Akuntansi Pajak dan Kebijakan Ekonomi Digital
Volume.2 Nomor. 3 Agustus 2025
e-ISSN:3046-8132; p-ISSN:3046-868X, Hal 216-231
DOI: https://doi.org/10.61132/apke.v2i3.1429
Available Online at: https://ejournal.areai.or.id/index.php/APKE

Integrasi Teknologi Informasi Akuntansi dan Proteksi Sistem Informasi Akuntansi Terhadap *Cybersecurity Accounting* di Era *Digital*

Sintiya Cahya Maulany[1*], Ety Meikhati[2] Putri Intan Prastiwi[3]
[1-3] Universitas Duta Bangsa, Indonesia

Alamat: Jl. Ki Mangun Sarkoro No.20, Nusukan, Kec. Banjarsari, Kota Surakarta, Jawa Tengah 57135
Korespondensi Penulis: 210416019@mhs.udb.ac.id[*]

Abstract. *This study aims to examine the influence of accounting information technology and accounting information system protection on cybersecurity accounting. Using a quantitative approach, data were collected through a structured survey of 100 respondents, selected using purposive sampling, and analyzed to assess the relationship between the research variables. The research instrument consisted of three main constructs: Accounting Information Technology (X1), Accounting Information System Protection (X2), and Cybersecurity Accounting (Y), each measured using 16 question items. Instrument validity testing revealed that 44 out of 48 items met the validity threshold, with correlation coefficients exceeding 0.300, while reliability analysis indicated Cronbach's Alpha values greater than 0.60 for all variables, confirming internal consistency. Data analysis was performed using multiple linear regression. The results demonstrate that accounting information technology has a positive and statistically significant effect on cybersecurity accounting (coefficient = 0.264; p < 0.05), suggesting that the integration and optimization of technology in accounting processes contribute to enhanced cybersecurity practices. Conversely, accounting information system protection exhibits a negative and statistically significant effect on cybersecurity accounting (coefficient = -0.149; p < 0.05). This unexpected finding indicates that certain protective measures within accounting information systems may, under certain conditions, hinder cybersecurity performance, potentially due to implementation complexity, inadequate configuration, or user resistance. The regression model as a whole is statistically significant (F = 18.577; p = 0.000), with a coefficient of determination (R^2) of 0.277. This implies that the two independent variables together explain 27.7% of the variance in cybersecurity accounting, while the remaining 72.3% is attributable to other factors not examined in this study.*

Keywords: *Accounting Information, Cybersecurity Accounting,System Protection, Technology*

Abstrak. Penelitian ini bertujuan untuk menguji pengaruh teknologi informasi akuntansi dan perlindungan sistem informasi akuntansi terhadap akuntansi keamanan siber. Dengan menggunakan pendekatan kuantitatif, data dikumpulkan melalui survei terstruktur terhadap 100 responden, dipilih menggunakan purposive sampling, dan dianalisis untuk menilai hubungan antara variabel penelitian. Instrumen penelitian terdiri dari tiga konstruk utama: Teknologi Informasi Akuntansi (X1), Perlindungan Sistem Informasi Akuntansi (X2), dan Akuntansi Keamanan Siber (Y), yang masing-masing diukur menggunakan 16 item pertanyaan. Pengujian validitas instrumen mengungkapkan bahwa 44 dari 48 item memenuhi ambang batas validitas, dengan koefisien korelasi melebihi 0,300, sementara analisis reliabilitas menunjukkan nilai Cronbach's Alpha lebih besar dari 0,60 untuk semua variabel, yang mengonfirmasi konsistensi internal. Analisis data dilakukan dengan menggunakan regresi linier berganda. Hasilnya menunjukkan bahwa teknologi informasi akuntansi memiliki efek positif dan signifikan secara statistik terhadap akuntansi keamanan siber (koefisien = 0,264; p < 0,05), yang menunjukkan bahwa integrasi dan optimalisasi teknologi dalam proses akuntansi berkontribusi pada peningkatan praktik keamanan siber. Sebaliknya, perlindungan sistem informasi akuntansi menunjukkan efek negatif dan signifikan secara statistik terhadap akuntansi keamanan siber (koefisien = -0,149; p < 0,05). Temuan tak terduga ini menunjukkan bahwa langkah-langkah perlindungan tertentu dalam sistem informasi akuntansi dapat, dalam kondisi tertentu, menghambat kinerja keamanan siber, kemungkinan karena kompleksitas implementasi, konfigurasi yang tidak memadai, atau resistensi pengguna. Model regresi secara keseluruhan signifikan secara statistik (F = 18,577; p = 0,000), dengan koefisien determinasi (R^2) sebesar 0,277. Hal ini menyiratkan bahwa kedua variabel independen bersama-sama menjelaskan 27,7% varians dalam akuntansi keamanan siber, sementara 72,3% sisanya disebabkan oleh faktor-faktor lain yang tidak diteliti dalam studi ini.

