JURNAL Ekonomi Manajemen Akuntansi Keuangan Bisnis Digital
JEMAK-BD

Pengaruh Peran Audit Dan Sistem Pengendalian Internal (SPI) Terhadap Risiko *Cyber Security*

The Influence Of The Role Of Audit And Internal Control System (ICS) On Cyber Security Risk

Indah Widia Rahma*, Nina Yulianasri, Winny Lian Seventeen
Fakultas Ekonomi dan Bisnis, Universitas Prof. Dr. Hazairin, SH
*Coresponding Email: indahwidiar20@gmail.com

Article history: Submitted: May 11, 2025 | Revised: June 18, 2025 | Accepted: July 02, 2025

Abstrak

Meningkatnya ancaman keamanan siber pada sektor jasa keuangan menuntut perusahaan memiliki sistem pertahanan digital yang kuat. Penelitian ini bertujuan untuk menganalisis pengaruh peran audit internal dan sistem pengendalian internal (SPI) terhadap risiko cyber security. Metode yang digunakan adalah pendekatan kuantitatif dengan desain asosiatif, melalui penyebaran kuesioner kepada 70 responden di PT Jasa Raharja Cabang Bengkulu dan dianalisis menggunakan regresi linier berganda. Hasil penelitian menunjukkan bahwa peran audit dan SPI berpengaruh signifikan terhadap risiko cyber security, baik secara parsial maupun simultan. Temuan ini menunjukkan bahwa integrasi antara audit dan pengendalian internal dapat menjadi langkah strategis untuk meminimalkan ancaman siber, khususnya pada lembaga keuangan non-bank di wilayah dengan keterbatasan infrastruktur digital.

Kata Kunci : Audit Internal, Sistem Pengendalian Internal, Risiko Cyber Security, Keamanan Siber.

Abstract

The increasing cyber threats in the financial services sector demand organizations to establish strong digital defenses. This study aims to analyze the influence of the audit role and internal control system (ICS) on cyber security risk. The method employed a quantitative approach with an associative design, using questionnaires distributed to 70 respondents at PT Jasa Raharja Bengkulu Branch, and analyzed with multiple linear regression. The results show that both audit role and ICS significantly affect cyber security risk, both partially and simultaneously. These findings suggest that integrating audit and ICS is a strategic approach to minimize cyber threats, especially in non-bank financial institutions operating in digitally underdeveloped regions.

Keywords : Internal Audit, Internal Control System, Cyber Security Risk, Cybersecurity

Pendahuluan

Perkembangan teknologi digital dalam sektor keuangan telah menciptakan tantangan baru yang kompleks, terutama dalam hal keamanan informasi dan perlindungan data. Seiring dengan semakin terintegrasinya sistem informasi dalam operasional organisasi, ancaman terhadap keamanan siber (cyber security) pun meningkat secara signifikan. Berdasarkan data dari BSSN., (2024), sepanjang tahun 2023 tercatat lebih dari 400 juta insiden anomali trafik siber di Indonesia, yang menandakan bahwa isu cyber security telah menjadi perhatian nasional yang mendesak dalam konteks pengelolaan risiko digital.

EISSN 2961-9394

Volume : 4
Nomor : 2
Bulan : July-December
Tahun : 2025
Halaman : 355-368

Institusi keuangan non-bank seperti perusahaan asuransi sosial memainkan peran penting dalam memberikan perlindungan finansial kepada masyarakat, termasuk dalam hal penanganan risiko kecelakaan. Salah satu contoh adalah PT Jasa Raharja Bengkulu, yang telah menunjukkan komitmen tinggi dalam menjalankan pelayanan berbasis digital guna meningkatkan efisiensi dan transparansi. Namun, seiring dengan meningkatnya ketergantungan pada sistem informasi dan teknologi digital, perusahaan juga menghadapi tantangan baru dalam menjaga keamanan data dan sistemnya. Tantangan tersebut tidak hanya bersifat teknis, tetapi juga menyangkut kebutuhan akan sistem pengawasan dan pengendalian internal yang adaptif terhadap dinamika ancaman siber yang terus berkembang.

