AKUA: Jurnal Akuntasi dan Keuangan
https://journal.yp3a.org/index.php/AKUA
e-ISSN 2809-851X | p-ISSN 2810-0735
Vol. 5 No. 3 (Juli 2026) 855-861
DOI: 10.54259/akua.v5i3.8330

Pengaruh Kesiapan Organisasi dan Kompetensi Auditor terhadap Keamanan Data Audit pada PT. Agrobisnis Banten Mandiri (Perseroda) Kota Serang

A Deni Iskandarsyah[1*], Fitriana[2], Zaenal Aripin[3]
[1,2,3]Faculty of Pascasarjana, Universitas Sangga Buana YPKP Bandung, Indonesia
Email: [1]adenyiskandarsyah@gmail.com, [2]fitriana@usbypkp.ac.id, [3]zaenal.arifin@usbypkp.ac.id

Abstract

Digital transformation in public sector auditing brings significant challenges to data security. In 2024, Indonesia recorded 21.7 million data breach cases, while audits of regional enterprises revealed weaknesses such as cash-based transactions, invalid attendance records, and unsecured digital assets. These conditions highlight the urgent need for organizational readiness and auditor competence in adopting secure audit technologies. This study aims to examine the influence of organizational readiness and auditor competence on audit data security at PT Agrobisnis Banten Mandiri (Perseroda) Kota Serang. A quantitative approach was applied using descriptive and verificative methods. The research involved all 30 staff members as respondents through total sampling, with data collected via questionnaires, interviews, and documentation. Analysis was conducted using multiple regression with SPSS, supported by validity, reliability, and classical assumption tests. Findings reveal that organizational readiness is relatively strong, though limited by infrastructure and digital oversight culture. Auditor competence is moderate, with adequate regulatory understanding but limited mastery of audit technology. Audit data security has not yet fully aligned with ISO 27001 and the Personal Data Protection Law. Verificative analysis shows organizational readiness has a significant effect on audit data security, auditor competence does not, and together both variables exert a significant influence with organizational readiness as the dominant factor. These results emphasize the importance of strengthening organizational structures to support secure digital audit transformation in regional enterprises.

Keywords: *Digital Transformation, Organizational Readiness, Auditor Competence, Audit Data Security, BUMD.*

Abstrak

Transformasi digital dalam audit sektor publik menghadirkan tantangan serius terhadap keamanan data. Indonesia mencatat 21,7 juta kasus kebocoran data pada tahun 2024, sementara hasil audit BUMD menunjukkan kelemahan seperti transaksi tunai, absensi tidak valid, dan aset digital yang belum diamankan. Penelitian ini bertujuan menganalisis pengaruh kesiapan organisasi dan kompetensi auditor terhadap keamanan data audit di PT Agrobisnis Banten Mandiri (Perseroda) Kota Serang. Pendekatan kuantitatif digunakan dengan metode deskriptif dan verifikatif. Populasi penelitian adalah seluruh staf PT ABM sebanyak 30 orang dengan teknik total sampling. Data dikumpulkan melalui kuesioner, wawancara, dan dokumentasi, kemudian dianalisis menggunakan regresi berganda melalui SPSS dengan uji validitas, reliabilitas, dan asumsi klasik. Hasil penelitian menunjukkan kesiapan organisasi berada pada kategori tinggi meskipun masih terbatas pada aspek infrastruktur dan budaya pengawasan digital. Kompetensi auditor berada pada tingkat sedang, dengan pemahaman regulasi cukup baik namun penguasaan teknologi audit terbatas. Keamanan data audit belum sepenuhnya terintegrasi dengan ISO 27001 dan UU PDP. Analisis verifikatif menegaskan bahwa kesiapan organisasi berpengaruh signifikan terhadap keamanan data audit, kompetensi auditor tidak berpengaruh signifikan, dan secara simultan keduanya berpengaruh dengan dominasi kesiapan organisasi. Temuan ini menekankan pentingnya penguatan kesiapan struktural organisasi dalam mendukung transformasi digital audit di BUMD.

