INTERAKSI ANTARA PRIVASI, KEAMANAN INFORMASI, DAN AKUNTABILITAS DALAM SISTEM INFORMASI AKUNTANSI: SYSTEMATIC LITERATURE REVIEW

Fajriyah Auliyah Anugrah[1], Dewi Dellviani[2], Joice Simanjuntak[3], Irwansyah[4]

[1,2,3,4]*Universitas Mulawarman*
E-mail : jhiahauliyah@gmail.com[1], dewi.dellvi@gmail.com[2], joicesimanjuntak16@gmail.com[3], irwansyah@feb.unmul.ac.id[4]

ABSTRAK

Penelitian ini bertujuan untuk menganalisis interaksi antara privasi, keamanan informasi, dan akuntabilitas dalam Sistem Informasi Akuntansi melalui pendekatan Systematic Literature Review (SLR). Literatur diperoleh dari Google Scholar, Scopus, ScienceDirect, dan Emerald Insight dengan proses seleksi yang mengacu pada kerangka PRISMA. Sebanyak 18 artikel periode 2021-2026 digunakan sebagai korpus utama dan dianalisis melalui proses ekstraksi data serta coding terhadap delapan tema, yaitu *privacy*, *information security/cybersecurity*, *accountability*, *internal control*, *audit/assurance*, *governance*, *transparency/disclosure*, dan *accounting/financial reporting quality*. Hasil penelitian menunjukkan bahwa *information security/cybersecurity* merupakan tema paling dominan, sedangkan *privacy* relatif lebih terbatas dan terutama berkaitan dengan perlindungan data, *information sharing*, serta penggunaan *artificial intelligence*. *Internal control* berperan sebagai mekanisme penghubung antara keamanan informasi dan kualitas informasi akuntansi, sedangkan audit dan *governance* berfungsi membentuk assurance, pengawasan, serta pembagian tanggung jawab yang mendukung *accountability*. Penelitian juga menemukan adanya ketegangan antara kebutuhan perlindungan informasi dan tuntutan *transparency* serta *disclosure* kepada *stakeholder*. Secara keseluruhan, interaksi *privacy*, *information security*, dan *accountability* tidak bersifat linear, tetapi berlangsung melalui *internal control*, audit, dan *governance* sebagai mekanisme penyeimbang. Temuan ini menghasilkan model sintesis konseptual yang menempatkan kualitas informasi akuntansi sebagai keluaran dari perlindungan, pengendalian, pengawasan, dan pertanggungjawaban informasi yang terintegrasi.

Kata Kunci : *Privasi; Keamanan Informasi; Cybersecurity; Akuntabilitas; Sistem Informasi Akuntansi; Pengendalian Internal; Tata Kelola; Systematic Literature Review*.

ABSTRACT

This study aims to analyze the interaction between privacy, information security, and accountability in Accounting Information Systems using a Systematic Literature Review (SLR) approach. The literature was collected from Google Scholar, Scopus, ScienceDirect, and Emerald Insight, with the selection process referring to the PRISMA framework. A total of 18 articles published between 2021 and 2026 were included in the main corpus and analyzed through data extraction and coding across eight themes: privacy, information security/cybersecurity, accountability, internal control, audit/assurance, governance, transparency/disclosure, and accounting/financial reporting quality. The findings show that information security/cybersecurity is the most dominant theme, while privacy receives relatively limited attention and is mainly associated with data protection, information sharing, and the use of artificial intelligence. Internal control serves as a bridging mechanism between information security and accounting information quality, whereas audit and governance support assurance, oversight, and the allocation of responsibilities that strengthen accountability. The review also identifies a tension between the need to protect information and the demand for transparency and disclosure to stakeholders. Overall, the interaction among privacy, information security, and accountability is not linear, but is mediated through internal control, audit, and governance as balancing mechanisms. The study proposes a conceptual synthesis model in which accounting information quality is viewed as an outcome of integrated information protection, control, oversight, and accountability.

Keywords : *Privacy; Information Security; Cybersecurity; Accountability; Accounting Information Systems; Internal Control; Governance; Systematic Literature Review.*

PENDAHULUAN

Digitalisasi telah mengubah cara organisasi mencatat, memproses, dan melaporkan informasi keuangan. Sistem informasi akuntansi (SIA) telah berkembang menjadi sistem akuntansi berbasis komputer yang semakin memanfaatkan teknologi seperti *blockchain* (Nhan et al., 2023). Aisyah dan Tjandrakirana DP (2025) menyatakan bahwa SIA berbasis cloud meningkatkan akurasi, deteksi kecurangan, dan pelaporan waktu nyata. Manfaat serupa juga dirasakan oleh perusahaan, ketika SIA meningkatkan kinerja perusahaan sekaligus memperbaiki pengendalian internal, akses informasi keuangan, transparansi, dan akuntabilitas (Wahyuni, 2023).

SIA mengumpulkan dan menyimpan data tentang aktivitas organisasi, mengubahnya menjadi informasi untuk pengambilan keputusan, serta menyediakan pengendalian yang memadai untuk mengamankan aset dan data (Romney & Steinbart, 2018). Data yang dikelola mencakup data transaksi, data keuangan, data pelanggan, dan data organisasi lainnya. Karena nilai data tersebut, perlindungannya menjadi isu sentral. Hasan et al. (2024) menyatakan bahwa keamanan siber dalam akuntansi esensial untuk melindungi data keuangan di era digital, sedangkan Cram et al. (2023) menempatkan isu keamanan siber sebagai bagian fundamental dari penelitian SIA.

Namun, digitalisasi juga memperluas risiko berupa kebocoran data, serangan siber, penyalahgunaan informasi, dan pelanggaran privasi. Kelemahan pengendalian internal teknologi informasi dapat menyebabkan misrepresentasi informasi keuangan, dan analisis atas laporan opini kontrol internal (Mojtahedi & Zhou, 2024).

Keamanan informasi diperlukan untuk melindungi data, tetapi perlindungan data tidak berhenti pada aspek teknis. Perlindungan data pribadi diatur oleh regulasi yang menempatkan akuntabilitas sebagai prinsip, sebagaimana *General Data Protection Regulation* (GDPR) yang mewajibkan pengendali data bertanggung jawab atas kepatuhan terhadap prinsip pemrosesan data dan mampu menunjukkannya (European Union, 2016).

Bukti empiris mendukung keterkaitan ketiga aspek tersebut. Shafa dan Islam (2025) menemukan bahwa privasi data dan keamanan siber sama-sama berpengaruh positif terhadap transparansi keuangan, dengan interaksi keduanya bersifat saling melengkapi, sedangkan kekuatan pengendalian SIA memediasi sebagian hubungan tersebut. Temuan ini mengisyaratkan bahwa privasi, keamanan informasi, dan akuntabilitas pelaporan perlu dipandang sebagai satu rangkaian tata kelola, bukan isu yang berdiri sendiri.