Kata Kunci: Cybersecurity Accounting,Informasi Akuntansi, Proteksi Sistem, Teknologi

Received: Juli 17, 2025; Revised: Juli 31,2025;Accepted: Agustus 05, 2025; Published: Agustus 07, 2025

1. LATAR BELAKANG

Perkembangan teknologi digital dalam sistem keuangan dan akuntansi meningkatkan efisiensi melalui otomatisasi, namun menimbulkan risiko *cybercrime* seperti peretasan dan serangan DDoS. Implementasi *cyber security* yang komprehensif terhadap ancaman eksternal dan internal menjadi krusial untuk menjaga integritas data, mendukung pengambilan keputusan yang optimal, dan mempertahankan kredibilitas perusahaan dalam era digital (Sutisnawinata, 2023. Sektor perbankan Indonesia mengalami peningkatan serangan siber yang signifikan, seperti kasus peretasan BSI oleh LockBit (Mei 2023) dengan kerugian Rp295,6 miliar dan serangan *Conti* terhadap Bank Indonesia (2021)(Hatta & Rahmah, 2024;Pusparisa, 2024). BSSN mencatat 122,79 juta anomali trafik pada Januari-Agustus 2024, dengan serangan utama berupa *ransomware*, *phishing*, dan *DDoS* yang menargetkan infrastruktur kritikal dan sektor keuangan. Kondisi ini menunjukkan urgensi implementasi kebijakan keamanan informasi komprehensif dan teknologi proteksi terkini untuk menjaga integritas sistem keuangan nasional.

Teknologi Informasi Akuntansi (TIA) didefinisikan sebagai *konvergensi sistemik* antara perangkat keras, perangkat lunak, dan infrastruktur sistem informasi yang dikonfigurasi untuk mengoptimalkan pemrosesan data akuntansi dengan tingkat efisiensi dan akurasi yang tinggi, sehingga memfasilitasi pengelolaan informasi keuangan yang responsif, transparan, dan terintegrasi secara *holistik*. Dalam dimensi keamanan informasi, (TIA) memainkan peran *fundamental* dalam *preservasi integritas* data melalui implementasi mekanisme proteksi berlapis yang mencakup *enkripsi data*, sistem *autentikasi multi-faktor*, dan *monitoring* sistem secara *real-time* untuk mitigasi risiko kebocoran informasi dan ancaman serangan siber (Madani et al., 2024; Eko & Mindy, 2025). Interkoneksi antara (TIA) dan *cybersecurity accounting* termanifestasi dalam kapasitas teknologi ini untuk mengidentifikasi, menganalisis, dan merespons ancaman siber yang berpotensi mengkompromikan integritas data finansial, sehingga berkontribusi pada peningkatan tingkat kepercayaan pengguna terhadap reliabilitas sistem keamanan data (Nurwanah, 2024; Morshed & Khrais, 2025). Namun demikian, temuan empiris Prabawa et al., (2024) mengindikasikan bahwa implementasi sistem kontrol teknologi informasi pada institusi keuangan masih menunjukkan gap efektivitas dalam pencegahan dan deteksi aktivitas *fraudulent,* sehingga memerlukan revitalisasi prosedur audit *internal* yang lebih komprehensif. Berdasarkan kerangka teoritis *IT Capability Theory* yang diajukan oleh Bharadwaj et al., (1999), optimalisasi kapabilitas (TIA) terbukti dapat mengakselerasi efisiensi operasional dan memperkuat arsitektur keamanan sistem, yang pada akhirnya mendukung *sustainabilitas* dan *kredibilitas* sistem informasi akuntansi dalam jangka panjang.

Proteksi Sistem Informasi Akuntansi merupakan implementasi mekanisme *defensif komprehensif* yang dirancang untuk mengamankan data akuntansi dari ancaman *eksternal* dan *internal* melalui penerapan teknologi *enkripsi, firewall,* kontrol akses, dan prosedur *mitigasi* ancaman (Husna et al., 2024; Vanhorn & Shutterstock, 2021). Korelasi integral antara proteksi sistem informasi akuntansi dan *cybersecurity accounting* termanifestasi dalam peningkatan kapabilitas organisasi untuk melindungi data keuangan dari ancaman *cyber* yang dapat mengkompromikan integritas laporan keuangan dan reputasi perusahaan (Kafi & Akter, 2017; Saputra et al., 2023). Berdasarkan *Protection Motivation Theory (PMT),* entitas bisnis mengadopsi langkah-langkah protektif melalui evaluasi sistematis terhadap tingkat ancaman dan efektivitas tindakan perlindungan yang diimplementasikan, sehingga organisasi dengan sistem proteksi optimal menunjukkan kapasitas superior dalam menghadapi ancaman keamanan *cyber* yang berpotensi mempengaruhi integritas data akuntansi (Siponen et al., 2023; Hapsah & Irwan, 2023).

Cybersecurity Accounting merupakan implementasi sistematis dari protokol keamanan dan infrastruktur teknologi yang dikonfigurasi untuk melindungi sistem informasi akuntansi dari spektrum ancaman siber, dengan tujuan memastikan kerahasiaan, integritas, dan *availabilitas* data akuntansi yang bersifat sensitif (Hasan et al., 2024). Konsep ini memainkan peran fundamental dalam preservasi data keuangan perusahaan dari risiko serangan *cyber* dan mempertahankan transparansi serta *kredibilitas* laporan keuangan yang dihasilkan melalui sistem akuntansi digital (Nyombi et al., 2024). *Cybersecurity accounting* menunjukkan interkoneksi yang signifikan dengan kebijakan keamanan informasi, teknologi informasi akuntansi, dan proteksi sistem informasi akuntansi, di mana integrasi yang efektif dari ketiga elemen tersebut dapat mengoptimalkan kapabilitas perlindungan terhadap ancaman *cyber* dan memastikan *preservasi* data dari serangan sistem akuntansi (Lehenchuk et al., 2022; Arfan et al., 2023; Lindemulder & Kosinski, 2024). Berdasarkan kerangka *Cybersecurity Management Theory,* pengelolaan risiko yang efektif melalui implementasi kebijakan keamanan yang komprehensif, teknologi yang *resilient,* dan proteksi yang *adequate* akan menciptakan ekosistem yang lebih *secure* untuk data keuangan perusahaan (Husna et al., 2024).