Submitted: 22-06-2026 | Accepted: 11-07-2026 | Published: 15-07-2026

Kata Kunci: Digital Informasi, Kesiapan Organisasi, Kompetensi Auditor, Keamanan Data Audit, BUMD.

1. PENDAHULUAN

Transformasi digital menjadi tantangan utama dalam tata kelola organisasi modern, khususnya dalam pengawasan keuangan. Teknologi audit berbasis digital mendorong efisiensi, transparansi, dan akurasi, tetapi juga membuka celah risiko seperti encryption failure, kebocoran data, dan manipulasi sistem[1]. Ketergantungan terhadap sistem digital menjadikan informasi audit rentan terhadap eksploitasi pihak tidak berwenang. Laporan IBM Security (2024) mencatat bahwa 55% insiden kebocoran data global disebabkan oleh serangan siber, diikuti kesalahan manusia (22%) dan kegagalan sistem informasi (23%)[2]. Data Surfshark (2024) menunjukkan Vietnam menempati posisi pertama di ASEAN dengan lebih dari 37 juta kasus pembajakan email, diikuti Filipina hampir 24 juta kasus. Indonesia berada di peringkat ketiga dengan 21,7 juta kasus, dikategorikan sebagai risiko tinggi[3].

Tabel 1.1 Top 5 Negara ASEAN dengan Kasus Pembajakan Email Tertinggi (2024)

No	Negara	Jumlah Kasus Pembajakan Email	Peringkat ASEAN	Level Risiko Sistem Informasi
1	Vietnam	37.608.041	1	Sangat Tinggi
2	Filipina	23.970.155	2	Tinggi
3	Indonesia	21.769.496	3	Tinggi
4	Malaysia	9.980.273	4	Sedang
5	Thailand	8.254.494	5	Sedang

Sumber: Surfshark Data Breach Recap 2024; diolah dari GoodStats

Fenomena regional ini juga nyata di tingkat lokal. Laporan Audit Operasional tahun 2024 pada salah satu BUMD di Kota Serang menemukan kelemahan dalam pengelolaan data dan sistem informasi. Temuan mencakup transaksi besar yang masih dilakukan tunai, absensi pegawai tidak sinkron, hingga aset digital yang belum diamankan.

Tabel 1.2 Fenomena Keamanan Data Audit di salah satu BUMD di Kota Serang

No	Area yang Ditinjau	Temuan Audit	Dampak terhadap Keamanan Data Audit
1	Pengelolaan Kas & Transaksi	Transaksi besar dilakukan tunai, termasuk gaji direksi dan biaya hukum	Tidak ada sistem cashless; audit trail tidak tercatat elektronik
2	Monitoring Realisasi Anggaran	Tidak tersedia sistem monitoring RKA dan realisasi anggaran	Data keuangan tidak terdokumentasi digital; sulit dilakukan audit forensik
3	Manajemen Rekening & Deposito	9 rekening bank dan 5 deposito tanpa integrasi sistem	Fragmentasi data; menyulitkan audit trail dan meningkatkan risiko manipulasi
4	Piutang Usaha	Piutang meningkat Rp2,4 miliar tanpa sistem penagihan digital	Tidak ada dashboard monitoring; data piutang rawan manipulasi atau kehilangan
5	SDM & Absensi	Absensi tidak sinkron dengan penugasan luar kota; HRIS tidak valid	Validitas data rendah; berpotensi menimbulkan ketidakakuratan audit SDM
6	Website & Transparansi Publik	Website resmi tidak diperbarui	Rendahnya transparansi eksternal; minim kesadaran keamanan informasi digital
7	Aset Digital & Sistem Informasi	Aplikasi internal belum dicatat sebagai aset tidak berwujud dan tidak diamankan	Tidak ada proteksi sistemik; rawan eksploitasi dan kebocoran data

Sumber: LHA Operasional BUMD X Tahun 2024

Temuan audit tersebut menunjukkan sistem informasi belum terintegrasi, transaksi besar masih tunai, dan aset digital belum diamankan. Praktik ini belum mencerminkan standar ideal audit berbasis teknologi yang seharusnya didukung pencatatan elektronik, pengendalian akses, dan proteksi data berbasis enkripsi. Lebih jauh, terdapat gap analysis antara kesiapan BUMD dan sektor swasta. Data OJK (2025) menunjukkan mayoritas bank swasta telah mengadopsi standar ISO 27001 dan sistem real-time monitoring[4]. Sebaliknya, BUMD masih tertinggal dalam penerapan sistem audit digital yang aman, menimbulkan risiko kebocoran data dan lemahnya integrasi pengawasan.