Meskipun demikian, penelitian terdahulu cenderung membahas aspek-aspek tersebut secara terpisah. Cram et al. (2023) meninjau 56 artikel di 11 jurnal berorientasi SIA dan mengelompokkannya ke dalam risiko dan ancaman, kontrol, asurans, serta pelanggaran siber. Amani et al. (2025) memfokuskan tinjauan pada pengungkapan risiko dan insiden siber, dan Winarto (2026) menelaah peningkatan keamanan siber melalui sistem akuntansi manajemen dengan analisis bibliometrik. Dari sisi pengendalian dan tata kelola, Mojtahedi dan Zhou (2024) menganalisis kelemahan material kontrol internal teknologi informasi, sedangkan Wu et al. (2024) mengkaji tata kelola dan pengendalian teknologi informasi dari perspektif audit internal.

Dengan demikian, terdapat celah penelitian berupa belum banyaknya telaah yang secara sistematis mengintegrasikan privasi, keamanan informasi, dan akuntabilitas dalam konteks SIA. Cram et al. (2023) sendiri menyoroti bahwa kekhasan dan kontribusi riset keamanan siber berbasis SIA relatif belum jelas dibandingkan disiplin ilmu lain. Studi yang menghubungkan privasi dan keamanan siber dengan hasil pelaporan, seperti Shafa dan Islam (2025), berupa studi empiris kuantitatif dengan ulasan literatur pendukung, bukan pemetaan sistematis atas penelitian SIA.

Berdasarkan penelusuran literatur yang dilakukan penulis, tinjauan sistematis yang secara eksplisit memetakan interaksi ketiga aspek tersebut dalam SIA belum ditemukan.

Penelitian ini bertujuan memetakan bagaimana privasi, keamanan informasi, dan akuntabilitas dibahas dalam penelitian SIA pada periode 2021–2026 melalui *systematic literature review*. Secara khusus, penelitian ini mengidentifikasi tema dan konteks yang dominan, menelaah keterkaitan antar ketiga aspek, serta merumuskan celah dan agenda penelitian mendatang. Proses telaah mengikuti pedoman pelaporan PRISMA 2020 (Page et al., 2021).

METODE

Penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) untuk mengidentifikasi, mengevaluasi, dan mensintesis hasil penelitian terdahulu mengenai interkasi antara privasi, keamanan informasi, dan akuntabilitas dalam pengelolaan informasi akuntansi. Pendekatan SLR dipilih karena penelitian ini menggunakan analisis dan mengintegrasikan temuan dari berbagai penelitian yang telah dipublikasikan, dimana fokus utama penelitian diarahkan pada bagaimana privasi, keamanan informasi, dan akuntabilitas dipahami dalam konteks informasi akuntansi, serta bagaimana ketiga konsep tersebut saling berhubungan. Analisis tidak hanya dilakukan dengan merangkum hasil penelitian terdahulu, tetapi juga dengan mengidentifikasi pola hubungan, kesamaan, perbedaan, serta kesenjangan penelitian yang masih ditemukan dalam literatur.

Pencarian literatur dilakukan secara sistematis untuk mengidentifikasi penelitian yang membahas privasi, keamanan informasi, dan akuntabilitas dalam konteks informasi akuntansi. Hal ini didasarkan pada pentingnya isu etika,privasi, dan keamanan dalam penelitian mengenai sistem informasi akuntansi (Guragai et al., 2017a) . Proses pencarian dirancang dengan mempertimbngkan keterkaitan antara konsep utama penelitian, yaitu *information Privacy*, *information security*, *accountability*, dan *accounting informastion system*. Strategi pencarian tersebut digunakan untuk memperolah literatur yang membahas keamanan informasi dalam konteks sistem informasi akuntansi, termasuk risiko, ancaman, pengendalian, assurance, dan kebocoran data (Cram et al., 2023a).

Literatur diperolah melalui beberapa basis data ilmiah, yaitu Google Scholar, Scopus, ScienceDirect, dan Emerld Insight. Pemilihan sumber tersebut dilakukan ntuk memperolah literatur internasioanl maupun nasional yang relevan dibidang akuntansi, sistem informasi akuntansi, keamanan informasi, dan tata kelola informasi. Pencarian dilaukan menggunakan kombinasi kata kunci operator Boolan *AND* dan *OR*, seperti "*information Privacy*" *AND* "*accounting information*", "*information security*" *AND* "*accounting information*", "*accountability*" *AND* "*acconting information*", serta "*Privacy*" *AND* "*security*" *AND* "*accountability*" *AND* "*accounting information systems*" (Page et al., 2021) .

Teknik Analisis Data

Pencarian juga difokuskan pada artikel ilmiah yang dipublikasikan dalam periode 2020-2026 untuk menangkap perkembangan penelitain yang relatif mutakhir mengenai pengelolaan informasi akuntansi dalam lingkungan digital. Meskipun demikian, beberpa sumber diterbitkan sebelum periode tersebut tetap dapat digunakan sebagai literatur pendukung apabila memiliki kontribusi konseptual yang penting terhadap pemahaman mengenai privasi, keamanan informasi, sistem informasi akuntansi, atau akuntabilitas. Setiap hasil pencarian kemudian didokumentasikan berdasarkan sumber data, kata kunci yang digunakan, tahun publikasi, dan jumlah. Selanjutnya,

artikel diperiksa untuk menghapus artikel yang sama atau duplikat. Setelah itu, artikel diseleksi berdasarkan judul dan abstraknya untuk melihat kesesuainnya dengan topik penelitian. Proses pencaciran dan pemilihan artikel dilakukan menggunakan kerangka PRISMA (Page et al., 2021) agar setiap tahapan dapat dijelaskan dengan jelas, mulai dari pencarian artikel sampai penentuan artikel yang digunakan dalam penelitian.

Strategi pencarian tersebut disusun untuk menangkap dua kelompok literatur. Kelompok pertama mencakup penelitian yang membhasa hubungan antara privasi dan keamanan informasi dalam pengelolaan data atau sistem informasi akuntansi. Kelompok kedua mencakup penelitian yang menghubungkan perlindungan dan keamanan informasi dengan akuntabilitas, transparansi, pengendalian, serta pertanggungjawaban organisasi. Pembagian tersebut memungkinkan penelitian ini tidak hanya mengidentifikasi penelitian yang membahas ketiga konsep secara bersamaan, tetapi juga mensintesis keterkaitan ketiganya berdasakan temuan dari penelitian yang membahas hubungan antarkonsep secara parsial.