Penelitian ini bertujuan untuk menguji secara empiris pengaruh Teknologi Informasi Akuntansi dan Proteksi Sistem Informasi Akuntansi terhadap penerapan Cybersecurity Accounting dalam menghadapi tantangan era digital, baik secara parsial maupun simultan. Melalui pendekatan analisis regresi linear berganda, penelitian ini berfokus pada sejauh mana integrasi teknologi informasi dan sistem proteksi mampu meningkatkan Cybersecurity dalam konteks akuntansi digital.

2. KAJIAN TEORITIS

Stakeholder Theory

Teori *stakeholder* merupakan *konstruk* teoretis dalam manajemen strategis yang menekankan *responsibilitas* perusahaan terhadap seluruh entitas berkepentingan, meliputi pemegang saham, karyawan, pelanggan, regulator, pemerintah, dan masyarakat (Harrison et al., 2015; Freeman & Verlag, 2024). Teori ini menunjukkan relevansi substansial karena *vulnerabilitas* sistem informasi akuntansi dapat mempengaruhi performansi operasional internal dan kredibilitas *stakeholder* eksternal, sementara teknologi informasi akuntansi yang mencakup sistem *cloud, big data*, dan (*ERP)* memerlukan integrasi manajemen risiko untuk menghadapi kompleksitas ancaman keamanan (Janvrin & Wang, 2019; Madani et al., 2024). Proteksi sistem informasi akuntansi merupakan *responsibilitas* kolektif yang melibatkan multipihak untuk melindungi data dari ancaman *cyber* melalui implementasi protokol teknis dan pemahaman peran setiap *stakeholder*, sehingga penelitian yang mengkaji pengaruh teknologi informasi akuntansi dan proteksi sistem informasi akuntansi dapat diselaraskan dengan teori *stakeholder* untuk menciptakan *value-added* yang signifikan dan menjadikan teori ini sebagai fondasi teoretis dalam pengelolaan sistem informasi akuntansi yang berkelanjutan (Kehista et al., 2023; Putri & Martha, 2022).

IT Capability Theory

Berdasarkan IT Capability Theory yang dikembangkan (Bharadwaj et al., 1999), optimalisasi kapabilitas Teknologi Informasi Akuntansi (TIA) merupakan proses integrasi tiga dimensi utama yaitu infrastruktur teknologi, kompetensi sumber daya manusia, dan aset pengetahuan perusahaan. Teori ini menjelaskan bahwa penguatan kapabilitas (TIA) secara sistematis akan menghasilkan peningkatan efisiensi operasional melalui otomatisasi proses dan minimalisasi kesalahan, serta penguatan sistem keamanan melalui implementasi kontrol *internal* yang efektif. Dampak jangka panjang dari optimalisasi ini adalah terciptanya *sustainabilitas* sistem yang mampu beradaptasi dengan dinamika regulasi dan kebutuhan organisasi, sekaligus meningkatkan kredibilitas informasi keuangan yang dihasilkan. Dengan demikian, penerapan *IT Capability Theory* dalam konteks (TIA) tidak hanya berfungsi sebagai enabler efisiensi operasional, tetapi juga sebagai fondasi strategis untuk mencapai keunggulan kompetitif berkelanjutan melalui penyediaan informasi akuntansi yang akurat, *reliabel*, dan tepat waktu.

Protection Motivation Theory

Protection Motivation Theory (PMT) yang dikembangkan oleh Ronald W. Rogers pada tahun 1975 dan disempurnakan pada 1983, menjelaskan bahwa organisasi terdorong untuk mengambil langkah-langkah proteksi, termasuk dalam konteks sistem informasi akuntansi, berdasarkan dua proses evaluasi utama, yaitu penilaian terhadap ancaman (threat appraisal) dan penilaian terhadap kemampuan mengatasi ancaman (coping appraisal). Dalam penilaian ancaman, organisasi mengevaluasi tingkat kerentanan dan keparahan risiko *cyber* yang dapat mengancam integritas data akuntansi, sedangkan dalam penilaian kemampuan mengatasi, organisasi menilai efektivitas, kapabilitas *internal*, dan biaya implementasi dari tindakan protektif yang akan diterapkan. Organisasi akan termotivasi mengimplementasikan kontrol keamanan seperti *enkripsi data*, sistem *backup*, *multi-factor authentication*, dan *monitoring* berkelanjutan ketika mereka *mempersepsikan* ancaman *cyber* sebagai serius namun yakin dapat mengatasinya dengan efektif dan biaya yang wajar. Penerapan PMT yang konsisten memungkinkan organisasi mengembangkan sistem proteksi optimal yang meningkatkan kapasitas dalam menghadapi ancaman keamanan *cyber* dan menjaga reliabilitas pelaporan keuangan serta kepatuhan regulasi akuntansi (Siponen et al., 2023).

