

PERAN KEAMANAN SIBER DALAM MENINGKATKAN TRANSPARANSI DAN AKUNTABILITAS TERHADAP LAPORAN KEUANGAN DI BANK SYARIAH INDONESIA

Putri Salbiah Sukma Br. Nst¹, Farida Khairani Lubis², Keisya Fitri Wulandari³, Nita Azhari Simanjuntak⁴

¹ Fakultas Ekonomi dan Bisnis, Universitas Islam Sumatera Utara

¹email: putrisalbiah734@gmail.com,

²Fakultas Ekonomi dan Bisnis, Universitas Islam Sumatera Utara

²email: farida.khairanilubis@gmail.com,

³Fakultas Ekonomi dan Bisnis, Universitas Islam Sumatera Utara

³email: wulandarikeisyafitri@gmail.com,

⁴Fakultas Ekonomi dan Bisnis, Universitas Islam Sumatera Utara

⁴ email; nitaazhari2023@gmail.com

ABSTRACT

The title of this study is "The Role of Cybersecurity in Enhancing Transparency and Accountability of Financial Reports in Islamic Banks in Indonesia." The aim of this study is to identify the relationship between the role of cybersecurity and the improvement of transparency and responsibility of financial reports in the Islamic banking industry. Data collected through quantitative surveys indicate that companies implementing good cybersecurity practices not only protect sensitive data but also improve the transparency of information presented to the public. The study also notes that the financial sector, including Bank Syariah Indonesia (BSI), faces serious threats from cyberattacks, such as phishing and malware, which can damage reputation and customer trust. The BSI Error incident that occurred in May 2023 serves as a real example of the challenges faced in maintaining data security. Utilizing a causal research design, the study shows that clear and comprehensible disclosures improve financial reporting transparency and accountability. These findings highlight the importance of improving cybersecurity to protect financial data and other sensitive information, as well as to comply with existing regulations in Indonesia regarding personal data protection and information security.

Keywords: Cybersecurity, Transparency, Accountability, Financial Reporting, Indonesia Islamic Bank

ABSTRAK

Judul penelitian ini adalah "Peran Keamanan Siber dalam Meningkatkan Transparansi dan Akuntabilitas Laporan Keuangan pada Bank Umum Syariah di Indonesia." Tujuan dari penelitian ini adalah untuk mengidentifikasi hubungan peran keamanan siber dengan peningkatan transparansi dan tanggung jawab laporan keuangan pada industri perbankan syariah. Data yang dikumpulkan melalui survei kuantitatif menunjukkan bahwa perusahaan yang menerapkan praktik keamanan siber yang baik tidak hanya melindungi data sensitif, tetapi juga meningkatkan transparansi informasi yang disampaikan kepada publik. Penelitian ini juga mencatat bahwa sektor keuangan, termasuk Bank Syariah Indonesia (BSI), menghadapi ancaman serius dari serangan siber, seperti phishing dan malware, yang dapat merusak reputasi dan kepercayaan nasabah. Insiden BSI Error yang terjadi pada Mei 2023 menjadi contoh nyata dari tantangan yang dihadapi dalam menjaga keamanan data. Dengan menggunakan desain penelitian kausal, penelitian ini membuktikan bahwa pengungkapan yang jelas dan mudah dipahami dapat meningkatkan transparansi dan akuntabilitas laporan keuangan. Temuan ini menunjukkan pentingnya peningkatan keamanan siber untuk melindungi data keuangan dan informasi sensitif lainnya, serta untuk memenuhi regulasi yang ada di Indonesia terkait perlindungan data pribadi dan keamanan informasi.

Kata kunci: Keamanan Siber, Transparansi, Akuntabilitas, Laporan Keuangan, Bank Syariah Indonesia

I. PENDAHULUAN

Keamanan siber berperan sebagai pelindung terhadap berbagai ancaman yang dapat mengganggu integritas laporan keuangan. Keamanan informasi mencakup aspek kerahasiaan yang harus dijaga agar terhindar dari retasan data. Dalam konteks ini, laporan keuangan perusahaan harus dapat diandalkan untuk menjaga kepercayaan investor dan pemangku kepentingan lainnya.(ISO 27001, 2013)