HASIL PENELITIAN DAN PEMBAHASAN

Hasil Identifikasi dan Ekstraksi Literatur

Berdasarkan proses seleksi literatur atau screening yang kemudian dilakukan ekstraksi data yang kurang relevan, sehingga muncul 18 artikel sebagai korpus utama analisis. Artikel yang dianalisis diterbitkan pada periode 2021–2026 dan memiliki keterkaitan dengan privasi, keamanan informasi atau *cybersecurity*, akuntabilitas, pengendalian internal, audit, tata kelola, transparansi, serta kualitas informasi akuntansi dan pelaporan keuangan.

Karakteristik artikel yang dianalisis menunjukkan keberagaman objek dan metode penelitian. Penelitian menggunakan survei, wawancara, *case study*, eksperimen, pengembangan kerangka, serta analisis data arsip. Keragaman tersebut menunjukkan bahwa hubungan antara keamanan informasi dan informasi akuntansi telah diteliti dari perspektif teknis, pengendalian, audit, tata kelola, pelaporan, maupun konsekuensi terhadap pengguna informasi.

Tabel 1. Karakteristik Artikel yang Dianalisis

No.	Penulis	Tahun	Fokus/Objek Penelitian	Metode/Data
1	Kogan & Yin	2021	*Privacy*-preserving information sharing dalam firma audit	Eksperimen/modeling
2	Slapničar et al.	2022	Efektivitas cybersecurity audit	Survei auditor/CAE
3	Blakely, Kurtenbach & Nowak	2022	Laporan cyber breach dan internal control	Review/taxonomy
4	Mahdi	2022	IT governance dan keamanan AIS	Case study/survei
5	Zhang et al.	2023	AI dalam managerial accounting dan isu etika	47 wawancara
6	Slapničar et al.	2023	Five lines of accountability dalam	24 wawancara

			cybersecurity governance	
7	Tadesse, Walton & Zhang	2026	COSO dan cybersecurity breaches	Data arsip/empiris
8	Rezaee, Zhou & Bu	2024	Corporate social irresponsibility dan data breaches	24.456 observasi
9	Calvin, Eulerich & Holt	2025	Internal audit dan cybersecurity assurance	Survei, 1.142 responden
10	Garg, Wang & Wilkin	2025	Security breach, accounting quality dan disclosure	Data arsip/empiris
11	Akin et al.	2026	AI-driven accounting, *Privacy* dan ethics	Mixed methods
12	Kim et al.	2025	Segregation of duties dalam accounting systems	Framework/design
13	Mojtahedi & Zhou	2024	IT internal control weaknesses dan financial reporting	Data arsip + analisis tematik/statistik
14	Liu	2025	Financial statement audit dan data breaches	Data arsip/empiris
15	Jiang, Xu & Counts	(Jiang et al., 2024)	XBRL reporting dan data breach	Data arsip/empiris
16	Seaton Kelton & Yang	2024	Cyber breach contagion dan internal controls	Data arsip/empiris
17	Vo & Pham	2025	Cybersecurity risk dan strategic voluntary disclosure	Data arsip/empiris
18	Chen, Goh, Lee & Li	2026	Cybersecurity breaches dan analyst earnings forecasts	Data arsip/empiris

Berdasarkan karakeristik tersebut, dapat dilihat bahwa sebagaian besar penelitian berorientasi pada keamanan informasi dan *cybersecurtiy*. Beberapa penelitian secara langsung membahas privasi, sementara akuntabilitas lebih banyak dikaji melalui *governance*, *audit*, *responsibility*, *internal control*, dan *disclosure*. *Data extraction* dilakukan dengan mengidentifikasi fokus penelitian, metode, konteks penelitian, serta keterkaitan artikel dengan delapan tema yang menjadi dasar analisis, yaitu *Privacy* (P), *Information Security*/*Cybersecurity* (S), *Accountability* (A), *Internal Control* (IC), *Audit/Assurance* (AU), *Governance* (G), *Transparency/Disclosure* (T), dan *Information/Financial Reporting Quality* (Q).

Tabel 2. Data Extraction dan Hasil Analisis Literature

No	Artikel	Fokus Utama	Temuan Utama	Hubungan/Mekanisme
1	Kogan & Yin (2021)	*Privacy*-preserving information sharing	Informasi perusahaan dapat dibagikan dalam firma audit dengan tetap menjaga kerahasiaan klien serta meningkatkan akurasi estimasi dan deteksi kesalahan.	*Privacy* → secure information sharing → audit/information quality
2	Slapničar et al. (2022)	Cybersecurity audit	Efektivitas cybersecurity audit berkaitan dengan kematangan cybersecurity risk management.	Audit → cybersecurity risk management → governance/accountability
3	Blakely et al. (2022)	Cyber breach reporting	Laporan breach mengandung informasi yang terbatas untuk memperbaiki profil risiko organisasi.	Breach reporting → risk assessment → internal control
4	Mahdi (2022)	IT governance dan AIS	IT governance mendukung reliabilitas AIS, pengendalian, audit, dan keamanan informasi.	IT governance → internal control/AIS security → information reliability
5	Zhang et al. (2023)	AI dan managerial accounting	*Privacy*, data security, misuse, accountability, transparency, dan trust merupakan isu etika utama dalam AI accounting.	*Privacy* + security → governance → accountability/transparency
6	Slapničar et al. (2023)	Cybersecurity governance	Akuntabilitas cybersecurity didistribusikan melalui fungsi kontrol, CISO, internal audit, manajemen dan board.	Cybersecurity → governance → accountability
7	Tadesse et al. (2026)	COSO dan cybersecurity	Adopsi COSO berkaitan dengan risiko breach yang lebih rendah dan membantu identifikasi IT material weaknesses.	Internal control/COSO → cybersecurity risk reduction
8	Rezaee et al. (2024)	Responsibility dan data breach	Corporate social irresponsibility	Responsibility/governance → data security → accountability

			berkaitan positif dengan data breach.	
9	Calvin et al. (2025)	Internal audit dan cybersecurity assurance	Kematangan internal audit dan pengetahuan TI berkaitan dengan keterlibatan internal audit dalam cybersecurity assurance.	Internal audit → cybersecurity assurance → governance
10	Garg et al. (2025)	Security breach, accounting quality dan disclosure	Security breach berkaitan dengan strategi disclosure dan konsekuensi terhadap kualitas pelaporan serta pasar.	Security breach → disclosure/transparency → information consequences
11	Akin et al. (2026)	AI accounting, *Privacy* dan accountability	AI menimbulkan persoalan data sensitif, opacity, algorithmic bias, *Privacy* dan accountability.	*Privacy*/security → organizational governance → accountability
12	Kim et al. (2025)	Segregation of duties	Pemisahan fungsi membantu mengendalikan akses dan konflik tugas dalam accounting systems.	Access control/SoD → internal control → accountability
13	Mojtahedi & Zhou (2024)	IT internal control weaknesses	Kelemahan kontrol TI dapat berkaitan dengan risiko terhadap representasi informasi keuangan.	IT control → financial reporting quality
14	Liu (2024)	Financial audit dan data breach	Audit sistem informasi yang material terhadap financial reporting memiliki implikasi terhadap risiko keamanan dan breach.	Audit/internal control → information security → reporting quality
15	Jiang et al. (2024)	XBRL dan data breach	Data breach berkaitan dengan perubahan kompleksitas pelaporan XBRL dan respons pelaporan perusahaan.	Security breach → reporting behavior → transparency/information quality
16	Seaton Kelton & Yang (2024)	Cyber breach contagion	Kualitas internal control dapat mengurangi dampak contagion dari	Cybersecurity → internal control → risk mitigation

