkan bahwa penerapan *continuous auditing* pada proses *User Access Review* mampu meningkatkan efisiensi audit secara signifikan dengan menurunkan waktu pelaksanaan dari 90 hari menjadi 17 hari (peningkatan 73 hari). Perbaikan ini didorong oleh digitalisasi, otomatisasi pengumpulan data, dan standardisasi proses yang mengurangi aktivitas manual serta meningkatkan pemanfaatan sumber daya.

Nilai *value per outcome driver* sebesar 83% menunjukkan efektivitas implementasi yang tinggi, sementara *overall outcome value* sebesar 17% mencerminkan kontribusinya terhadap kinerja organisasi. Selain meningkatkan efisiensi, *continuous auditing* juga memperkuat pengendalian internal melalui pemantauan yang lebih cepat, konsisten, dan berbasis data.

Namun, keberhasilan implementasi sangat bergantung pada kualitas data, kesiapan teknologi, dukungan manajemen, dan kompetensi SDM. Risiko seperti ketergantungan pada sistem, kesalahan algoritma, dan resistensi terhadap perubahan perlu dikelola dengan baik. Secara keseluruhan, penelitian ini menegaskan bahwa *continuous auditing* merupakan pendekatan yang efektif dan strategis untuk mendukung fungsi audit internal di industri telekomunikasi yang kompleks dan data-*intensive*.

4.2 Saran

Berdasarkan hasil penelitian dan kesimpulan yang diperoleh, berikut beberapa rekomendasi yang dapat dipertimbangkan untuk pengembangan lebih lanjut:

1. Saran Praktis bagi Organisasi
   - Organisasi disarankan untuk memperkuat *governance continuous auditing*, termasuk penetapan kebijakan, prosedur, dan peran yang jelas antara fungsi audit, TI, dan manajemen risiko.
   - Perlu dilakukan investasi pada infrastruktur data dan integrasi sistem, sehingga data yang digunakan dalam *continuous auditing* memiliki kualitas yang tinggi (akurat, lengkap, dan konsisten).
   - Pengembangan kompetensi auditor di bidang data *analytics*, AI, dan teknologi informasi menjadi krusial untuk mendukung efektivitas implementasi.
   - Organisasi juga perlu menerapkan mekanisme validasi dan *oversight*, guna menghindari *over-reliance* terhadap sistem serta memastikan bahwa auditor tetap menggunakan *professional judgment*.
   - Untuk mengatasi *resistance to change*, diperlukan strategi *change management* yang efektif, termasuk pelatihan, sosialisasi, dan dukungan manajemen (*tone at the top*).
2. Saran Pengembangan *Continuous Auditing*
   - *Continuous auditing* sebaiknya tidak hanya diterapkan pada *User Access Review*, tetapi diperluas ke area audit lain seperti *revenue assurance*, *procurement*, *fraud detection*, dan *compliance monitoring*.
   - Pengembangan sistem yang lebih adaptif dengan memanfaatkan *machine learning*, *anomaly detection*, dan *predictive analytics* perlu dipertimbangkan untuk meningkatkan kemampuan deteksi risiko secara *real-time* dan dinamis.
   - Organisasi juga disarankan untuk beralih dari pendekatan *rule-based* menuju *risk-based continuous auditing* yang lebih fleksibel dan responsif terhadap perubahan risiko.

3. Saran untuk Penelitian Selanjutnya
   - Penelitian selanjutnya disarankan untuk melakukan studi lintas industri guna meningkatkan generalisasi hasil penelitian.
   - Perlu dikembangkan indikator evaluasi yang lebih komprehensif, tidak hanya mencakup efisiensi waktu, tetapi juga kualitas audit, akurasi deteksi, serta dampak terhadap pengendalian internal dan kinerja organisasi.
   - Penelitian berbasis studi kasus (*case study*) atau *mixed-method* dengan pendekatan kuantitatif yang lebih kuat dapat memberikan validasi empiris yang lebih mendalam.
   - Eksplorasi terkait integrasi continuous auditing dengan *framework* global seperti IIA, COSO, dan ISACA juga perlu diperluas untuk memperkuat kontribusi teoritis.

5. UCAPAN TERIMA KASIH

Penulis memanjatkan puji syukur kepada Tuhan Yang Maha Esa atas terselesaikannya jurnal ini. Penulis menyampaikan apresiasi kepada VP Internal Audit dan Principal Audit Support and System Development atas dukungan, arahan, dan masukan berharga selama proses penyusunan jurnal. Ucapan terima kasih juga diberikan kepada seluruh pihak yang telah membantu melalui penyediaan data, diskusi, dan berbagai kontribusi konstruktif. Semoga jurnal ini dapat memberikan manfaat bagi pengembangan praktik continuous auditing dan peningkatan efektivitas fungsi Internal Audit.

6. DAFTAR PUSTAKA

1. Alwi, M. (2023). The Use of Continuous Audit to Improve the Effectiveness and Efficiency of Internal Audit Activities: A Practical Study of Distribution Sharia Company in Indonesia. *Journal Page is available to*, 12(2), 603-622.
2. Andriyanto, R., & Januarti, I. (2026). Implementing Artificial Intelligence in Auditing: A Systematic Literature Review of Trends, Challenges, and Adoption. *Owner: Riset dan Jurnal Akuntansi*, 10(2), 1925-1937.
3. Auditor. (2020). *Internal Audit Charter* (pp. 4–5). Jakarta: PT Telekomunikasi Selular.
4. Auditor. (2024). *Manual Audit & Konsultasi* (pp. 31–46). Jakarta: PT Telekomunikasi Selular.
5. Chan, D. Y., Chiu, V., & Vasarhelyi, M. A. (Eds.). (2018). *Continuous auditing: theory and application*. Emerald Publishing Limited.
6. Coso. (2023*). Internal Control*. (https://www.coso.org/guidance-on-ic). Diakses tanggal 2 Juni 2026.
7. Deloitte. (2018). *Internal Audit 3.0*. (https://www.deloitte.com/kz/ru/services/audit-assurance/perspectives/internal-audit-3-0.html). Diakses tanggal 2 Juni 2026.
8. Farhadighalati, N., Jimenez, L. A., Hojjati, S. N., & Barata, J. (2025). A Systematic Review of Access Control Models: Background, Existing Research, and Challenges. *IEEE Access*, 17777-17806.
9. The IIA. (2025). *Continuous Auditing and Monitoring, 3rd Edition*. (https://www.theiia.org/en/content/guidance/recommended/supplemental/gtags/continuous-auditing-and-monitoring). Diakses tanggal 2 Juni 2026.
10. VandenBrink, Rob. (2021). *Linux for Networking Professionals: Securely configure and operate Linux network services for the enterprise*. Packt Publishing.