Penelitian oleh Alhassan et al. (2019) menunjukkan bahwa perusahaan yang menerapkan praktik keamanan siber yang baik tidak hanya melindungi data sensitif, tetapi juga meningkatkan transparansi informasi yang disampaikan kepada publik. Keberhasilan dalam hal ini sangat bergantung pada pengungkapan yang jelas dan mudah dipahami, yang pada akhirnya dapat mengurangi biaya audit internal. Ini menunjukkan bahwa adanya korelasi antara praktik keamanan siber yang efektif dan tingkat akuntabilitas laporan keuangan.(Alhassan et al., 2019b)

Menurut data Badan Siber salah satu sektor yang paling sering dilaporkan pada tahun 2022 adalah sektor perbankan dan jasa keuangan, yang mencakup 23% dari seluruh pelanggaran yang dilaporkan oleh orang dalam. Hal ini menunjukkan betapa pentingnya memperkuat keamanan siber di industri ini untuk melindungi data keuangan dan informasi sensitif lainnya.(Direktorat Operasi Keamanan Siber & Negara, 2022). Persoalan krusial lainnya adalah landasan hukum keamanan data di Indonesia. Keamanan informasi dan perlindungan data pribadi diatur oleh undang-undang No. 19/2016 Peraturan ini mewajibkan perusahaan untuk melindungi data mereka guna mencegah sanksi hukum yang dapat merugikan reputasi dan operasi bisnis mereka.(Republik Indonesia, 2008)

Dalam industri perbankan, ancaman keamanan siber sering kali terjadi, terutama dalam bentuk Phishing, Malware, dan kebocoran data. Phishing adalah suatu jenis aktivitas yang bertujuan mengelabui atau menipu seseorang dengan tujuan memancingnya.(Wibowo & Fatimah, 2017) Dalam beberapa tahun terakhir, malware bank menjadi semakin umum dan menimbulkan ancaman serius bagi lembaga keuangan dan nasabahnya. Hal ini dapat mencegah kebocoran informasi sensitif, kerugian finansial, dan rusaknya reputasi seseorang.(Fitria, 2023) Kebocoran data terjadi ketika informasi sensitif nasabah atau bank terekspos, baik melalui peretasan langsung atau kesalahan internal. Tujuan utama dari Cybercrime adalah mendapatkan keuntungan pribadi secara ilegal, terutama dalam sektor keuangan. Peningkatan keamanan jaringan dalam industri jasa finansial menjadi fokus utama karena adanya peningkatan serangan siber terhadap sektor ini.(Azzahra et al., 2024)

Saat ini, industri perbankan syariah, seperti Bank Syariah Indonesia (BSI), didasarkan pada risiko keamanan yang semakin rumit. Salah satu isu paling signifikan yang diangkat adalah peretasan, yang memiliki kemampuan mengungkap data nasabah dan merusak kepercayaan masyarakat terhadap bank. Saat ini BSI menghadapi tantangan yang cukup besar terkait masalah teknis dan pemeliharaan. Salah satu insiden yang paling menonjol adalah Kesalahan BSI menjelang akhir tahun 2023, yang mengganggu operasional bank secara signifikan.

Selain itu, muncul dugaan adanya tindakan peretasan, yang semakin memperkuat kekhawatiran mengenai keamanan data dan informasi pelanggan. Berdasarkan laporan media, insiden ini menimbulkan rasa khawatir di kalangan nasabah terhadap perlindungan data mereka dan menurunkan tingkat kepercayaan mereka terhadap bank. Tidak hanya itu, insiden ini juga

menyebabkan ketidaknyamanan bagi nasabah, membuat mereka kesulitan dalam melakukan transaksi. Peristiwa ini memunculkan pertanyaan mendalam tentang kesiapan teknis dan keamanan BSI dalam menghadapi tantangan era modern serta implikasinya terhadap transparansi dan akuntabilitas laporan keuangan.