			cyber breach terhadap perusahaan lain.	
17	Vo & Pham (2025)	Cybersecurity risk dan voluntary disclosure	Risiko cybersecurity meningkatkan kebutuhan informasi, tetapi disclosure dapat bersifat strategis dan kurang informatif.	Cyber risk → information demand → disclosure/accountability tension
18	Chen et al. (2026)	Cyber breach dan analyst forecasts	Breach membuat forecast analis kurang akurat dan lebih tersebar.	Cyber breach → information environment → reporting quality

Hasil extraction memperlihatkan bahwa hubungan antara keamanan informasi dan informasi akuntansi paling sering dibangun melalui mekanisme pengendalian, audit, governance, dan disclosure. Sementara itu, *Privacy* lebih banyak muncul dalam konteks perlindungan data, *information sharing*, dan penggunaan AI.

Hasil Coding Literatur

Untuk memudahkan mengidentifikasi pola konseptual dalam literatur, setiap artikel diberi kode berdasarkan delapan tema dan angka. *Coding* dilakukan secara kategorikal berdasarkan keterdapatan dan relevansi tema dalam setiap artikel. Kode 1 menunjukkan bahwa tema dibahas secara eksplisit, sedangkan kode 0 menunjukkan bahwa tema tidak dibahas secara eksplisit. Hubungan yang bersifat tidak langsung dicatat pada kolom mekanisme atau temuan penelitian. Kategori dan aturan coding dikembangkan oleh peneliti berdasarkan sintesis literatur dan diterapkan secara konsisten pada seluruh artikel.

Tabel 3. Hasil Coding Literatur

No.	Artikel	P	S	A	IC	AU	G	T	Q	Catatan/Mekanisme
1	Kogan & Yin (2021)	1	1	0	1	1	0	1	1	*Privacy* digunakan untuk menjaga kerahasiaan dalam information sharing; audit menjadi mekanisme assurance dan information quality.
2	Slapničar et al. (2022)	0	1	1	1	1	1	1	0	Cybersecurity audit mendukung risk management; hasil audit berkaitan dengan governance dan accountability.
3	Blakely et al. (2022)	0	1	1	1	1	1	1	1	Cyber breach reporting berkaitan dengan risk assessment dan internal control; disclosure menjadi sumber informasi risiko.
4	Mahdi (2022)	0	1	1	1	1	1	0	1	IT governance mendukung keamananAIS, internal control, adit, dan reliabilits informasi.
5	Zhang et al. (2023)	1	1	1	1	0	1	1	1	*Privacy*, data securit, accountability, transprencydan trust munul sebagai isu etika dalm AI accounting.
6	Slapničar et al. (2023)	0	1	1	1	1	1	1	0	Accountabilitycybersecurity didistribuskan melalui fungsi kontrol,

										CISO, internal audit, manajemen, dan board.
7	Tadesse et al. (2026)	0	1	1	1	1	1	0	1	Adopsi COSO dan internal control berkaitan dengan pengurangan risiko cybersecurity dan identifikasi IT material weaknesses.
8	Rezaee et al. (2024)	1	1	1	1	0	1	1	1	Corporate social responsibility/responsibility berkaitan dengan data breach dan governance organisasi.
9	Calvin et al. (2025)	0	1	1	1	1	1	1	0	Internal audit dan pengetahuan TI meningkatkan keterlibatan audit dalam cybersecurity assurance dan governance.
10	Garg et al. (2025)	0	1	1	1	1	1	1	1	Security breach berkaitan dengan disclosure, accounting quality, dan konsekuensi terhadap pasar.
11	Akin et al. (2026)	1	1	1	1	1	1	1	1	AI accounting menimbulkan isu *Privacy*, data security,accountability, transparency, dan kualitas informasi.
12	Kim et al. (2025)	1	1	1	1	1	1	0	1	Segregation of duties mengendalikan akses dan konflik tugas dalam accounting systems serta mendukung accountability.
13	Mojtahedi & Zhou (2024)	0	1	1	1	1	1	0	1	IT internal control weaknesses berhubungan dengan risiko terhadap financial reporting dan kualitas informasi.
14	Liu (2024)	0	1	1	1	1	1	1	1	Financial statement audit dan internal controls berkaitan dengan sistem informasi yangmaterial terhadap financial reporting dan risiko breach.
15	Jiang et al. (2024)	0	1	1	1	0	1	1	1	Data breach berkaitan dengan perubahan XBRL reporting dan respons disclosure perusahaan.
16	Seaton Kelton & Yang (2024)	0	1	1	1	0	1	0	1	Kualitas internal control memitigasi dampak contagion dari cybersecurity breach.
17	Vo & Pham (2025)	0	1	1	0	0	1	1	1	Cybersecurity risk meningkatkan kebutuhan informasi dan mendorongstrategic voluntaryisclosure.
18	Chen et al. (2026)	0	1	1	1	1	1	1	1	Cyber breach memengaruhi akurasi dan dispersi analyst forecasts; internal

	information environment memengaruhi dampaknya.

Keterangan:

P = *Privacy*;
S = *Information Security/Cybersecurity*;
A = *Accountability*;
IC = *Internal Control*;
AU = *Audit/Assurance*;
G = *Governance*;
T = *Transparency/Disclosure*;
Q = *Accounting/Financial Reporting Quality*.

Coding tersebut menunjukkan pola yang cukup jelas. *Information security/cybersecurity* menjadi tema yang paling dominan, sedangkan *Privacy* merupakan tema yang paling terbatas. Accountability muncul cukup luas, tetapi sering kali melalui *governance*, *responsibility*, *audit*, atau *disclosure*.

Tabel 4. Rekapitulasi Pola Coding

Tema	Hasil Analisis	Peran dalam Model
Privacy	Relatif terbatas; muncul terutama dalam information sharing, AI, dan perlindungan data sensitif.	Perlindungan dan pembatasan akses informasi
Information Security	Tema paling dominan dalam literatur.	Perlindungan informasi dan pengelolaan cyber risk
Accountability	Banyak muncul melalui governance, responsibility, audit, dan disclosure.	Pertanggungjawaban atas pengelolaan informasi dan risiko
Internal Control	Sering menjadi penghubung antara security dan kualitas informasi.	Mengendalikan akses, proses dan risiko
Audit/Assurance	Kuat dalam cybersecurity audit dan assurance.	Monitoring dan assurance
Governance	Sering dikaitkan dengan cybersecurity dan accountability.	Struktur tanggung jawab dan pengawasan
Transparency/Disclosure	Menonjol dalam penelitian mengenai breach dan reporting.	Penyediaan informasi kepada stakeholder
Information Quality	Muncul sebagai konsekuensi security, control, audit dan disclosure.	Reliabilitas dan decision usefulness informasi

Sintesis Tematik

Berdasarkan hasil extraction dan coding, ditemukan lima tema utama yang menjelaskan hubungan antarvariabel dalam literatur.