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Penelitian ini hadir untuk mengevaluasi efektivitas sistem pengawasan berbasis teknologi di sektor BUMD, dengan fokus pada kesiapan organisasi dan kompetensi auditor sebagai variabel utama dalam menjaga keamanan data audit. Kajian mengenai transformasi digital dalam audit sektor publik telah banyak dilakukan, namun studi empiris yang menyoroti hubungan kesiapan digital organisasi dan perlindungan keamanan data audit pada level BUMD masih terbatas. Penelitian sebelumnya lebih banyak berfokus pada institusi pusat[5].

Hal ini membuka ruang penelitian untuk menggali efektivitas sistem keamanan data audit berbasis digital dalam organisasi publik yang sedang bertransisi. Penelitian sebelumnya seperti identifikasi tantangan literasi digital auditor[6], ketidaksiapan auditor publik terhadap disrupsi digital[7] dan sebagian besar Supreme Audit Institutions belum memiliki strategi digital terencana, lebih bersifat responsif dibanding berbasis kesiapan internal[8]. Belum banyak riset yang mengombinasikan dimensi kesiapan organisasi dan kompetensi auditor dalam pengawasan berbasis teknologi audit pada sektor BUMD. Padahal, BUMD memiliki karakteristik berbeda dari institusi pusat, terutama dalam hal keterbatasan infrastruktur TI, budaya pengawasan digital yang belum mapan, serta ketergantungan pada transaksi manual. Celah literatur ini penting untuk diisi karena keamanan data audit di BUMD berimplikasi langsung pada akuntabilitas publik daerah. Oleh karena itu, penelitian ini berkontribusi dengan mengkaji pengaruh kesiapan organisasi dan kompetensi auditor terhadap keamanan data audit di BUMD, sebuah konteks yang belum banyak diteliti dalam literatur akuntansi publik. Dari latar belakang tersebut, penulis mengusulkan penelitian tesis berjudul: “Pengaruh Kesiapan Organisasi dan Kompetensi Auditor terhadap Keamanan Data Audit pada PT Agrobisnis Banten Mandiri (Perseroda) Kota Serang.”

Secara teoritis, penelitian ini didukung oleh beberapa kerangka konseptual mutakhir. Pertama, Technology Acceptance Model (TAM) yang menjelaskan penerimaan auditor terhadap teknologi audit digital melalui persepsi kegunaan dan kemudahan penggunaan sistem[9],[10]. Kedua, Resource-Based View (RBV) menekankan bahwa kesiapan organisasi berupa infrastruktur TI, kebijakan keamanan data, dan budaya pengawasan digital merupakan sumber daya strategis yang menentukan keunggulan kompetitif dalam menjaga keamanan data audit[11],[12]. Ketiga, Institutional Theory memberikan perspektif bahwa penerapan audit digital di BUMD tidak hanya dipengaruhi faktor internal, tetapi juga tekanan eksternal berupa regulasi, standar internasional, dan ekspektasi publik[13]. Dengan mengintegrasikan ketiga teori ini, penelitian ini berupaya memberikan pemahaman komprehensif mengenai faktor-faktor yang memengaruhi keamanan data audit di sektor BUMD.

Identifikasi masalah meliputi: sistem keamanan data audit belum sesuai standar ISO 27001 dan UU PDP; kesiapan organisasi menghadapi transformasi digital masih rendah; serta kompetensi auditor dalam teknologi audit masih terbatas. Rumusan masalah mencakup kondisi kesiapan organisasi dan auditor, serta pengaruh keduanya terhadap keamanan data audit. Tujuan penelitian adalah menganalisis kesiapan digital organisasi PT ABM, mengukur pengaruh kesiapan organisasi dan kompetensi auditor terhadap keamanan data audit, serta menilai pengaruh simultan keduanya dalam hal implementasi teknologi audit.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan analisis deskriptif dan verifikatif. Data dikumpulkan melalui kuesioner, wawancara, serta dokumentasi, kemudian diolah menggunakan program SPSS dengan tahapan uji validitas, reliabilitas, asumsi klasik, dan regresi berganda[14]. Jenis data terdiri atas data primer berupa hasil kuesioner staf PT ABM, wawancara informan kunci, serta observasi langsung, dan data sekunder berupa laporan audit operasional, regulasi OJK, UU PDP 2022, serta literatur akademik terkait.