Meningkatkan kepercayaan pemegang saham sangat penting bagi perusahaan yang terdaftar di BEI untuk menerapkan strategi keamanan yang tidak hanya mematuhi peraturan tetapi juga meningkatkan kepercayaan investor. Menganalisis dan mengidentifikasi peran siber keamanan dalam meningkatkan transparansi dan akuntabilitas transaksi keuangan di Bank Syariah Indonesia merupakan tujuan penelitian ini. Fokus utama penelitian ini adalah pada praktik manajemen siber praktis yang digunakan oleh perusahaan tercatat dan pengaruhnya terhadap keamanan data keuangan. (Luthfah, 2023)

LANDASAN TEORI

Teori Keamanan Siber

Dalam konteks institusi keuangan, keamanan siber berfungsi untuk menjaga integritas dan kerahasiaan data keuangan yang sangat sensitif. Menurut Kaur dan Kumar (2021), dengan meningkatnya kompleksitas serangan siber, institusi keuangan perlu mengimplementasikan strategi keamanan yang komprehensif untuk mengurangi risiko. Hal ini mencakup penggunaan teknologi mutakhir seperti enkripsi data dan autentikasi multi-faktor yang dapat melindungi informasi dari akses yang tidak sah. (Akhta et al., 2021)

Selain itu, serangan siber yang berhasil dapat berakibat fatal bagi reputasi dan kepercayaan publik terhadap institusi keuangan. Penelitian oleh Verma dan Sharma (2022) menunjukkan bahwa serangan yang mengakibatkan kebocoran data tidak hanya menyebabkan kerugian finansial, tetapi juga merusak hubungan dengan pelanggan dan pemangku kepentingan. Dalam era di mana informasi lebih mudah diakses dan dibagikan, penting bagi institusi untuk menjaga perlindungan data personal dalam pengungkapan risiko keamanan yang dihadapi. Keterbukaan mengenai langkah-langkah yang diambil untuk mengamankan informasi dapat meningkatkan kepercayaan investor. (Verma et al., 2022)

Dalam era digital, ancaman phishing menjadi salah satu tantangan utama dalam keamanan siber, terutama bagi pengguna media sosial dan organisasi. Ancaman phishing terhadap pengguna media sosial merupakan salah satu bentuk kejahatan siber yang dapat merugikan individu dan organisasi. Kejahatan ini sering kali memanfaatkan kelalaian pengguna untuk mengakses informasi sensitif, yang dapat berdampak serius pada reputasi dan integritas data. Oleh karena itu, kesadaran dan edukasi pengguna menjadi sangat penting dalam menghadapi ancaman ini, sehingga organisasi dapat melindungi data keuangan dan informasi lainnya dari serangan yang merugikan. (Wibowo & Fatimah, 2017)

Sebagai tambahan, regulasi yang ketat di sektor keuangan juga menekankan pentingnya keamanan siber. Banyak negara, termasuk Indonesia, telah mengadopsi kerangka kerja regulasi yang mengharuskan perusahaan untuk mematuhi standar tertentu dalam hal perlindungan data. Ketaatan terhadap regulasi ini bukan hanya untuk menghindari sanksi hukum, tetapi juga untuk membangun reputasi yang kuat dan meningkatkan daya saing di pasar global. Dalam hal ini, keamanan siber tidak hanya menjadi sebuah kebutuhan, tetapi juga merupakan investasi strategis untuk keberlangsungan dan pertumbuhan perusahaan di sektor keuangan. (Swajati, 2019)

Transparansi

Transparansi laporan keuangan merupakan aspek krusial dalam meningkatkan kepercayaan publik terhadap perusahaan. Menurut Sari dan Santoso (2021), transparansi dalam laporan keuangan memungkinkan pemangku kepentingan, termasuk investor dan kreditur, untuk memahami kondisi keuangan dan kinerja perusahaan dengan lebih baik. Hal ini penting karena informasi yang jelas dan akurat dapat mengurangi ketidakpastian yang sering kali mengelilingi keputusan investasi dan meminimalkan risiko informasi asimetris. (Eka Puspita Sari, Aprih Santoso, 2021)

Transparansi laporan keuangan memainkan peran penting dalam menciptakan lingkungan pasar yang sehat. Tingkat transparansi laporan keuangan yang tinggi berhubungan positif dengan kepuasan investor dan keputusan investasi. Ketika perusahaan mengungkapkan informasi keuangan secara terbuka, mereka tidak hanya memenuhi regulasi tetapi juga memberikan sinyal positif kepada pasar. Hal ini berpotensi meningkatkan nilai saham dan menarik lebih banyak minat dari investor baru, sehingga menciptakan ekosistem investasi yang lebih dinamis. (Saputra, 2023)