1. Information Security sebagai Tema Sentral

   Tema pertama adalah dominasi *information security* dan *cybersecurity*. Hampir seluruh artikel berkaitan dengan *cybersecurity risk*, *data breach*, *cybersecurity audit*, keamanan AIS, dan dampak *breach* terhadap informasi. Hal ini menunjukkan bahwa keamanan informasi menjadi

isu penting dalam penelitian akuntansi dan AIS, tidak hanya sebagai persoalan teknologi, tetapi juga sebagai bagian dari pengelolaan risiko dan kualitas informasi.

2. Privacy sebagai Perlindungan Informasi
   Tema kedua adalah *privacy*, yang ditemukan dalam penelitian lebih terbatas dibandingkan *cybersecurity*. *Privacy* berkaitan dengan kerahasiaan data klien, penggunaan data dalam AI, dan pembatasan akses informasi. Kogan & Yin (2021) menunjukkan bahwa informasi dapat dibagikan untuk meningkatkan kualitas audit tanpa menghilangkan kerahasiaan, sehingga *privacy* menekankan bahwa *sharing* harus dilakukan berdasarkan otorisasi dan mekanisme perlindungan yang tepat.
3. Internal Control sebagai Mekanisme Penghubung
   Tema ketiga adalah *internal control*, yang sering muncul sebagai penghubung antara *cybersecurity* dan kualitas informasi. COSO, *IT controls*, *segregation of duties*, dan pengendalian akses berperan dalam mengurangi risiko keamanan serta menjaga kualitas informasi. Dengan demikian, *internal control* menerjemahkan kebijakan keamanan menjadi prosedur operasional dengan hubungan: Information Security → Internal Control → Accounting Information Quality.
4. Audit dan Governance sebagai Mekanisme Akuntabilitas
   Tema keempat adalah audit dan *governance*. Audit memberikan *assurance* atas efektivitas pengendalian dan pengelolaan risiko *cybersecurity*, sedangkan *governance* menentukan pihak yang bertanggung jawab dan mekanisme pengawasannya. Slapničar et al. (2022) menunjukkan bahwa *cybersecurity accountability* melibatkan beberapa lapisan organisasi hingga *board*. Hubungannya dapat dirumuskan: Information Security → Internal Control → Audit/Assurance → Governance → Accountability
5. Transparency dan Disclosure sebagai Dimensi Eksternal
   Tema kelima adalah *transparency* dan *disclosure*, terutama ketika terjadi *security breach*. Informasi mengenai *breach* dapat memengaruhi kebutuhan informasi investor, *analyst forecast*, XBRL reporting, dan respons pasar.

Temuan ini menunjukkan bahwa keamanan informasi berpengaruh terhadap kualitas lingkungan informasi, sehingga organisasi tidak hanya perlu melindungi informasi dari akses tidak sah, tetapi juga menentukan informasi yang perlu diungkapkan kepada *stakeholder*.

Hubungan Antartema dan Mekanisme yang Ditemukan

Hasil *coding* memperlihatkan bahwa hubungan antar konsep dapat dikelompokkan ke dalam beberapa mekansime utama.

Tabel 5. Sintesis Hubungan Antartema dan Mekanisme yang Ditemukan

Hubungan	Mekanisme	Artikel Pendukung
Privacy → Information Sharing	Perlindungan kerahasiaan memungkinkan sharing informasi secara terkendali.	Kogan & Yin (2021)
Information Security → Internal Control	Security membutuhkan kontrol akses, monitoring dan risk management.	Blakely et al. (2022); Tadesse et al. (2026); Kim et al. (2025)
Internal Control → Information Quality	Kontrol TI dan internal control mendukung reliabilitas informasi keuangan.	Mojtahedi & Zhou (2024); Liu (2024)

Information Security → Audit	Cybersecurity menjadi objek audit dan assurance.	Slapničar et al. (2022); Calvin et al. (2025)
Audit → Governance	Assurance mendukung monitoring dan pengawasan risiko.	Slapničar et al. (2022, 2023); Calvin et al. (2025)
Governance → Accountability	Struktur governance mendistribusikan tanggung jawab.	Slapničar et al. (2023); Rezaee et al. (2024)
Security Breach → Disclosure	Insiden keamanan meningkatkan kebutuhan dan strategi disclosure.	Garg et al. (2025); Vo & Pham (2025)
Security Breach → Information Quality	Breach dapat menurunkan kualitas lingkungan informasi dan forecast.	Jiang et al. (2024); Chen et al. (2026)
Internal Control → Risk Mitigation	Kualitas control dapat mengurangi dampak cybersecurity risk/breach.	Tadesse et al. (2026); Seaton Kelton & Yang (2024)

Tabel tersebut menunjukkan bahwa ketiga konsep utama—*Privacy*, *information security*, dan *accountability*—tidak selalu berhubungan secara langsung. Hubungan tersebut lebih sering dibangun melalui mekanisme *internal control*, *audit*, dan *governance*.

Sintesis Interaksi *Privacy*, Information Security, dan Accountability

Berdasarkan keseluruhan hasil *extraction* dan *coding*, penelitian ini mengidentifikasi suatu pola konseptual mengenai interaksi *Privacy*, *information security*, dan *accountability* dalam informasi akuntansi. *Privacy* berfungsi sebagai prinsip yang mengatur perlindungan dan penggunaan informasi. Information security menyediakan mekanisme untuk melindungi informasi dari akses tidak sah, kehilangan, manipulasi, dan ancaman lainnya. Selanjutnya, internal control menerjemahkan kebutuhan perlindungan tersebut ke dalam prosedur dan mekanisme operasional. *Audit* dan *assurance* kemudian memberikan evaluasi terhadap efektivitas pengendalian, sedangkan *governance* menyediakan struktur pembagian tanggung jawab. Dari struktur tersebut muncul *accountability* terhadap pengelolaan risiko dan informasi. Pada sisi eksternal, *accountability* berkaitan dengan *transparency* dan *disclosure* kepada *stakeholder*.