Populasi penelitian adalah seluruh staf PT ABM yang berjumlah 30 orang, dengan teknik total sampling sehingga seluruh populasi dijadikan sampel. Hal ini sesuai dengan konsep *organizational readiness* yang menekankan pentingnya persepsi kolektif anggota organisasi dalam menilai kesiapan menghadapi perubahan[15]. Meskipun jumlah ini relatif kecil untuk analisis regresi berganda, pendekatan ini tetap digunakan karena penelitian mencakup seluruh populasi, bukan sekadar sampel. Validitas penggunaan regresi linear berganda pada sampel kecil didukung oleh Teori Hair yang menegaskan bahwa regresi tetap dapat digunakan apabila asumsi klasik terpenuhi[16]. Dalam penelitian ini, uji normalitas, multikolinearitas, dan heteroskedastisitas menunjukkan hasil yang memenuhi syarat, serta reliabilitas instrumen sangat tinggi (Cronbach’s Alpha > 0.90). Oleh karena itu, regresi linear berganda dipandang dapat untuk menguji pengaruh kesiapan organisasi dan kompetensi auditor terhadap keamanan data audit di BUMD.

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Variabel penelitian terdiri dari variabel independen yaitu kesiapan organisasi (X1) dan kompetensi auditor (X2), serta variabel dependen yaitu keamanan data audit (Y). Kesiapan organisasi diukur melalui indikator infrastruktur TI, kebijakan keamanan data, dan budaya pengawasan digital. Kompetensi auditor diukur melalui pemahaman regulasi, penguasaan teknologi audit, dan kemampuan analisis digital. Keamanan data audit diukur melalui perlindungan data pribadi, sistem enkripsi, dan audit trail digital.

Tabel 2.1 Definisi Variabel Operasional

Variabel & Definisi Operasional	Indikator	Skala	Item Kuesioner
Kesiapan Organisasi: kondisi kolektif institusi dalam merespons perubahan digital	Infrastruktur TI, Kebijakan keamanan data, Budaya pengawasan digital	Ordinal	1–5
Kompetensi Auditor: kemampuan auditor dalam teknologi audit & regulasi	Pemahaman regulasi, Penguasaan teknologi audit, Analisis digital	Ordinal	6–10
Keamanan Data Audit: perlindungan data dari kebocoran/manipulasi	Perlindungan data pribadi, Sistem enkripsi, Audit trail digital	Ordinal	11–15

Sumber: UU PDP 2022; Jaya (2020)

Indikator kesiapan organisasi diadaptasi dari Teori Weiner, indikator kompetensi auditor dari penelitian Mokhtar, indikator keamanan data audit dari UU PDP tahun 2022 serta ISO 27001.

Skala pengukuran menggunakan ordinal 1–5 (STS–SS). Analisis deskriptif digunakan untuk menggambarkan profil responden dan distribusi jawaban, sedangkan analisis verifikatif digunakan untuk menguji hipotesis melalui regresi berganda[17]. Perhitungan mean dilakukan dengan rumus:

$$\bar{x} = \frac{\sum x}{n}$$

Nilai mean diinterpretasikan ke dalam kategori berikut:

Tabel 2.2 Kategori Interpretatif Nilai Mean

Rentang Nilai Mean	Kategori
1,00 – 1,79	Sangat Rendah
1,80 – 2,59	Rendah
2,60 – 3,39	Sedang
3,40 – 4,19	Tinggi
4,20 – 5,00	Sangat Tinggi

Sumber: Sugiyono (2020)

Analisis regresi berganda digunakan untuk menguji pengaruh simultan dan parsial variabel independen terhadap variabel dependen[18]. Persamaan regresi yang digunakan adalah:

$$Y = \alpha + \beta_1 X_1 + \beta_2 X_2 + e$$

Keterangan:

Y= Keamanan Data Audit;
X_1= Kesiapan Organisasi;
X_2= Kompetensi Auditor;
α= Konstanta;
β_1, β_2= Koefisien regresi;
e= Error term.