Namun, untuk mencapai tingkat transparansi yang optimal, perusahaan harus menghadapi tantangan yang beragam, termasuk kompleksitas informasi dan kebutuhan untuk mematuhi regulasi yang ada. Banyak perusahaan masih berjuang untuk memenuhi standar transparansi yang diharapkan oleh pemangku kepentingan, terutama di sektor keuangan. Kegagalan dalam menyediakan laporan yang transparan dapat mengakibatkan hilangnya kepercayaan publik dan, pada gilirannya, dampak negatif terhadap kinerja perusahaan. Oleh karena itu, integrasi praktik keamanan siber yang baik dapat menjadi langkah penting untuk memastikan bahwa informasi keuangan yang disajikan tetap aman dan transparan. (Hanisa et al., 2024)

Dengan mempertimbangkan pentingnya transparansi laporan keuangan, jelas bahwa upaya untuk meningkatkannya harus menjadi prioritas bagi perusahaan, terutama di sektor keuangan. Keterbukaan informasi tidak hanya memperkuat kepercayaan investor, tetapi juga berkontribusi pada stabilitas pasar secara keseluruhan. Namun, untuk mencapai transparansi yang optimal, perusahaan harus mengatasi berbagai tantangan, termasuk kompleksitas informasi dan kepatuhan terhadap regulasi. Dalam konteks ini, adopsi praktik keamanan siber yang efektif dapat memainkan peran krusial dalam melindungi integritas informasi keuangan, yang selanjutnya akan memperkuat kepercayaan publik dan mendukung akuntabilitas yang lebih tinggi. Dengan demikian, transparansi laporan keuangan dan keamanan siber saling terkait erat dalam menciptakan ekosistem bisnis yang sehat dan berkelanjutan.

Akuntabilitas

Akuntabilitas dalam laporan keuangan merujuk pada kewajiban entitas untuk menyampaikan informasi yang akurat dan transparan kepada pemangku kepentingan. Konsep ini mencakup prinsip-prinsip fundamental seperti transparansi, keandalan, relevansi, dan kepatuhan. Relevansi menunjukkan pentingnya informasi dalam membantu pengambilan keputusan, sedangkan kepatuhan memastikan bahwa laporan mengikuti standar akuntansi dan peraturan yang berlaku.

Dalam konteks teori legitimasi, organisasi berusaha untuk memperoleh dan mempertahankan legitimasi di mata publik. Penyajian laporan keuangan yang akuntabel tidak hanya menciptakan kepercayaan di antara pemangku kepentingan, tetapi juga dapat meningkatkan kinerja organisasi. Penelitian terdahulu menemukan adanya korelasi variabel dependen yang positif antara akuntabilitas dan kinerja, seperti yang diungkapkan oleh Hastuti (2019), yang menemukan

bahwa organisasi dengan akuntabilitas tinggi cenderung memiliki kinerja yang lebih baik.(Cahyono & Hastuti, 2024) transparansi laporan keuangan berkontribusi pada peningkatan akuntabilitas publik di sektor pemerintahan.(Zubaidah & Nugraeni, 2023) Telah diketahui bahwa kepatuhan terhadap standar akuntansi berpengaruh signifikan terhadap tingkat akuntabilitas laporan keuangan. Dengan demikian, akuntabilitas dalam laporan keuangan menjadi aspek yang krusial bagi entitas untuk membangun kepercayaan dan legitimasi di mata pemangku kepentingan.

II. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah metode kualitatif yaitu penelitian yang dapat dikonstruksi sebagai strategi penelitian yang biasanya menekankan pada kata-kata daripada kuantifikasi terhadap pengumpulan dan analisis data. Penelitian kualitatif biasanya merupakan penelitian yang menekankan pada pendekatan induktif dalam pengertian antara teori dan penelitian, dimana teori merupakan hasil dari penelitian dari data-data yang telah dikumpulkan.(Bryman, 2012). Peneliti menggunakan pendekatan penelitian kualitatif untuk menilai hubungan antara variabel independen dan dependen. Perancangan kualitatif ini bertujuan untuk mengidentifikasi akar penyebab permasalahan tersebut guna mengantisipasi dampak keamanan siber terhadap peningkatan transparansi dan akuntabilitas laporan keuangan Bank Syariah Indonesia.