Namun, hubungan tersebut tidak bersifat linear sepenuhnya. Hasil penelitian justru menunjukkan adanya *tension* antara *protection* dan *disclosure*. *Privacy* dan *security* membutuhkan pembatasan akses terhadap informasi. Sebaliknya, *accountability* dan *transparency* membutuhkan tersedianya informasi yang memadai bagi stakeholder. Oleh karena itu, organisasi harus menentukan batas antara informasi yang harus dilindungi dan informasi yang harus diungkapkan. Dalam konteks tersebut, *internal control*, *audit*, dan *governance* dapat berfungsi sebagai mekanisme penyeimbang. Ketiga mekanisme tersebut membantu menentukan siapa yang memiliki akses, bagaimana informasi dikendalikan, bagaimana risiko diawasi, serta informasi apa yang perlu dipertanggungjawabkan kepada stakeholder.

Model Sintesis Hasil SLR

Berdasarkan temuan tersebut, penelitian ini mengusulkan model sintesis

Tabel 6. Model Sintesis Hasil SLR

Level	Konsep	Fungsi	Output
1	*Privacy*	Melindungi kerahasiaan dan mengatur penggunaan informasi.	Controlled access
2	Information Security	Melindungi informasi dan sistem dari ancaman.	Secure information

3	Internal Control	Mengendalikan akses, proses dan risiko.	Controlled process
4	Audit/Assurance	Mengevaluasi efektivitas kontrol.	Assurance
5	Governance	Mengatur struktur, monitoring dan tanggung jawab.	Oversight
6	Accountability	Menetapkan pihak yang bertanggung jawab.	Responsibility
7	Transparency/Disclosure	Menyediakan informasi kepada stakeholder.	External information
8	Accounting Information Quality	Menunjukkan konsekuensi terhadap kualitas informasi.	Reliable/useful information

Model tersebut menunjukkan bahwa kualitas informasi akuntansi dapat dipandang sebagai hasil akhir dari proses yang tidak hanya bergantung pada sistem pencatatan dan pelaporan, tetapi juga pada perlindungan informasi, pengendalian internal, *assurance*, *governance*, dan akuntabilitas.

Research Gap

Tabel 7. Reserach Gap Berdasarkan Hasil Coding

Temuan Literatur	**Keterbatasan**	**Research Gap**
Cybersecurity sangat dominan.	Banyak penelitian berfokus pada breach/risk secara terpisah.	Integrasi cybersecurity dengan *Privacy* dan accountability.
Privacy muncul relatif terbatas.	Banyak dibahas dalam konteks data dan AI.	*Privacy* dalam konteks informasi akuntansi dan governance.
Accountability banyak dikaji melalui governance.	Jarang diposisikan bersama *Privacy* dan security.	Model integratif *Privacy*–security–accountability.
Internal control banyak menjadi mekanisme penghubung.	Hubungan antar mekanisme belum selalu disatukan.	Peran internal control sebagai *bridging mechanism*.
Audit banyak dikaitkan dengan cybersecurity.	Fokus terutama pada assurance/risk management.	Hubungan audit dengan accountability atas informasi.
Disclosure meningkat relevansinya setelah breach.	Security dan transparency dapat menciptakan konflik.	Bagaimana organisasi menyeimbangkan protection dan disclosure.
Information quality muncul sebagai konsekuensi.	Tidak semua penelitian menghubungkan kualitas informasi dengan *Privacy*.	Dampak integrasi *Privacy*–security–accountability terhadap kualitas informasi.

Gap utama yang ditemukan bukan semata-mata kurangnya penelitian mengenai cybersecurity. Penelitian mengenai cybersecurity dalam akuntansi telah berkembang. *Gap* yang lebih spesifik terletak pada belum terintegrasinya *Privacy*, *information security*, dan accountability dalam satu kerangka yang menjelaskan pengelolaan informasi akuntansi. Selain itu, penelitian terdahulu menunjukkan bahwa *internal control*, *audit*, dan *governance* memiliki potensi sebagai mekanisme penghubung. Namun, ketiga mekanisme tersebut masih sering diteliti secara terpisah. Hal ini memberikan peluang untuk mengembangkan perspektif yang lebih integratif.

Ringkasan Hasil Penelitian

Secara keseluruhan, hasil SLR menunjukkan lima temuan utama. Pertama, *information secuirty/cybersecurity* merupakan tema paling dominan dalam literatur yang dianalisis. Kedua, *Privacy* memiliki rung penelitian yang lebih terbatas, terutama dalam konteks information sharing, *Artificial Intellegence*, dan perlindungan data sensitif. Ketiga, internal control berperan sebagai mekanisma penghubung antara keamanan informasi dan kualitas informasi akuntansi. Keempat, *audit* dan *governance* menjadi mekanisme penting dalam membangun *accountability* atas pengelolaan *cybersecurity*. Kelima, *transparency* dan *disclosure* menunjukkan adanya ketegangan antara kebutuhan perlindungan informasi dan kebutuhan akuntabilitas kepada *stakeholder*.

Berdadarkan hasil tersebut, interaksi antara *Privacy*, information secrity, dan *accountability* dapat dipahami sebagai suatu sistem yang melibatkan mekanisme pengendalian dan *governance*. *Privacy* menentukan batas perlindungan informasi, *information security* menjaga informasi dari ancaman, *internal control* mengoperasionalkan perlindunan tersebut, *audit* menyediakan *assurance*, *governance* menetapkan struktur tanggung jawab, dan *accountbility* diwujudkan melalu *transparancey* serta *disclosure* yang tepat.

Dengan demikian, hasil penelitian menunjukkan bahwa kualitas informasi akuntansi tidak hanya ditentukan oleh kemampuan organisasi menghasilkan informasi, tetapi juga oleh kemampuan organisasi melindungi, mengendalikan, mengawasi, dan mempertanggungjawabkan informasi tersebut.

Pembahasan

Dominasi *Information Security* dalam Informasi Akuntansi

Hasil *Systematic Literature Review* terhadap 18 artikel menunjukkan bahwa *information security* merupakan tema paling dominan dalam perlindungan informasi akuntansi. Digitalisasi meningkatkan ketergantungan organisasi terhadap sistem dan data digital sehingga keamanan terhadap akses tidak sah, manipulasi, kehilangan data, dan *cybersecurity breach* menjadi sangat penting. Keamanan informasi tidak hanya berkaitan dengan teknologi, tetapi juga berhubungan dengan *internal control*, audit, dan *governance*. *Internal control* berperan menerjemahkan kebutuhan keamanan melalui pengendalian akses, *segregation of duties*, *risk assessment*, dan monitoring, sedangkan audit dan *governance* mendukung evaluasi, pengawasan, serta pembagian tanggung jawab.