Cybersecurity Management Theory

Berdasarkan *Cybersecurity Management Theory*, pengelolaan risiko yang efektif melalui implementasi kebijakan keamanan yang komprehensif, teknologi yang resilient, dan proteksi yang *adequate* akan menciptakan ekosistem yang lebih *secure* untuk data keuangan perusahaan. Dalam penelitian *cybersecurity accounting*, teori ini memberikan fondasi teoretis yang kuat untuk memahami bagaimana sistem akuntansi modern memerlukan integrasi strategi keamanan siber yang *holistik* guna melindungi integritas, kerahasiaan, dan ketersediaan informasi keuangan. Implementasi *cybersecurity* dalam praktik akuntansi tidak hanya melibatkan aspek teknis seperti *enkripsi data* dan kontrol akses, tetapi juga mencakup dimensi organisasional berupa kebijakan tata kelola risiko, pelatihan kesadaran keamanan, dan mekanisme respons insiden. Kerangka ini menekankan pentingnya pendekatan berlapis (*defense-in-depth*) dalam melindungi aset informasi keuangan, dimana setiap lapisan keamanan saling memperkuat untuk menciptakan ekosistem yang *robust* terhadap ancaman siber yang terus berkembang, sekaligus memastikan kepatuhan terhadap regulasi keuangan yang berlaku (Salim et al., 2016)

Penelitian Terdahulu

Implementasi teknologi informasi akuntansi menunjukkan pengaruh positif signifikan terhadap *cybersecurity accounting* melalui *enkripsi, autentikasi multi*-faktor, dan AI (Kafi & Akter, 2017), Penelitian tersebut tidak sejalan dengan penelitian Eaton et al. (2019), menunjukkan bahwa keterbatasan efektivitas teknologi diakibatkan oleh kegagalan organisasi dalam mengungkapkan informasi material terkait serangan siber.

Penelitian Lehenchuk et. al. (2022) menunjukkan bahwa penerapan budaya *cybersecurity* yang menyeluruh memberikan pengaruh signifikan terhadap peningkatan keamanan sistem informasi akuntansi. Penelitian tersebut tidak sejalan dengan penelitian menunjukkan Nurwanah (2024) faktor manusia tetap menjadi kelemahan utama yang dapat menurunkan efektivitas *cybersecurity accounting.*

Siponen et al. (2023) dalam penelitiannya menunjukkan bahwa *cybersecurity accounting* memberikan kontribusi signifikan pada kualitas pelaporan keuangan dan nilai pasar. Namun, Tidak sejalan dengan penelitian Gordon et al., (2021) menunjukkan pengukuran dampak jangka panjang dari sistem informasi akuntansi dan keamanan siber memerlukan pendekatan metodologis yang lebih kuat dan kuantitatif

3. METODE PENELITIAN

Ruang Lingkup Penelitian

Penelitian ini mengkaji pengaruh teknologi informasi akuntansi dan proteksi sistem informasi akuntansi terhadap *cybersecurity accounting* melalui pendekatan kuantitatif dengan instrumen kuesioner yang disebarkan kepada profesional akuntansi, auditor, dan praktisi teknologi informasi pada perusahaan yang mengimplementasikan sistem informasi akuntansi digital. Variabel independen meliputi teknologi informasi akuntansi yang dioperasionalkan melalui dimensi infrastruktur, kapabilitas, keahlian, dan integrasi sistem, serta proteksi sistem informasi akuntansi yang diukur berdasarkan perlindungan data, sistem pertahanan *cyber*, respons ancaman, dan keberlanjutan proteksi. Variabel dependen *cybersecurity accounting* dikonstruksi berdasarkan aspek kerahasiaan, integritas, ketersediaan, dan pemulihan pasca-insiden, dengan analisis data menggunakan regresi linier berganda untuk menguji pengaruh simultan dan parsial guna menghasilkan *evidensi* empiris kontribusi faktor-faktor determinan *cybersecurity accounting.*

Sumber dan Jenis Data

Sumber Penelitian

Penelitian ini menggunakan data primer yang diperoleh melalui instrumen survei kuesioner yang disebarkan kepada responden profesional akuntansi, auditor, dan praktisi teknologi informasi yang memiliki pengalaman dalam implementasi sistem informasi akuntansi digital. Instrumen kuesioner dirancang untuk mengoperasionalkan dan mengukur variabel teknologi informasi akuntansi, proteksi sistem informasi akuntansi, dan *cybersecurity accounting* guna memperoleh data empiris yang relevan dengan *konstruk* penelitian.

Jenis Data

Data kuantitatif dikumpulkan melalui kuesioner skala *Likert* untuk mengukur variabel teknologi informasi akuntansi, proteksi sistem informasi akuntansi, dan *cybersecurity accounting*, yang memfasilitasi analisis statistik untuk pengujian hipotesis dan menghasilkan temuan yang objektif serta dapat digeneralisasikan.

Populasi, metode Sampling dan sampel penelitian

Populasi penelitian ini terdefinisi sebagai perusahaan dan institusi *multisektor* (pendidikan, perdagangan, teknologi) yang mengoperasionalkan sistem informasi akuntansi berbasis digital dengan *eksposur* terhadap risiko ancaman siber. Teknik *purposive* sampling diimplementasikan berdasarkan kriteria seleksi yang mencakup *utilisasi* teknologi informasi dalam pengelolaan sistem akuntansi dan implementasi proteksi sistem informasi untuk *mitigasi* ancaman siber, yang bertujuan memastikan responden memiliki kompetensi dan pengalaman yang relevan dengan *konstruk* penelitian. Determinasi ukuran sampel menggunakan formula *Slovin* dengan margin *of error* 10% untuk memperoleh representasi sampel yang optimal dari populasi dengan parameter yang tidak diketahui secara keseluruhan, sehingga memfasilitasi generalisasi temuan penelitian dengan tingkat akurasi yang memadai.