Uji F digunakan untuk menilai signifikansi simultan, uji t untuk pengaruh parsial, dan R^2 untuk menilai kekuatan variabel independen dalam menjelaskan variabel dependen.

3. HASIL DAN PEMBAHASAN

Profil responden menunjukkan mayoritas berjenis kelamin laki-laki (76,67%), dengan dominasi usia produktif 25–35 tahun (63,33%). Tingkat pendidikan didominasi lulusan S1 (63,33%), sementara jabatan terbagi antara manajer/supervisor (26,67%), kepala seksi/bidang (33,33%), dan staf administrasi (26,67%). Masa kerja sebagian besar berada pada rentang 1–3 tahun (56,67%), menandakan responden cukup mengenal sistem internal namun masih dalam fase adaptasi terhadap transformasi digital. Kondisi ini sejalan dengan pandangan Weiner bahwa kesiapan organisasi dipengaruhi oleh persepsi kolektif anggota terhadap perubahan.

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Analisis deskriptif menunjukkan kesiapan organisasi (X1) berada pada kategori tinggi (mean 3.72). Aturan menjaga data dan pembatasan akses menjadi aspek paling kuat, menandakan adanya kebijakan internal yang jelas. Namun, persepsi terhadap kualitas sistem keamanan masih sedang (mean 3.27), sehingga perlu peningkatan teknis. Hal ini mendukung temuan Jaya bahwa kesiapan organisasi tidak hanya ditentukan oleh kebijakan, tetapi juga oleh kualitas implementasi sistem[19].

Tabel 3.1 Hasil Analisis Deskriptif Variabel (X1 – Kesiapan Organisasi)

Item	Pernyataan	Mean	Kategori
X1.1	Sistem keamanan data perusahaan dinilai baik	3.27	Sedang
X1.2	Ada aturan menjaga data perusahaan	4.13	Tinggi
X1.3	Hanya orang tertentu boleh membuka data penting	4.07	Tinggi
X1.4	Penggunaan komputer/sistem dicatat oleh perusahaan	3.80	Tinggi
X1.5	Perusahaan rutin memeriksa sistem keamanan data	3.43	Tinggi
X1	**Rata-rata keseluruhan**	**3.72**	**Tinggi**

Kompetensi auditor (X2) juga berada pada kategori tinggi (mean 3.56), terutama dalam pemahaman regulasi perlindungan data dan kemampuan mencegah kebocoran. Namun, pelatihan audit digital masih sedang (mean 3.33). Kondisi ini menunjukkan bahwa kompetensi auditor lebih banyak terbentuk dari pengalaman dan pemahaman aturan, bukan dari pelatihan formal berkelanjutan. Temuan ini sejalan dengan Mokhtar et al. yang menekankan pentingnya literasi digital auditor dalam menghadapi risiko kebocoran informasi.

Tabel 3.2 Hasil Analisis Deskriptif Variabel (X2 – Kompetensi Auditor)

Item	Pernyataan	Mean	Kategori
X2.1	Auditor bisa menggunakan sistem audit berbasis komputer	3.57	Tinggi
X2.2	Auditor memahami aturan perlindungan data pribadi	3.73	Tinggi
X2.3	Auditor mampu mencegah risiko kebocoran data	3.60	Tinggi
X2.4	Auditor rutin ikut pelatihan audit digital	3.33	Sedang
X2	**Rata-rata keseluruhan**	**3.56**	**Tinggi**

Keamanan data audit (Y) berada pada kategori tinggi (mean 3.54). Proteksi akses dan integritas data dinilai baik, kepatuhan terhadap aturan pemerintah juga terjaga. Namun, ketersediaan data masih perlu diperkuat agar sistem lebih andal. Hal ini sejalan dengan prinsip UU PDP 2022 yang menekankan pentingnya keandalan sistem elektronik dalam melindungi data pribadi[20].