Dalam konteks manajemen risiko organisasi, audit internal dan sistem pengendalian internal (SPI) merupakan dua komponen utama yang dapat digunakan sebagai alat mitigasi terhadap risiko cyber security. Audit internal memiliki fungsi untuk mengevaluasi dan memastikan efektivitas sistem pengendalian dan manajemen risiko dalam organisasi. Sementara itu, SPI menyediakan kerangka kerja struktural yang bertujuan untuk mendeteksi, mencegah, dan merespons berbagai bentuk ancaman terhadap sistem informasi perusahaan.

Namun demikian, literatur empiris yang secara khusus mengkaji keterkaitan antara peran audit, SPI, dan risiko cyber security dalam konteks perusahaan keuangan non-bank daerah masih sangat terbatas. Mayoritas studi sebelumnya lebih terfokus pada sektor perbankan atau institusi di tingkat pusat, sehingga tidak mencerminkan kompleksitas yang dihadapi unit organisasi di tingkat daerah, terutama dalam lingkungan BUMN seperti PT Jasa Raharja.

Berdasarkan gap tersebut, artikel ini bertujuan untuk memberikan kontribusi empiris terhadap kajian akuntansi dan manajemen risiko, khususnya dengan mengevaluasi secara sistematis pengaruh audit internal dan sistem pengendalian internal terhadap risiko cyber security. Penelitian ini diharapkan dapat memberikan wawasan baru bagi praktisi dan akademisi mengenai pentingnya penguatan fungsi audit dan pengendalian internal dalam membangun ketahanan digital organisasi, terutama di sektor publik dan institusi yang sedang dalam proses transformasi digital.

.

Landasan Teori

Teori *Agency*

Teori *Agency* diperkenalkan oleh Jensen dan Meckling yang menggambarkan hubungan antara *principal* (pemilik) dan *agent* (manajer). Hubungan ini penuh dengan potensi konflik kepentingan akibat asimetri informasi, di mana *agent* dapat bertindak untuk kepentingan pribadinya yang tidak selalu sejalan dengan tujuan *principal*. Dalam konteks keamanan siber, lemahnya sistem audit dan pengendalian internal dapat memperbesar ruang bagi perilaku *oportunistik agent*, seperti kelalaian dalam pengelolaan keamanan informasi (Prasetyo & Sanjaya, 2020 hal. 123-135)

Teori Pengendalian Internal (COSO *Framework*)

Kerangka COSO (2013) dalam Kirana, (2017 hal. 4) menyatakan bahwa pengendalian internal adalah proses yang dirancang untuk memberikan keyakinan memadai terhadap pencapaian tujuan operasional, pelaporan keuangan, dan kepatuhan terhadap regulasi. COSO membagi pengendalian internal ke dalam lima komponen utama : (1) lingkungan pengendalian, (2) penilaian risiko, (3) aktivitas pengendalian, (4) informasi dan komunikasi, serta (5) pemantauan. Dalam konteks keamanan siber, Sistem Pengendalian Internal (SPI) bertindak sebagai alat manajerial yang sistematis untuk mencegah kebocoran data, meminimalkan kesalahan operasional, dan menanggulangi serangan digital (Hasanah & Siregar, 2020).

Teori Manajemen Risiko (*Risk Management Theory*)

Teori ini menekankan pentingnya pendekatan sistematis dalam mengidentifikasi, menilai, merespons, dan memantau risiko, termasuk yang bersifat digital (ISO 31000:2018). Dalam perusahaan berbasis teknologi, **risiko cyber security** termasuk dalam kategori risiko operasional yang harus dikelola secara aktif dan berkelanjutan. Manajemen risiko siber yang efektif mengharuskan organisasi memiliki sistem deteksi dini, protokol respons insiden, dan kebijakan keamanan informasi yang sesuai standar seperti ISO 27001 (Ningsih, 2024).

Audit Internal

Audit internal adalah proses sistematis, independen, dan objektif yang dirancang untuk mengevaluasi dan meningkatkan efektivitas manajemen risiko, pengendalian, dan tata kelola organisasi (IIA, 2021). Dalam konteks cyber security, audit internal tidak hanya mencakup audit keuangan, tetapi juga audit sistem informasi, audit kepatuhan, dan evaluasi pengendalian teknologi. Indikator Audit Internal: Independensi auditor, Kompetensi auditor TI, Risk-based auditing, Frekuensi audit sistem informasi, Implementasi rekomendasi hasil audit (Sudarmanto & Utami, 2021).