Selain itu, *privacy* dan *transparency* menjadi dimensi penting yang perlu diseimbangkan dengan keamanan informasi. *Privacy* menentukan batas penggunaan dan pembagian informasi, sementara *transparency* memastikan informasi yang relevan dapat tersedia bagi pihak yang berkepentingan. Hubungan *privacy–security–accountability* tidak bersifat linear, tetapi dibentuk melalui *internal control*, audit, dan *governance* sebagai mekanisme penghubung dan penyeimbang. Dengan demikian, *information security* dapat dipandang sebagai fondasi perlindungan informasi akuntansi, sedangkan *privacy* dan *accountability* menjadi bagian dari tata kelola yang mendukung penggunaan, pengawasan, dan pertanggungjawaban informasi secara tepat.

***Privacy* sebagai Dimensi Perlindungan Informasi**

Hasil *Systematic Literature Review* menunjukkan bahwa *privacy* memiliki posisi penting sebagai dimensi perlindungan informasi akuntansi meskipun kemunculannya lebih terbatas dibandingkan *information security*. *Privacy* berkaitan dengan batas penggunaan, akses, dan pembagian informasi, terutama informasi sensitif. Dalam kerangka ETHOs, *privacy* dan *security* dipandang sebagai bagian dari isu etika dalam *Accounting Information Systems* (AIS), sehingga

perlindungan informasi tidak hanya menjadi persoalan teknis, tetapi juga tanggung jawab etis dalam pengelolaan informasi.

Perkembangan teknologi seperti *artificial intelligence* semakin meningkatkan tantangan terhadap *privacy*, terutama terkait data sensitif, akses, dan *consent*. Oleh karena itu, perlindungan *privacy* tidak cukup hanya dilakukan melalui mekanisme teknis atau kepatuhan formal, tetapi membutuhkan pengawasan profesional dan mekanisme organisasi yang jelas. *Privacy* juga perlu diseimbangkan dengan kebutuhan *information sharing*, karena pembatasan akses yang terlalu ketat dapat mengurangi manfaat informasi, sedangkan keterbukaan berlebihan dapat meningkatkan risiko terhadap kerahasiaan informasi.

***Internal Control* sebagai Mekanisme Penghubung**

Hasil SLR menunjukkan bahwa *internal control* memiliki posisi strategis sebagai mekanisme penghubung antara *information security* dan kualitas informasi akuntansi. Berdasarkan kerangka COSO, *risk assessment*, *control activities*, *information and communication*, serta *monitoring activities* merupakan komponen yang saling terintegrasi dalam pengendalian. *Internal control* juga mencakup pengendalian teknologi informasi dan akuntabilitas atas pengendalian di seluruh organisasi, sehingga dapat membantu mengurangi risiko yang memengaruhi keandalan informasi akuntansi.

Secara kritis, *internal control* tidak dapat dipandang sebagai mekanisme yang berdiri sendiri karena efektivitasnya bergantung pada penerapan dan integrasinya dalam proses organisasi. Pengendalian seperti pengendalian akses, *segregation of duties*, evaluasi risiko, dan pemantauan menerjemahkan kebutuhan keamanan informasi ke dalam praktik konkret. Dengan demikian, *internal control* menjadi titik temu antara *information security*, kualitas informasi akuntansi, dan *governance*, sehingga keamanan informasi tidak hanya bergantung pada teknologi, tetapi juga pada struktur pengendalian organisasi.

Audit dan *Governance* dalam Membentuk *Accountability*

Hasil SLR menunjukkan bahwa *accountability* dalam keamanan informasi akuntansi dibentuk melalui interaksi antara *internal audit* dan *governance*. Audit berperan sebagai mekanisme *assurance* dan evaluasi risiko, sedangkan *governance* mengatur pembagian peran dan tanggung jawab antara fungsi pengendalian, CISO, *internal audit*, manajemen, dan dewan direksi. Efektivitas fungsi *assurance* juga dipengaruhi oleh kematangan fungsi audit serta kompetensi dan pengetahuan teknologi informasi yang dimiliki auditor.

Dengan demikian, *accountability* tidak cukup dibentuk melalui pemeriksaan setelah risiko terjadi, tetapi membutuhkan pembagian peran, kompetensi, keterlibatan manajemen, dan *oversight* dari dewan. *Internal audit* berfungsi sebagai mekanisme *assurance*, sedangkan *governance* menyediakan struktur untuk menentukan siapa yang bertanggung jawab, kepada siapa pertanggungjawaban diberikan, dan bagaimana organisasi merespons risiko. Oleh karena itu, *accountability* lebih tepat dipahami sebagai hasil dari tata kelola yang terintegrasi.

Tension* antara *Privacy*, *Security*, dan *Transparency

Hasil SLR menunjukkan bahwa *privacy*, *information security*, dan *transparency* memiliki tujuan yang saling melengkapi, tetapi juga dapat menimbulkan ketegangan dalam pengelolaan informasi akuntansi. *Privacy* dan *security* menekankan perlindungan informasi dari akses atau penggunaan yang tidak semestinya, sedangkan *transparency* menuntut tersedianya informasi yang memadai bagi pihak yang berkepentingan. Oleh karena itu, keterbukaan informasi perlu dilakukan secara terkendali agar kebutuhan *disclosure* tidak mengabaikan perlindungan terhadap kerahasiaan dan keamanan informasi.

KESIMPULAN

Berdasarkan *Systematic Literature Review* terhadap 18 artikel, penelitian ini menunjukkan bahwa *privacy*, *information security*, dan *accountability* dalam Sistem Informasi Akuntansi merupakan konsep yang saling terkait. *Information security/cybersecurity* menjadi tema dominan karena digitalisasi meningkatkan ketergantungan organisasi pada sistem dan data digital, sehingga perlindungan terhadap akses tidak sah, manipulasi, kehilangan informasi, dan *data breach* menjadi penting. Sementara itu, *privacy* menentukan batas penggunaan, akses, dan pembagian informasi, khususnya terkait data sensitif dan pemanfaatan *artificial intelligence*. Hubungan antara keamanan informasi dan *accountability* tidak berlangsung secara langsung, tetapi dimediasi oleh *internal control*, audit/*assurance*, dan governance. *Internal control* menerjemahkan kebutuhan perlindungan informasi melalui pengendalian akses, *segregation of duties*, *risk assessment*, *monitoring*, dan pengendalian teknologi informasi, sedangkan audit dan *assurance* mengevaluasi efektivitas pengendalian, serta *governance* mengatur pengawasan dan pembagian tanggung jawab. Penelitian juga menemukan adanya *tension* antara *privacy* dan *security* dengan tuntutan *transparency* dan *disclosure*, di mana transparansi tidak berarti membuka seluruh informasi, tetapi menyediakan informasi yang relevan dan memadai melalui mekanisme pengungkapan yang terkontrol. Dengan demikian, *privacy* menentukan batas perlindungan informasi, *information security* menjaga keamanan sistem dan informasi, *internal control* mengendalikan akses dan risiko, audit/*assurance* mengevaluasi pengendalian, dan *governance* mengatur pengawasan serta tanggung jawab. Keseluruhan mekanisme tersebut mendukung terwujudnya *accountability* melalui *responsibility*, *transparency*, dan *disclosure*, sehingga menghasilkan informasi akuntansi yang lebih andal dan berguna bagi pengambilan keputusan. Model yang dihasilkan merupakan sintesis konseptual dari literatur dan bukan hubungan kausal yang telah diuji secara langsung. Oleh karena itu, penelitian selanjutnya dapat menguji secara empiris model integratif *privacy–information security–accountability*, khususnya peran *internal control*, audit, dan *governance* sebagai mekanisme penghubung dalam berbagai konteks organisasi dan perkembangan teknologi.