Sesuai dengan tujuan peneliti, maka dalam penelitian dengan standar tertentu, populasi dalam penelitian ini sebanyak 78 responden nasabah sebagai sampel pengguna Bank Syariah Indonesia (BSI). Data kuantitatif digunakan dalam penyelidikan ini, dan dikumpulkan dengan menggunakan skala Likert atau format kuesioner dan teknik analisis data. Pertanyaan ini akan digunakan untuk mengukur seberapa puas pelanggan terhadap keamanan siber, transparansi, dan daya tanggap laporan keuangan BSI. Pengolahan datanya menggunakan *Statistic Package for Social (SPSS) versi 20*. Alat analisis yang digunakan yaitu metode statistik deskriptif, analisis regresi linier berganda, uji koefisien determinasi (R^2), uji signifikan simultan (uji f), uji signifikansi parameter individual (uji t), dan pengujian hipotesis.

III. HASIL DAN PEMBAHASAN

Statistik Deskriptif

Menurut Ghozali (Ghozali, 2011) Statistik deskriptif menggunakan kriteria berikut untuk menjelaskan atau mendeskripsikan data: mean, standar deviasi, varians, maksimum, minimum, bilangan, luas, kurtosis, serta skewness (kemencengan distribusi). Hasil dari uji analisis statistik deskriptif dapat dilihat pada tabel 1.

Tabel 1. Uji Statistik Deskriptif
Descriptive Statistics

	N	Minimum	Maximum	Sum	Mean	Std. Deviation
Keamanan Siber (X1)	78	2	10	639	8.19	1.546
Transparansi (X2)	78	2	10	621	7.96	1.516
Akuntabilitas (X3)	78	2	10	613	7.86	1.569
Laporan Keuangan di BSI (Y)	78	2	10	613	7.86	1.569
Valid N (listwise)	78					

Sumber: Olahan Data SPSS, 2025

Terlihat dari tabel di atas terdapat 78 jumlah responden dalam penelitian ini. Hasil uji statistik deskriptif pada variabel “Keamanan Siber” menunjukkan tingkat keamanan yang tinggi, dengan nilai minimum 2, nilai maksimum 10, dan nilai sedang sebesar 8,19. Namun terdapat standar deviasi sebesar 1.546 yang terdapat pada 78 jawaban responden. Temuan penelitian ini dapat dianggap homogen jika standar deviasinya lebih kecil dari mean. Variabel transparansi memiliki rentang nilai 2 sampai 10 dengan rata-rata sebesar 7,96 dan standar deviasi sekitar 1,516. Variabel Akuntabilitas memiliki rentang nilai 2 sampai 10, dengan rata-rata sebesar 7,86 dan standar deviasi sekitar 1,569. Laporan keuangan dianggap berkualitas tinggi.

Analisis Regresi Linear Berganda

Analisis ini diterapkan untuk memahami seberapa besar kontribusi variabel independen (X) terhadap variabel dependen (Y), dengan output yang diperoleh melalui pemrosesan menggunakan perangkat lunak SPSS versi 20. Berikut adalah hasil pembahasan:

Tabel 2. Uji Hipotesis Analisis Regresi Berganda
Coefficients^a

Model	Unstandardized Coefficients	
	B	Std. Error
(Constant)	.312	.432
1 Total_X1	.130	.082
Total_X2	.453	.103
Total_X3	.377	.105

a. Dependent Variable: Total_Y

Sumber: Olahan Data SPSS, 2025

Berdasarkan hasil tabel di atas, yang perlu diinterpretasikan adalah kolom B. Baris pertama menunjukkan konstanta (α), sementara baris-baris berikutnya menunjukkan konstanta untuk variabel independen. Oleh karena itu, persamaan regresi linier berganda dapat dirumuskan sebagai berikut:

$$Y = 0,312 + 0,130X_1 + 0,453X_2 + 0,377X_3 + \varepsilon$$

Keterangan :

Y : Laporan keuangan di BSI

X₁ : Peran keamanan siber

X₂ : Transparansi

X₃ : Akuntabilitas

ε : Error (faktor kesalahan)

Penjelasan hasil regresi :

1. **Keamanan Siber (X₁)** berpengaruh positif terhadap laporan keuangan BSI dengan koefisien regresi sebesar 0,130. Artinya, setiap peningkatan praktik keamanan siber sebesar 1 satuan akan meningkatkan laporan keuangan sebesar 0,130 satuan, meskipun berdasarkan uji t, pengaruh ini tidak signifikan secara statistik.