Teknik Pengumpulan Data

Teknik pengumpulan data adalah prosedur yang digunakan oleh peneliti untuk memperoleh informasi yang relevan dengan tujuan penelitian., pengumpulan data dalam penelitian ilmiah adalah prosedur yang sistematis untuk memperoleh data yang diperlukan (Sugiyono, 2013). Kuesioner adalah instrumen pengumpulan data berupa pertanyaan terstruktur yang diadministrasikan kepada responden, menurut Sugiyono, (2013) efektif digunakan peneliti telah mengidentifikasi variabel yang akan dioperasionalkan. Dalam

penelitian *cybersecurity accounting*, implementasi kuesioner dilakukan melalui prosedur sistematis meliputi konstruksi instrumen yang mengintegrasikan dimensi teknologi informasi akuntansi dan proteksi sistem informasi akuntansi, seleksi responden kompeten dari personel IT, akuntan, auditor internal, dan manajer keuangan, serta distribusi melalui platform digital atau cetak untuk menganalisis pengaruh variabel independen terhadap cybersecurity accounting sebagai dasar optimalisasi strategi keamanan siber organisasi.

Teknik Analisis Data

Analisis Statistik Deskriptif

Metode evaluasi untuk mengukur tingkat kesadaran keamanan informasi, kepatuhan kebijakan, dan efektivitas sistem keamanan akuntansi digital. Berguna untuk mengidentifikasi tren risiko dan mengembangkan strategi pencegahan ancaman siber yang terukur.

Analisis Regresi Linier Berganda

Teknik statistik untuk mengukur kontribusi teknologi informasi akuntansi dan sistem proteksi keamanan terhadap efektivitas cybersecurity accounting. Menggunakan rumus $Y = \alpha + \beta_1X_1 + \beta_2X_2 + e$ untuk menentukan signifikansi hubungan antar variabel.

Uji Asumsi Klasik

Uji Normalitas

Prosedur untuk mengevaluasi distribusi normal residual model regresi menggunakan Kolmogorov-Smirnov. Data normal jika signifikansi > 0,05, tidak normal jika < 0,05.

Uji Multikolinearitas

Pengujian korelasi antar variabel independen dalam model regresi. Tidak terjadi multikolinearitas jika nilai tolerance > 0,10 atau VIF < 10.

Uji Heteroskedastisitas

Evaluasi konsistensi variance residual menggunakan uji Glejser. Tidak ada heteroskedastisitas jika p-value > 0,05, ada heteroskedastisitas jika p-value < 0,05.

Koefisien Determinasi (R^2)

Ukuran proporsi variasi variabel dependen yang dijelaskan oleh variabel independen (nilai 0-1). Nilai mendekati 1 menunjukkan kemampuan prediksi tinggi, mendekati 0 menunjukkan kemampuan prediksi rendah.

Pengujian Hipotesis

Uji t untuk menguji pengaruh variabel independen terhadap dependen dengan tingkat signifikansi 0,05. H_0 ditolak jika signifikansi < 0,05 (ada pengaruh signifikan), H_0 diterima jika signifikansi > 0,05 (tidak ada pengaruh signifikan).

4. HASIL DAN PEMBAHASAN

Analisis Dekriptif

Tabel 5. Hasil Uji Analisis Deskriptif

	N	Range	Minimum	Maximum	Mean	Std. Deviation	Variance
X1. Teknologi	100	59	28	86	57.36	12.600	158.768
X2. Proteksi	100	27	47	74	59.95	5.014	25.137
Y.Cybersecurity	100	27	41	68	55.82	5.875	34.518
Valid N (listwise)	100						

Sumber: Kuesioner, 2025(diolah)

a. Variabel X1 Menunjukkan rentang nilai sebesar 59 dengan nilai minimum 28 dan maksimum 86. Nilai rata-rata sebesar 57,36 dengan standar deviasi 12,600 dan varians 158,768. Variabel ini memiliki tingkat variabilitas yang tertinggi.
b. Variabel X2 Menunjukkan rentang nilai sebesar 27 dengan nilai minimum 47 dan maksimum 74. Nilai rata-rata sebesar 59,95 dengan standar deviasi 5,014 dan varians 25,137. Variabel ini memiliki tingkat variabilitas yang terendah.
c. Variabel Y Memiliki rentang nilai sebesar 27 dengan nilai minimum 41 dan maksimum 68. Nilai rata-rata sebesar 55,82 dengan standar deviasi 5,875 dan varians 34,518. Variabel Y menunjukkan distribusi yang paling homogen dengan tingkat variabilitas lebih rendah dari X2.

Uji Asumsi Klasik

1. Uji Normalitas

Tabel 6. Uji Normalitas

Variabel	Asymp.Sig	Keterangan
Teknologi Informasi Akuntansi	.200	Normal
Proteksi Sistem Informasi Akuntansi	.200	Normal
Cybersecurity Accounting	.146	Normal

Sumber : Kuesioner, 2025(diolah)

Berdasarkan hasil uji normalitas *Kolmogorov-Smirnov* yang disajikan dalam tabel, dapat diketahui bahwa ketiga variabel (X1, X2, dan Y1) memiliki distribusi data yang normal. Hal ini ditunjukkan oleh nilai signifikansi (*Asymp. Sig*. 2-tailed) untuk masing-masing variabel yaitu X1 sebesar 0,200, X2 sebesar 0,200, dan Y sebesar 0,146, dimana ketiga nilai tersebut lebih besar dari tingkat signifikansi α = 0,05. Dengan demikian, hipotesis nol (H0) yang menyatakan bahwa data berdistribusi normal diterima, sehingga asumsi *normalitas* untuk analisis statistik *parametrik* telah terpenuhi. Hasil ini mengindikasikan bahwa data penelitian layak untuk dianalisis menggunakan uji statistik *parametrik* yang mensyaratkan distribusi data normal.