DAFTAR PUSTAKA

Akin, I., Wilczkowska, L., & Akin, M. (2026). Ethical and Data *Privacy* Risks in AI-Driven Accounting: A Mixed-Methods Study. *Human Behavior and Emerging Technologies*, *2026*(1). https://doi.org/10.1155/hbe2/6048044

Blakely, B., Kurtenbach, J., & Nowak, L. (2022). Exploring the information content of cyber breach reports and the relationship to internal controls. *International Journal of Accounting Information Systems*, *46*, 100568. https://doi.org/https://doi.org/10.1016/j.accinf.2022.100568

Calvin, C., Eulerich, M., & Holt, M. (2025a). Characteristics of cybersecurity and IT involvement by the IA activity. *International Journal of Accounting Information Systems*, *56*. https://doi.org/10.1016/j.accinf.2025.100726

Calvin, C., Eulerich, M., & Holt, M. (2025b). Characteristics of cybersecurity and IT involvement by the IA activity. *International Journal of Accounting Information Systems*, *56*. https://doi.org/10.1016/j.accinf.2025.100726

Chen, C.-Y., Goh, B. W., Lee, J., & Li, N. (2026). The Effect of Cybersecurity Breaches on Analysts' Earnings Forecasts. *European Accounting Review*, *35*(1), 263–289. https://doi.org/10.1080/09638180.2025.2476760

Cram, W. A., Wang, T., & Yuan, J. (2023a). Cybersecurity Research in Accounting Information Systems: A Review and Framework. *Journal of Emerging Technologies in Accounting*, *20*(1), 15–38. https://doi.org/10.2308/JETA-2020-081

Cram, W. A., Wang, T., & Yuan, J. (2023b). Cybersecurity Research in Accounting Information Systems: A Review and Framework. *Journal of Emerging Technologies in Accounting*, *20*(1), 15–38. https://doi.org/10.2308/JETA-2020-081

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. In *Current Issues in Auditing* (Vol. 13, Number 2, pp. C1–C9). American Accounting Association. https://doi.org/10.2308/ciia-52419

Garg, M., Wang, T., & Wilkin, C. L. (2025). Impact of reporting information security breaches, accounting quality, and the opportunistic disclosure of good news and bad news. *International Journal of Accounting Information Systems*, *56*, 100729. https://doi.org/https://doi.org/10.1016/j.accinf.2025.100729

Guragai, B., Hunt, N. C., Neri, M. P., & Taylor, E. Z. (2017a). Accounting Information Systems and Ethics Research: Review, Synthesis, and the Future. *Journal of Information Systems*, *31*(2), 65–81. https://doi.org/10.2308/isys-51265

Guragai, B., Hunt, N. C., Neri, M. P., & Taylor, E. Z. (2017b). Accounting Information Systems and Ethics Research: Review, Synthesis, and the Future. *Journal of Information Systems*, *31*(2), 65–81. https://doi.org/10.2308/isys-51265

Jiang, W., Xu, C., & Counts, R. W. (2024). XBRL reporting in firms with data breach incidents. *Journal of Corporate Accounting & Finance*, *35*(3), 146–156. https://doi.org/10.1002/jcaf.22701

Kim, R., Hedley, T., Gangolly, J., & Ravi, S. S. (2025). Segregation of duties in accounting systems: A framework. *International Journal of Accounting Information Systems*, *56*, 100725. https://doi.org/https://doi.org/10.1016/j.accinf.2025.100725

Kogan, A., & Yin, C. (2021). *Privacy*-Preserving Information Sharing within an Audit Firm. *Journal of Information Systems*, *35*(2), 243–268. https://doi.org/10.2308/ISYS-2020-017

Liu, L. Y. (2025). Financial Statement Audits and Data Breaches. *Management Science*, *71*(8), 6340–6366. https://doi.org/10.1287/mnsc.2023.01357

Mahdi, Z. R. (2022). IT GOVERNANCE AND INFORMATION SECURITY OF ACCOUNTING INFORMATION SYSTEMS: A CASE STUDY. *Akkad Journal Of Contemporary Accounting Studies*, *1*(2), 75–93. https://doi.org/10.55202/ajcas.v1i2.12

Mojtahedi, A., & Zhou, L. (2024a). Information technology internal control material weaknesses in financial reporting: Categories, trends, associations, and industry effects. *International Journal of Accounting Information Systems*, *53*, 100679. https://doi.org/https://doi.org/10.1016/j.accinf.2024.100679

Mojtahedi, A., & Zhou, L. (2024b). Information technology internal control material weaknesses in financial reporting: Categories, trends, associations, and industry effects. *International Journal of Accounting Information Systems*, *53*, 100679. https://doi.org/https://doi.org/10.1016/j.accinf.2024.100679

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw,

J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, n71. https://doi.org/10.1136/bmj.n71

Rezaee, Z., Zhou, G., & Bu, L. (Luther). (2024). Corporate social irresponsibility and the occurrence of data breaches: A stakeholder management perspective. *International Journal of Accounting Information Systems*, *53*, 100677. https://doi.org/https://doi.org/10.1016/j.accinf.2024.100677

Seaton Kelton, A., & Yang, Y.-W. (2024). Understanding cybersecurity breach contagion effects: The role of the loss heuristic and internal controls. *International Journal of Accounting Information Systems*, *55*, 100714. https://doi.org/https://doi.org/10.1016/j.accinf.2024.100714

Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. *International Journal of Accounting Information Systems*, *51*. https://doi.org/10.1016/j.accinf.2023.100642

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, *44*. https://doi.org/10.1016/j.accinf.2021.100548

Tadesse, A., Walton, S., & Zhang, Y. (2026). COSO Framework Adoption and Cybersecurity Breaches. *Journal of Information Systems*, *40*(1), 47–75. https://doi.org/10.2308/ISYS-2024-044

Vo, H., & Pham, M. D. (2025). Beware of false prophets: Cybersecurity risk and strategic voluntary disclosure. *British Accounting Review*. https://doi.org/10.1016/j.bar.2025.101578

Zhang, C., Zhu, W., Dai, J., Wu, Y., & Chen, X. (2023). Ethical impact of artificial intelligence in managerial accounting. *International Journal of Accounting Information Systems*, *49*, 100619. https://doi.org/https://doi.org/10.1016/j.accinf.2023.100619