Tabel 3.3 Hasil Analisis Deskriptif Variabel (Y – Keamanan Data Audit)

Item	Pernyataan	Mean	Kategori
Y1	Data penting tidak bisa dibuka sembarang orang	3.47	Tinggi
Y2	Data tidak bisa diubah pihak tidak bertanggung jawab	3.63	Tinggi
Y3	Data penting selalu tersedia saat dibutuhkan	3.47	Tinggi
Y4	Sistem audit sesuai aturan pemerintah	3.60	Tinggi
Y	**Rata-rata keseluruhan**	**3.54**	**Tinggi**

Uji validitas menunjukkan semua item pernyataan valid (r-hitung > r-tabel), sedangkan uji reliabilitas menghasilkan Cronbach's Alpha > 0.90, menandakan instrumen penelitian reliabel. Uji asumsi klasik menunjukkan data berdistribusi normal, tidak terjadi multikolinearitas, dan tidak terdapat heteroskedastisitas.

Tabel 3.4 Ringkasan Uji Validitas dan Reliabilitas

Variabel	Item	r-hitung	r-tabel	Status	Cronbach's Alpha	Status
Kesiapan Organisasi (X1)	5	0.612–0.781	0.361	Valid	0.912	Reliabel
Kompetensi Auditor (X2)	4	0.598–0.745	0.361	Valid	0.905	Reliabel
Keamanan Data Audit (Y)	4	0.633–0.769	0.361	Valid	0.918	Reliabel

Tabel 3.5 Ringkasan Uji Asumsi Klasik

Uji Asumsi Klasik	Hasil Uji	Status
Normalitas	Kolmogorov-Smirnov p > 0.05	Data normal
Multikolinearitas	VIF < 10; Tolerance > 0.1	Tidak ada masalah
Heteroskedastisitas	Sig. > 0.05 (Glejser Test)	Tidak ada masalah

Hasil uji validitas menunjukkan seluruh item memiliki nilai r-hitung lebih besar dari r-tabel (0.361), sehingga dinyatakan valid. Reliabilitas instrumen juga sangat tinggi dengan Cronbach's Alpha di atas 0.90 untuk semua variabel. Uji asumsi klasik menunjukkan data berdistribusi normal, tidak terjadi multikolinearitas, dan tidak terdapat heteroskedastisitas. Ringkasan hasil uji validitas, reliabilitas, dan asumsi klasik ditampilkan pada Tabel 3.4 dan Tabel 3.5 sebagai bukti transparansi data.

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Hasil uji F menunjukkan kesiapan organisasi dan kompetensi auditor secara simultan berpengaruh signifikan terhadap keamanan data audit (F-hitung 51.963 > F-tabel 2.960; p-value 0.000 < 0.05). Namun, uji t menunjukkan hanya kesiapan organisasi yang berpengaruh signifikan (t-hitung 5.450 > t-tabel; p-value 0.000 < 0.05), sedangkan kompetensi auditor tidak signifikan (t-hitung 0.921 < t-tabel; p-value 0.365 > 0.05).

Koefisien determinasi (adjusted R^2 = 0.779) menunjukkan bahwa 77,9% variasi keamanan data audit dijelaskan oleh kesiapan organisasi dan kompetensi auditor, sementara 22,1% dipengaruhi faktor lain. Persamaan regresi yang diperoleh adalah:

$$Y = 1.393 + 0.638X_1 + 0.139X_2$$

Koefisien X1 signifikan, menunjukkan bahwa peningkatan kesiapan organisasi akan meningkatkan keamanan data audit sebesar 0.638. Koefisien X2 tidak signifikan, menandakan kompetensi auditor belum memberi pengaruh nyata. Temuan ini sejalan dengan Volodina & Grossi yang menegaskan bahwa keberhasilan transformasi digital lebih ditentukan oleh kesiapan struktural organisasi dibandingkan faktor individu.