2. Uji Multikolineritas

Tabel 7. Uji Multikolineritas

Model	Tolerance	VIF	Keterangan
Teknologi Informasi Akuntansi	.954	1.048	Tidak ada gejala
Proteksi Sistem Informasi Akuntansi	.954	1.048	Tidak ada gejala

Sumber : Kuesioner,2025(diolah)

1. Variabel Teknologi Informasi Akuntansi memiliki nilai tolerance sebesar 0,954 dimana 0,954 > 0,10 dan nilai VIF sebesar 1,048 dimana 1,048 < 10,00 maka dapat disimpulkan bahwa tidak terjadi gejala multikolineritas dalam model regresi.
2. Variabel Proteksi Sistem Informasi Akuntansi memiliki nilai tolerance sebesar 0,954 dimana 0,954 > 0,10 dan nilai VIF sebesar 1,048 dimana 1,048 < 10,00 maka dapat disimpulkan bahwa tidak terjadi gejala multikolineritas dalam model regresi.

3. Uji Heteroskedasitas

Tabel. 8 Hasil Uji Heteroskedasitas

Model	Sig.	Keterangan
Teknologi Informasi Akuntansi	.052	Tidak terjadi gejala
Proteksi Sistem Informasi Akuntansi	.537	Tidak terjadi gejala

Sumber: Kuesioner, 2025(diolah)

Berdasarkan tabel tersebut didapatkan hasil seperti berikut :

a. Variabel Teknologi Informasi Akuntansi memiliki nilai signifikansi sebesar 0,052 dimana 0,052 > 0,05 dan nilai maka dapat disimpulkan bahwa tidak terjadi gejala heteroskdastisitas dalam model regresi.
b. Variabel Proteksi Sistem Informasi Akuntansi memiliki nilai signifikansi sebesar 0,537 dimana 0,537 > 0,05 dan nilai maka dapat disimpulkan bahwa tidak terjadi gejala heteroskdastisitas dalam model regresi.

Analisis Regresi Linier Berganda

1. UJI F

Tabel 9. Hasil Uji F

Model	F	Sig.
Regression	30.095	.000

Sumber: Kuesioner, 2025(diolah)

Hasil analisis regresi menunjukkan model penelitian signifikan secara statistik dengan nilai F hitung 30.095 ($p < 0,05$), membuktikan bahwa teknologi informasi akuntansi dan proteksi sistem informasi akuntansi secara simultan memberikan pengaruh signifikan terhadap *cybersecurity accounting*. Temuan ini mendukung teori stakeholder yang menggarisbawahi tanggung jawab perusahaan kepada seluruh pihak berkepentingan (Harrison et al., 2015; Freeman & Menghwar, 2024)

Berdasarkan perspektif teori stakeholder, penerapan teknologi informasi akuntansi yang optimal dan perlindungan sistem informasi akuntansi yang komprehensif mencerminkan komitmen perusahaan dalam menjaga kepentingan stakeholder. Kehista et al., (2023) dan Putri & Martha, (2022) menegaskan bahwa proteksi sistem informasi akuntansi merupakan tanggung jawab kolektif yang mengintegrasikan berbagai pihak untuk mengamankan data dari ancaman siber, sehingga menghasilkan nilai tambah yang substansial bagi keseluruhan stakeholder.

2. UJI T

Tabel 10. Hasil Uji T

Model	B	Beta	Sig.
Constanta	56.164		.000
Teknologi Informasi Akuntansi	.251	.539	.000
Proteksi Sistem Informasi Akuntansi	-.246	-.210	.012

Sumber: Kuesioner, 2025(diolah)

Berdasarkan hasil Uji T maka diperoleh persamaan model regresi sebagai berikut :

Cybersecurity Accounting = 56.164 + 0,251(Teknologi) – 0,246(Proteksi)

Hasil uji t menunjukkan bahwa Teknologi Informasi Akuntansi (X1) berpengaruh positif dan signifikan terhadap *Cybersecurity Accounting* (Y) dengan koefisien 0,251 ($p < 0,05$). Temuan ini mengonfirmasi konsep Qur'ani, (2022) bahwa Teknologi Informasi Akuntansi merupakan implementasi sistematis untuk meningkatkan efisiensi dan efektivitas pencapaian akurasi laporan keuangan. Pengaruh positif ini selaras dengan karakteristik sistem informasi akuntansi yang dikemukakan Endaryati et al., (2023), dimana sistem memiliki komponen terintegrasi untuk menghasilkan *output* laporan

optimal. Implementasi teknologi informasi akuntansi yang baik akan meningkatkan kapabilitas *cybersecurity accounting* dalam menghadapi ancaman siber yang kompleks. Hasil penelitian juga konsisten dengan pandangan Janvrin & Wang, (2019) serta Madani et al., (2024) yang menyatakan bahwa teknologi informasi akuntansi yang mencakup sistem *cloud, big* data, dan *ERP* memerlukan integrasi manajemen risiko untuk menghadapi kompleksitas ancaman keamanan. Dengan demikian, semakin baik implementasi teknologi informasi akuntansi, semakin efektif *cybersecurity accounting* dalam memberikan proteksi sistem informasi.