Variabel Sistem Pengendalian Internal (SPI)

SPI adalah struktur kebijakan dan prosedur yang dirancang untuk melindungi aset organisasi, menjamin akurasi informasi, serta memastikan kepatuhan terhadap regulasi. Dalam konteks keamanan informasi, SPI mencakup pengendalian akses sistem, segmentasi jaringan, backup data, serta pelatihan berkala kepada pegawai (COSO, 2013) dalam (Kirana, 2017 hal. 4). Indikator SPI: Efektivitas lingkungan pengendalian, Penilaian risiko siber secara berkala, Kepatuhan terhadap prosedur pengendalian, Efisiensi komunikasi informasi digital, Kualitas pemantauan sistem kontrol (Adiputra, dkk., 2018).

Risiko *Cyber Security*

Risiko *cyber security* merujuk pada potensi ancaman terhadap integritas, kerahasiaan, dan ketersediaan data akibat insiden digital seperti serangan malware, ransomware, phishing, atau kesalahan manusia. Risiko ini dapat menyebabkan gangguan operasional, kerugian finansial, hingga kerusakan reputasi (Putra, A. R., & Sari, 2020). Indikator Risiko *Cyber Security*: Frekuensi insiden keamanan, Tingkat kebocoran data, Efektivitas respons insiden, Kepatuhan terhadap kebijakan keamanan informasi, Gangguan operasional akibat serangan siber (Ningsih, 2024).

EISSN 2961-9394

Volume : 4
Nomor : 2
Bulan : July-December
Tahun : 2025
Halaman : 355-368

Metode

Penelitian ini menggunakan pendekatan kuantitatif dengan desain asosiatif untuk menguji hubungan antara peran audit, sistem pengendalian internal (SPI), dan risiko cyber security. Analisis dilakukan terhadap data primer yang diperoleh dari 70 responden tetap di PT Jasa Raharja Bengkulu menggunakan instrumen kuesioner tertutup berbasis skala Likert. Teknik analisis data yang digunakan adalah regresi linier berganda untuk menguji pengaruh simultan dan parsial antar variabel, dengan pengujian hipotesis berbasis nilai signifikansi ($\alpha = 0,05$). Sebelum dilakukan regresi, data diuji terlebih dahulu menggunakan uji validitas dan reliabilitas untuk memastikan kualitas instrumen, serta diuji asumsi klasik (uji normalitas, multikolinearitas, heteroskedastisitas) sebagai syarat kelayakan model regresi.

Hasil dan Pembahasan

Uji Validitas

Pengujian validitas dilakukan untuk mengukur sah atau valid tidaknya suatu kuesioner dari masing-masing variabel. Hasil uji validitas dalam penelitian ini dapat dilihat pada tabel berikut :

Tabel 1. Hasil Uji Validitas

No	Variabel	R Hitung	R Tabel	Keterangan
1	Peran Audit			
	Pernyataan 1	0,788	0,2352	Valid
	Pernyataan 2	0,764	0,2352	Valid
	Pernyataan 3	0,672	0,2352	Valid
	Pernyataan 4	0,799	0,2352	Valid
	Pernyataan 5	0,830	0,2352	Valid
2	Sistem Pengendalian Internal (SPI)			
	Pernyataan 1	0,725	0,2352	Valid
	Pernyataan 2	0,867	0,2352	Valid
	Pernyataan 3	0,693	0,2352	Valid
	Pernyataan 4	0,862	0,2352	Valid
	Pernyataan 5	0,808	0,2352	Valid
3	Risiko *Cyber security*			
	Pernyataan 1	0,907	0,2352	Valid
	Pernyataan 2	0,912	0,2352	Valid
	Pernyataan 3	0,458	0,2352	Valid
	Pernyataan 4	0,718	0,2352	Valid
	Pernyataan 5	0,900	0,2352	Valid

Berdasarkan tabel 1 dapat dilihat semua pertanyaan dalam kuesioner dikatakan valid dikarenakan tingkat signifikannya yaitu r hitung > r tabel. Dimana pada variabel peran audit (X_1) berada pada nilai 0,672 sampai 0,830. Variabel Sistem Pengendalian Internal (SPI) (X_2) berada di nilai 0,693 sampai nilai 0,867. Dan pada variabel Risiko *Cyber security* (Y) berada pada nilai 0,458 sampai 0,912.