Hasil penelitian menunjukkan bahwa kompetensi auditor tidak berpengaruh signifikan terhadap keamanan data audit. Temuan ini menekankan bahwa keberhasilan digitalisasi audit lebih ditentukan oleh kesiapan struktural organisasi dibandingkan faktor individu[13]. Dalam BUMD, meskipun auditor memiliki pemahaman regulasi dan kemampuan mencegah kebocoran data, keterbatasan infrastruktur TI dan lemahnya budaya pengawasan digital membuat kompetensi tersebut tidak cukup untuk menjamin keamanan data. Hal ini mendukung perspektif internal kontrol bahwa sistem pengendalian organisasi harus kuat agar kompetensi individu dapat berfungsi optimal. Dengan kata lain, sehebat apa pun auditor, jika sistem organisasi tidak siap, maka data tetap rentan terhadap kebocoran. Temuan ini juga konsisten dalam menyoroti tantangan literasi digital auditor di sektor publik, di mana kompetensi individu sering terhambat oleh keterbatasan sistem kelembagaan[6]. Implikasi praktis dari hasil ini adalah perlunya BUMD memperkuat kebijakan TI, integrasi sistem pengawasan digital, dan budaya keamanan data agar kompetensi auditor dapat berkontribusi lebih signifikan terhadap keamanan data audit.

Secara keseluruhan, hasil penelitian menegaskan bahwa kesiapan organisasi merupakan faktor dominan dalam menjaga keamanan data audit berbasis teknologi. Kompetensi auditor tetap penting sebagai faktor pendukung, namun tanpa dukungan sistem organisasi yang kuat, peran mereka tidak cukup untuk menjamin keamanan data. Implikasi praktis dari temuan ini adalah perlunya BUMD memperkuat kebijakan TI, melakukan integrasi sistem pengawasan berbasis digital, serta meningkatkan kesadaran keamanan data di seluruh level organisasi. Dengan demikian, transformasi digital audit dapat berjalan lebih efektif, aman, dan akuntabel.

4. KESIMPULAN

Penelitian ini menunjukkan bahwa kesiapan organisasi berpengaruh signifikan terhadap keamanan data audit berbasis teknologi, sedangkan kompetensi auditor tidak memberikan pengaruh langsung yang signifikan. Hal ini menegaskan bahwa faktor struktural seperti kebijakan keamanan data, infrastruktur TI, dan budaya pengawasan digital menjadi penentu utama dalam menjaga integritas sistem audit. Dengan adjusted R^2 sebesar 0.779, dapat disimpulkan bahwa sebagian besar variasi keamanan data audit dijelaskan oleh kesiapan organisasi, sementara sisanya dipengaruhi faktor eksternal lain.

Penelitian ini memiliki beberapa keterbatasan. Pertama, jumlah responden relatif kecil (30 orang) karena penelitian menggunakan total sampling pada satu entitas BUMD, sehingga hasilnya belum dapat digeneralisasi ke seluruh BUMD di Indonesia. Kedua, metode analisis yang digunakan adalah regresi linear berganda, yang meskipun sahih untuk populasi kecil, tetap memiliki keterbatasan dalam menangkap kompleksitas hubungan antar variabel dibandingkan metode SEM-PLS. Ketiga, variabel penelitian hanya mencakup kesiapan organisasi dan kompetensi auditor, sementara faktor eksternal seperti dukungan regulasi, budaya kerja, dan teknologi eksternal belum dimasukkan.

Penelitian berikutnya disarankan untuk menggunakan sampel yang lebih luas mencakup beberapa BUMD atau entitas publik lainnya agar hasil dapat digeneralisasi. Selain itu, penggunaan metode analisis yang lebih kompleks seperti SEM-PLS atau multilevel modeling dapat memberikan gambaran yang lebih komprehensif[21]. Penelitian lanjutan juga dapat menambahkan variabel lain seperti budaya kerja, dukungan regulasi, dan faktor teknologi eksternal untuk memperkaya pemahaman mengenai determinan keamanan data audit di sektor publik.