Hasil penelitian menunjukkan bahwa Proteksi Sistem Informasi Akuntansi (X2) berpengaruh negatif dan signifikan terhadap *Cybersecurity Accounting* (Y) dengan koefisien -0,264 ($p < 0,05$). Setiap peningkatan satu-satuan dalam upaya keamanan data justru menurunkan nilai *cybersecurity accounting* sebesar -0,246 poin. Hal ini mengindikasikan adanya kemungkinan proteksi system informasi akuntansi yang belum efektif, tidak tepat sasaran, atau menciptakan efek kontra-produktif terhadap sistem keamanan siber akuntansi secara kesuluruhan. Temuan ini memerlukan interpretasi mendalam dalam konteks teoritis yang ada. Pengaruh negatif ini dapat dijelaskan melalui perspektif bahwa proteksi sistem informasi akuntansi yang berlebihan atau tidak tepat sasaran dapat menghambat efektivitas *cybersecurity accounting*. Vanhorn & Shutterstock, (2021) mengemukakan bahwa proteksi keamanan sistem akuntansi merupakan implementasi sistematis strategi *defensif* untuk mempertahankan kerahasiaan, integritas, dan *availability* data akuntansi. Namun, ketika implementasi proteksi sistem informasi akuntansi terlalu rigid atau tidak selaras dengan kebutuhan *cybersecurity accounting*, hal ini dapat menciptakan hambatan operasional. Kontrol akses yang terlalu ketat dapat menghambat proses monitoring dan analisis yang diperlukan dalam *cybersecurity accounting*, sementara enkripsi data yang berlebihan dapat memperlambat proses deteksi ancaman dan respons insiden.

Koefisien Determinasi

Tabel 11. Hasil Uji Koefisien Determinasi

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.619[a]	.383	.370	4.663

Sumber: Kuesioner, 2025(diolah)

Hasil uji koefisien determinasi menunjukkan nilai R sebesar 0,619 yang mengindikasikan hubungan positif moderat antar variabel. Nilai R Square sebesar 0,383 menjelaskan bahwa

variabel independen mampu menjelaskan 38,3% variasi variabel dependen, sementara 61,7% dijelaskan oleh faktor lain. Dengan Adjusted R Square 0,370 dan Standard Error 4,663 model memiliki kemampuan prediksi moderat namun cukup reliabel untuk analisis hubungan antar variabel.

5. KESIMPULAN DAN SARAN

Kesimpulan

Penelitian ini membuktikan bahwa teknologi informasi akuntansi dan proteksi sistem informasi akuntansi secara bersama-sama berpengaruh signifikan terhadap *cybersecurity accounting* ($F = 30.095$, $p < 0,05$). Secara individual, teknologi informasi akuntansi menunjukkan pengaruh positif signifikan ($\beta = 0,251$, $p < 0,05$), yang berarti semakin baik penerapan teknologi informasi akuntansi, semakin efektif *cybersecurity accounting* dalam organisasi. Sebaliknya, proteksi sistem informasi akuntansi menunjukkan pengaruh negatif yang signifikan terhadap cybersecurity accounting ($\beta = -0,246$, $p < 0,05$). Temuan ini mengindikasikan bahwa tingkat proteksi yang berlebihan atau tidak proporsional justru dapat menjadi penghambat efektivitas implementasi cybersecurity accounting, kemungkinan karena menimbulkan kompleksitas sistem, penurunan fleksibilitas operasional, atau resistensi pengguna terhadap sistem yang terlalu ketat. Hasil ini selaras dengan pandangan dalam Protection Motivation Theory (PMT), di mana respons protektif yang tidak seimbang dengan persepsi ancaman dapat menimbulkan efek maladaptif, seperti penolakan atau penghindaran penggunaan sistem oleh pengguna. Oleh karena itu, proteksi perlu dirancang secara proporsional dan berbasis risiko nyata yang teridentifikasi.

Saran

Organisasi disarankan untuk mengoptimalkan penerapan teknologi informasi akuntansi guna meningkatkan efektivitas cybersecurity accounting. Selain itu, evaluasi berkala terhadap strategi proteksi sistem informasi akuntansi perlu dilakukan untuk memastikan bahwa upaya pengamanan tidak justru menghambat kinerja sistem. Keseimbangan antara tingkat keamanan dan efisiensi operasional menjadi kunci dalam implementasi sistem keamanan siber akuntansi yang efektif.

Keterbatasan penelitian ini terletak pada kemampuan prediktif model yang masih terbatas (38,3%) serta penggunaan desain cross-sectional, yang tidak menangkap perubahan dinamis dari waktu ke waktu. Oleh karena itu, penelitian selanjutnya disarankan untuk mengeksplorasi faktor-faktor lain, seperti kompetensi sumber daya manusia dan budaya

organisasi, serta menggunakan desain longitudinal untuk memahami dinamika hubungan antarvariabel secara lebih mendalam. Selain itu, penelitian komparatif antar industri dapat memberikan wawasan yang lebih luas mengenai efektivitas penerapan cybersecurity accounting dalam berbagai konteks organisasi.

DAFTAR REFERENSI

Aulia Rahma Qur'ani. (2022, July 19). Penerapan teknologi informasi di bidang akuntansi. Serambiupdate.com. https://www.serambiupdate.com/2022/08/penerapan-teknologi-informasi-bidang.html

Bharadwaj, A. S., Sambamurthy, V., Smith, R. H., & Zmud, R. W. (1999). IT capabilities: Theoretical perspectives and empirical operationalization. https://doi.org/10.1145/352925.352962

Cahyono, I., Marsitiningsih, M., & Widodo, S. (2020). Peran Badan Pengawas Obat dan Makanan terhadap peredaran obat tradisional yang mengandung bahan kimia obat berbahaya dalam perlindungan konsumen. Kosmik Hukum, 19(2).

Eko Prasetyo, S., & Mindy, A. (2025). Implementasi multi-factor authentication untuk optimalisasi keamanan akses data. Jurnal Manajemen Informatika (JAMIKA), 15(1). https://doi.org/10.34010/jamika.v15i1.14190

Endaryati, E., Kom, S., & Si, M. (2021). Sistem informasi akuntansi.