2. **Transparansi (X₂)** menunjukkan koefisien sebesar 0,453, yang berarti transparansi berpengaruh positif dan signifikan terhadap laporan keuangan BSI. Semakin tinggi transparansi, maka semakin meningkat kualitas laporan keuangan.
3. **Akuntabilitas (X₃)** memiliki koefisien sebesar 0,377, yang juga menunjukkan pengaruh positif dan signifikan terhadap laporan keuangan. Artinya, peningkatan akuntabilitas dalam pelaporan keuangan akan memperbaiki kepercayaan stakeholder terhadap laporan tersebut.

Uji Koefisien Determinasi (R²)

Tabel 3. Hasil Uji Koefisien Determinan (R²)

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.907 ^a	.823	.816	.663

a. Predictors: (Constant), Total_X3, Total_X1, Total_X2

Sumber: Olahan Data SPSS, 2025

Adjusted R-Quadratwert digunakan pada tabel di atas untuk mengukur sejauh mana kontribusi variabel “Keamanan Siber” (X₁), “Transparansi” (X₂), dan “Akuntabilitas” (X₃) terhadap pengaruh variabel Laporan Keuangan di BSI (Y), yaitu 0,816. Hal ini menunjukkan bahwa transparansi, tanggung jawab, dan keamanan siber menyumbang sekitar 81,6 persen variasi keputusan. Namun belum diketahui faktor apa saja yang mempengaruhi sekitar 18,4%.

Uji Signifikan Simultan (Uji F)

Uji F bertujuan untuk mengetahui pengaruh uji statistik yang digunakan untuk menentukan apakah ada pengaruh yang signifikan dari satu atau lebih variabel independen terhadap variabel dependen dalam model regresi. (Ghozali, 2011)

Tabel 4. Hasil Uji F

ANOVA^a

Model	Sum of Squares	Df	Mean Square	F	Sig.
1 Regression	151.221	3	50.407	114.514	.000 ^b
Residual	32.574	74	.440		
Total	183.795	77			

a. Dependent Variable: Total_Y

b. Predictors: (Constant), Total_X3, Total_X1, Total_X2

Sumber: Olahan Data SPSS, 2025

Berdasarkan tabel di atas, diketahui bahwa nilai akuntabilitas sebesar 0,000, yang berarti semua variabel independen dalam penelitian ini secara bersama-sama (simultan) memiliki pengaruh yang signifikan terhadap variabel dependen.

Uji Signifikansi Parameter Individual T

Signifikansi pengaruh variabel independen terhadap variabel dependen diuji dengan menggunakan uji t atau uji parsial. Hasil uji-t disajikan di bawah ini:

Tabel 5. Hasil Uji T

Coefficients^a

Model	Unstandardized Coefficients		standardized Coefficients	t.	Sig.
	B	Std. Error	Beta		
(Constant)	.312	.432		.722	.472
1 Keamanan Siber	.130	.082	.130	1.583	.118
Transparansi	.453	.103	.444	4.381	.000
Akuntabilitas	.377	.105	.383	3.593	.001

a. Dependent Variable: Laporan Keuangan BSI

Sumber: Olahan Data SPSS, 2025

Tujuan dari uji statistik t adalah untuk melihat bagaimana variabel dependen dipengaruhi oleh variabel independen secara parsial. Berdasarkan hasil penelitian, nilai T-hitung dihitung dan dibandingkan dengan nilai T-tabel menggunakan rumus $df = n$ (jumlah sampel) – k (jumlah variabel independen) – 1, atau $78 - 3 - 1 = 74$, yang menghasilkan nilai T-tabel sebesar 1,992 dengan tingkat signifikansi 0,05. Selain membandingkan nilai T-hitung dan T-tabel, hipotesis juga dapat diuji dengan menghitung tingkat signifikansi. Penjelasan untuk Hipotesis 1-3 adalah sebagai berikut:

1) Dampak Keamanan Siber terhadap Laporan Keuangan BSI

Hipotesis yang diuji adalah:

H0: Peran Keamanan Siber tidak berpengaruh signifikan terhadap Laporan Keuangan di BSI