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Berdasarkan temuan penelitian, terdapat beberapa rekomendasi praktis bagi BUMD diantaranya Integrasi sistem pengawasan digital dengan standar keamanan internasional (misalnya ISO 27001) agar audit trail lebih transparan dan akuntabel, Peningkatan kesadaran keamanan data di seluruh level organisasi melalui sosialisasi, pelatihan, dan kampanye internal dan Penguatan kebijakan TI yang mencakup perlindungan data pribadi, sistem enkripsi, dan kontrol akses berbasis digital.

REFERENCES

[1] Mulyadi, *Auditing Berbasis Teknologi Informasi*. Salemba Empat, 2020.

[2] I. B. M. Security, “Cost of a Data Breach Report,” 2024.

[3] Surfshark, “Data Breach Recap 2024,” 2024. [Online]. Available: https://surfshark.com/research/data-breach

[4] O. J. Keuangan, “Laporan Keuangan dan Teknologi Audit 2025,” 2025. [Online]. Available: https://www.ojk.go.id

[5] Mahmudi, “Pengawasan Keuangan Publik di Era Digital,” *Jurnal Akuntansi Publik*, 2022.

[6] A. Mokhtar and others, “Digital Literacy Challenges in Public Audit,” *Journal of Public Sector Accounting*, 2024.

[7] A. Volodina and G. Grossi, “Digital Disruption in Public Audit Institutions,” *International Journal of Public Administration*, 2024.

[8] E. Otia and E. Bracci, “Digital Readiness of Supreme Audit Institutions,” *Public Money & Management*, 2022.

[9] I. S. Latif, R. E. Saputro, and A. S. Barkah, “Technology Acceptance Model using PLS-SEM: A Systematic Literature Review,” *Journal of Information Systems and Informatics*, vol. 7, no. 2, pp. 1191–1201, 2025, doi: 10.51519/journalisi.v7i2.1104.

[10] A. T. Sasongko, M. Ekhsan, and M. Fatchan, “Dataset on technology acceptance in E-learning: A PLS-SEM analysis using extended TAM,” *Telematics and Informatics Reports*, vol. 18, p. 100192, 2025, doi: 10.1016/j.teler.2025.100192.

[11] H. Kuncoro and R. Sari, “RBV in Digital Transformation: Evidence from Indonesian SMEs,” *Journal of Asian Business and Economic Studies*, vol. 29, no. 3, pp. 250–265, 2022, doi: 10.1108/JABES-09-2021-0123.

[12] Z. F. Al-Azzam and M. Al-Qudah, “RBV and IT capabilities in public sector organizations,” *International Journal of Public Sector Management*, vol. 36, no. 2, pp. 145–162, 2023, doi: 10.1108/IJPSM-07-2022-0154.

[13] G. Grossi and I. Steccolini, “Institutional pressures and digitalization in public sector auditing,” *International Journal of Public Administration*, vol. 47, no. 5, pp. 389–402, 2024, doi: 10.1080/01900692.2023.2174567.

[14] I. M. L. M. Jaya, *Metode Penelitian Kuantitatif dan Kualitatif: Teori, Penerapan, dan Riset Nyata*. Anak Hebat Indonesia, 2020. [Online]. Available: https://books.google.co.id/books?id=yz8KEAAAQBAJ

[15] B. Weiner, “A Theory of Organizational Readiness for Change,” *Implementation Science*, vol. 4, no. 67, 2009, doi: 10.1186/1748-5908-4-67.

[16] J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 3rd ed. Sage Publications, 2021.

[17] N. N. Wahid and others, *Metode Penelitian dalam Akuntansi: Pendekatan Kualitatif dan Kuantitatif*. Bayfa Cendekia Indonesia, 2025. [Online]. Available: https://books.google.co.id/books?id=q6ZzEQAAQBAJ

[18] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Alfabeta, 2020.

[19] I. Jaya, *Metode Penelitian Kuantitatif*. Prenada Media, 2020.

[20] R. Indonesia, “Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi,” 2022.

[21] M. Sarstedt, J. F. Hair, M. Pick, B. D. Liengaard, L. Radomir, and C. M. Ringle, “Progress in partial least squares structural equation modeling use in marketing research in the last decade,” *Psychol. Mark.*, vol. 39, no. 5, pp. 1035–1064, 2022, doi: 10.1002/mar.21640.

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)