Freeman, R. E., & Menghwar, P. S. (2024). Stakeholder theory and communities: Navigating processes of meaningful engagement with marginalized communities. In The Routledge handbook on meaningful stakeholder engagement (pp. 43–55). Taylor and Francis. https://doi.org/10.4324/9781003388227-4

Freeman, R. E., & Verlag, R. H. (2024). The stakeholder approach revisited. www.ssoar.info

Gordon, L. A., Loeb, M. P., & Zhou, L. (2021). Information segmentation and investing in cybersecurity. Journal of Information Security, 12(1), 115–136. https://doi.org/10.4236/jis.2021.121006

Hapsah Fatni, Z., & Nastion Padli Irwan, M. (2023). Analisis tingkat keamanan data perusahaan yang rentan terhadap serangan cyber dalam sistem informasi manajemen. Wanargi. https://doi.org/10.62017/wanargi

Harrison, J. S., Freeman, R. E., & de Abreu, M. C. S. (2015). Stakeholder theory as an ethical approach to effective management: Applying the theory to multiple contexts. Revista Brasileira de Gestão de Negócios, 17(55), 858–869. https://doi.org/10.7819/rbgn.v17i55.2647

Hasan, L., Hossain, M. Z., Johora, F. T., & Hasan, M. H. (2024). Cybersecurity in accounting: Protecting financial data in the digital age. European Journal of Applied Science, Engineering and Technology, 2(6), 64–80. https://doi.org/10.59324/ejaset.2024.2(6).06

Hatta, M., & Rahmah, G. (2024, December 19). Daftar serangan ransomware ke lembaga keuangan Indonesia: BI, BSI, dan terbaru BRI. Tempo. https://www.tempo.co/sains/daftar-serangan-ransomware-ke-lembaga-keuangan-indonesia-bi-bsi-dan-terbaru-bri-1183490

Husna, H., Nasution, A. K., Afriliani, I., & Fitriana, N. (2024). Manajemen risiko keamanan sistem informasi akuntansi pada perusahaan otomotif PT. Astra Internasional. Jurnal Akuntansi Keuangan dan Bisnis, 2(2), 296–299. https://jurnal.ittc.web.id/index.php/jakbs/index

Janvrin, D. J., & Wang, T. (2019). Implications of cybersecurity on accounting information. Journal of Information Systems, 33(3), A1–A2. https://doi.org/10.2308/isys-10715

Kafi, A., & Akter, N. (2017). Securing financial information in the digital realm: Case studies in cybersecurity for accounting data protection.

Kania Sutisnawinata. (2023, July 12). Keamanan siber dalam industri akuntansi. ASDF.ID. https://www.asdf.id/keamanan-siber-dalam-akuntansi/?utm_source=chatgpt.com

Lehenchuk, S. F., Vygivska, I. M., & Hryhorevska, O. O. (2022). Protection of accounting information in the conditions of cyber security. Problems of Theory and Methodology of Accounting, Control and Analysis, 2(52), 40–46. https://doi.org/10.26642/pbo-2022-2(52)-40-46

Lindemulder, G., & Kosinski, M. (2024, July 12). Apa itu keamanan siber? IBM. https://www.ibm.com/id-id/topics/cybersecurity

Madani, L., Sofia, A., Widarsono, A., Akuntansi, J. P., & Keuangan, D. (2024). The influence of cybersecurity disclosure, tax risk, reputation and auditor experience on audit quality. JPAK: Jurnal Pendidikan Akuntansi dan Keuangan, 12(2), 138–149. https://doi.org/10.17509/jpak.v12i2.64236

Morshed, A., & Khrais, L. T. (2025). Cybersecurity in digital accounting systems: Challenges and solutions in the Arab Gulf region. Journal of Risk and Financial Management, 18(1). https://doi.org/10.3390/jrfm18010041

Nurwanah, A. (2024). Cybersecurity in accounting information systems: Challenges and solutions. Advances in Applied Accounting Research, 2(3), 157–168. https://doi.org/10.60079/aaar.v2i3.336

Poeja Kehista, A., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Analisis keamanan data pribadi pada pengguna e-commerce: Ancaman, risiko, strategi kemanan (literature review). Jurnal Ilmiah Mahasiswa Teknik (JIMT), 4(5). https://doi.org/10.31933/jimt.v4i5

Putri, E. P., & Elmina Martha, A. (2022). The importance of enacting Indonesian data protection law as a legal responsibility for data leakage. Varia Justicia, 17(3), 287–303. https://doi.org/10.31603/variajusticia.v17i3.6231

Salim, H., & Madnick, S. (2016). Cyber safety: A systems theory approach to managing cyber security risks – Applied to TJX cyber attack.

Saputra, L. A., Akbar, F. M., Cahyaningtias, F., Ningrum, M. P., & Fauzi, A. (2023). Ancaman keamanan pada sistem informasi manajemen perusahaan. Jurnal Pendidikan Siber Nusantara. https://doi.org/10.38035/jpsn.v1i12

Siponen, M., Rönkkö, M., L., F., Haag, S., & Laatikainen, G. (2023). Protection motivation theory in information security behavior research: Reconsidering the fundamentals research (Vol. 53). http://aisel.aisnet.org/cais/

Sugiyono. (2013). Metode penelitian kuantitatif.

Vanhorn, S. (2021). Accounting information systems. FuzzBones/Shutterstock.

Yosepha Debrina Ratih Pusparisa. (2024, December 19). Tak pernah transparan, serangan ke sektor perbankan terus berulang. Kompas.id. https://www.kompas.id/artikel/lagi-dugaan-serangan-siber-terhadap-sektor-perbankan