H1: Peran Keamanan Siber berpengaruh signifikan terhadap Laporan Keuangan di BSI

Hasil uji dan pembahasan : Berdasarkan hasil penelitian, diperoleh nilai T-hitung sebesar 1,583 untuk variabel keamanan siber (X1) dengan tingkat signifikansi sebesar 0,118. Karena T-hitung lebih kecil dari T- table 1,992 dan nilai p-value lebih besar dari 0,05, maka H0 diterima dan H1 ditolak. Hasil ini menunjukkan bahwa keamanan siber tidak berpengaruh signifikan terhadap laporan keuangan BSI. Hal ini berbeda dengan penelitian terdahulu yang mengungkapkan bahwa penerapan keamanan siber yang baik dapat meningkatkan transparansi informasi dan menurunkan biaya audit internal. (Alhassan et al., 2019a) Dalam kasus BSI, kemungkinan keamanan siber belum sepenuhnya teintegrasi ke dalam sistem pelaporan keuangan, terlebih adanya insiden BSI Error 2023 memperlihatkan adanya celah yang masih perlu diperbaiki.

2) Pengaruh Transparansi terhadap Laporan Keuangan di BSI

Hipotesis yang diuji adalah:

H0 : Transparansi tidak berpengaruh signifikan terhadap Laporan Keuangan di BSI

H2 : Transparansi berpengaruh signifikan terhadap Laporan Keuangan di BSI

Hasil uji dan pembahasan : Berdasarkan hasil analisis, diperoleh nilai T-hitung sebesar 4,381 untuk variable transparansi (X2) dengan tingkat signifikansi 0,000. Karena T-hitung lebih besar dari T-tabel 1,992 dan nilai p-value lebih kecil dari 0,05, maka H0 ditolak dan H2 diterima. Hasil ini memperlihatkan bahwa transparansi berpengaruh positif dan signifikan terhadap laporan keuangan di BSI. Temuan ini sejalan dengan penelitian terdahulu yang menyatakan bahwa transparansi mampu meningkatkan kepercayaan stakeholder terhadap perusahaan. (Eka Puspita Sari, Aprih Santoso, 2021)

3) Dampak Akuntabilitas Terhadap Laporan Keuangan di BSI

Hipotesis yang diuji adalah:

H0 : Akuntabilitas tidak berpengaruh signifikan terhadap Laporan Keuangan di BSI

H3 : Akuntabilitas berpengaruh signifikan terhadap Laporan Keuangan di BSI

Hasil uji dan pembahasan : berdasarkan hasil penelitian, diperoleh nilai T-hitung sebesar 3,593 untuk variabel akuntabilitas (X3) dengan tingkat signifikansi 0,001. Karena T-hitung lebih besar dari T-tabel 1,992 dan nilai p-value lebih kecil dari 0,05, maka H0 ditolak dan H3 diterima. Ini berarti bahwa akuntabilitas memiliki pengaruh positif dan signifikan terhadap laporan keuangan di BSI. Temuan ini konsisten dengan hasil penelitian terdahulu yang menekankan bahwa akuntabilitas tinggi berhubungan erat dengan peningkatan kinerja organisasi dan menyatakan juga bahwa akuntabilitas dapat meningkatkan kualitas laporan keuangan dan memperkuat legitimasi perusahaan di mata publik. (Zubaidah & Nugraeni, 2023)

IV. SIMPULAN

Hasil penelitian menunjukkan bahwa hipotesis teruji dan peran keamanan siber tidak berpengaruh signifikan terhadap laporan tahunan Bank Syariah Indonesia. Hal ini menunjukkan bahwa meskipun langkah-langkah keamanan siber telah diterapkan dengan baik, Bank Syariah Indonesia perlu memperkuat kebijakan dan implementasi keamanan siber untuk mendukung transparansi dan tanggung jawab dalam laporan tahunannya. Di sisi lain, penulis menyarankan agar penelitian selanjutnya membandingkan dampak keamanan siber pada Bank Syariah Indonesia dengan bank syariah lainnya agar memperoleh gambaran yang lebih komprehensif dan mendalam.

V. DAFTAR PUSTAKA

- Akhta, S., Sheorey, P. A., Bhattacharya, S., & Ajith, K. V. V. (2021). Cyber security solutions for businesses in financial services: Challenges, opportunities, and the way Forward. *International Journal of Business Intelligence Research*, 12(1), 82–97. <https://doi.org/10.4018/IJBIR.20210101.0a5>
- Alhassan, I., Sammon, D., & Daly, M. (2019a). Critical Success Factors for Data Governance : A Theory Building Approach. *Information Systems Management*, 0(0), 1–13. <https://doi.org/10.1080/10580530.2019.1589670>
- Alhassan, I., Sammon, D., & Daly, M. (2019b). Critical Success Factors for Data Governance: A Theory Building Approach. *Information Systems Management*, 36(2), 98–110. <https://doi.org/10.1080/10580530.2019.1589670>
- Azzahra, N. S., Tambunan, A. M., Aulia, N. N., Binarsih, A., & Saepudin, T. H. (2024). Tinjauan Literatur Tentang Ancaman Cybercrime Dan Implementasi Keamanan Siber Di Industri Perbankan. *HUMANITIS: Jurnal Humaniora, Sosial Dan Bisnis*, 2(7), 692–700.
- Bryman, A. (2012). *Social research methods*. 809.
- Cahyono, G. J., & Hastuti, T. D. (2024). *The Impact of Competence , Accountability , Professional Skills , and Professional Skepticism on Audit Quality with Time Budget Pressure as a Moderating Variable*. 07(07), 4106–4126. <https://doi.org/10.47191/jefms/v7-i7-28>
- Direktorat Operasi Keamanan Siber, & Negara, B. S. D. S. (2022). Laporan Tahunan Monitoring Keamanan Siber. *Direktorat Operasi Keamanan Siber Badan Siber Dan Sandi Negara*, 1–236. <https://cloud.bssn.go.id/s/Lyw8E4LxwNiJoNw>
- Eka Puspita Sari, Aprih Santoso. (2021). The Role of Financial Literacy as One of the Influences of Financial Behavior. *Jurnal Manajemen*, 25(3), 415. <https://doi.org/10.24912/jm.v25i3.758>
- Fitria, K. M. (2023). Analisis Serangan Malware Dalam Perbankan Dan Perencanaan Solusi Keamanan. *Jurnal Informatika Dan Teknik Elektro Terapan*, 11(3).

- <https://doi.org/10.23960/jitet.v1i13.3312>
- Ghozali, I. (2011). *Ghozali Imam 2011 Aplikasi Analisis Mult.pdf* (p. 129).
- Hanisa, M., Wahyuningsih, T. L., Atriani, D., & Alif, P. (2024). Media Hukum Indonesia (MHI) Analisis Hukum Terhadap Kurangnya Transparansi Serta Akuntabilitas Pelaporan Keuangan Dalam Suatu Perusahaan Media Hukum Indonesia (MHI). *Media Hukum Indonesia (MHI) Published by Yayasan Daarul Huda Krueng Mane*, 2(3), 88–94.
- ISO 27001. (2013). *Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan Information technology – Security techniques – Information security management systems – Requirements*. 54.
- Republik Indonesia. (2008). Undang-Undang tentang Informasi dan Transaksi Elektronik. *Bi.Go.Id, September*, 1–2. <https://peraturan.bpk.go.id/Home/Details/37589/uu-no-11-tahun-2008>
- Saputra, M. G. (2023). Analisis Dampak Laporan Keuangan Yang Transparan Terhadap Keputusan Investasi Saham. *Jurnal Ilmiah Manajemen, Ekonomi, & Akuntansi (MEA)*, 7(3), 1162–1175. <https://doi.org/10.31955/mea.v7i3.3508>
- Swajati, W. G. (2019). Strategi Implementasi Regulasi Perlindungan Data Pribadi di Indonesia. *Indonesiana*, 1–26. <https://www.indonesiana.id/read/68772/urgensi-regulasipelindungan-data-pribadi-di-indonesia>
- Verma, S., Sharma, J., Kaushik, K., & Vyas, V. (2022). Mounting cases of cyber-attacks and digital payment. *Cybersecurity Issues, Challenges, and Solutions in the Business World*, 59–80. <https://doi.org/10.4018/978-1-6684-5827-3.ch005>
- Wibowo, M. H., & Fatimah, N. (2017). Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime. *JoEICT (Journal of Education And ICT)*, 1(1), 1–5. <https://jurnal.stkipgritlungagung.ac.id/index.php/joeict/article/view/69>
- Zubaidah, A. N., & Nugraeni, N. (2023). Pengaruh Akuntabilitas Dan Transparansi Terhadap Kualitas Laporan Keuangan Pada Pemerintah Kabupaten Sleman. *Jurnal Ilmiah Manajemen, Ekonomi, & Akuntansi (MEA)*, 7(3), 978–988. <https://doi.org/10.31955/mea.v7i3.3475>