Uji Reliabilitas

Suatu kuesioner dikatakan reliabel atau handal jika jawaban seseorang terhadap pernyataan adalah konsisten atau stabil dari waktu ke waktu (Ghozali, 2021, hal. 149). Jika nilai koefisien cronbach alpha > 0,70 maka dikatakan reliabel.

Tabel 2. Hasil Uji Reliabilitas

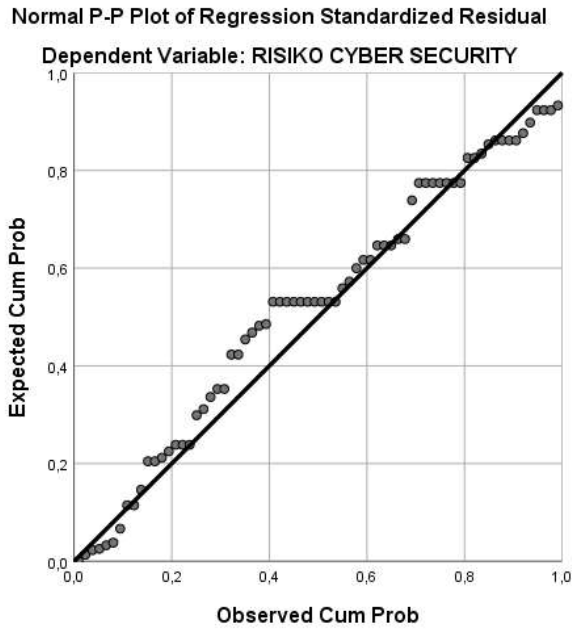
Variabel	***Reliability Statistics***		Keterangan
	Cronbach's Alpha	N of Items	
Peran Audit	0,828	5	Reliabel
Sistem Pengendalian Internal (SPI)	0,848	5	Reliabel
Risiko *Cyber security*	0,836	5	Reliabel

Berdasarkan hasil yang ditampilkan pada Tabel di atas, diketahui bahwa variabel Peran Audit (X1) memiliki nilai Cronbach's Alpha sebesar 0,828, yang berarti lebih besar dari ambang batas 0,70. Dengan demikian, instrumen pengukuran pada variabel X1 dapat dikatakan reliabel. Selanjutnya, variabel Sistem Pengendalian Internal (SPI) (X2) memiliki nilai Cronbach's Alpha sebesar 0,848, yang juga melebihi nilai minimum yang ditetapkan, sehingga instrumen X2 dinyatakan reliabel. Adapun variabel Risiko *Cyber security* (Y) menunjukkan nilai Cronbach's Alpha sebesar 0,836, yang kembali menunjukkan angka di atas 0,70, sehingga instrumen yang digunakan untuk mengukur variabel Y juga dinyatakan reliabel.

Uji Asumsi Klasik

Uji Normalitas

Menurut Ghozali, (2021, hal. 161) uji normalitas dilakukan untuk menguji apakah dalam model regresi, variabel pengganggu atau residual memiliki distribusi yang normal atau tidak normal. Pengujian normalitas dengan metode grafik normal Probability Plots berikut :



Gambar 1. Uji Normalitas P-Plot Regresi

EISSN 2961-9394

Volume : 4
Nomor : 2
Bulan : July-December
Tahun : 2025
Halaman : 355-368

Dari gambar 1. di atas dapat dilihat bahwa pada grafik normal plot terlihat titik-titik atau data menyebar disekitaran garis diagonal dan mengikuti arah garis diagonal, maka dapat disimpulkan bahwa model regresi memenuhi asumsi normalitas.

Uji Multikolinearitas

Model regresi yang baik seharusnya tidak terjadi korelasi di antara variabel independen. Untuk mendeteksi ada atau tidaknya multikolinieritas di dalam model regresi adalah dengan nilai Variance Inflation Factor (VIF) kurang dari 10 (Ghozali, 2021, hal. 165). Dan menggunakan nilai tolerance lebih dari 0,1 atau mendekati 1.

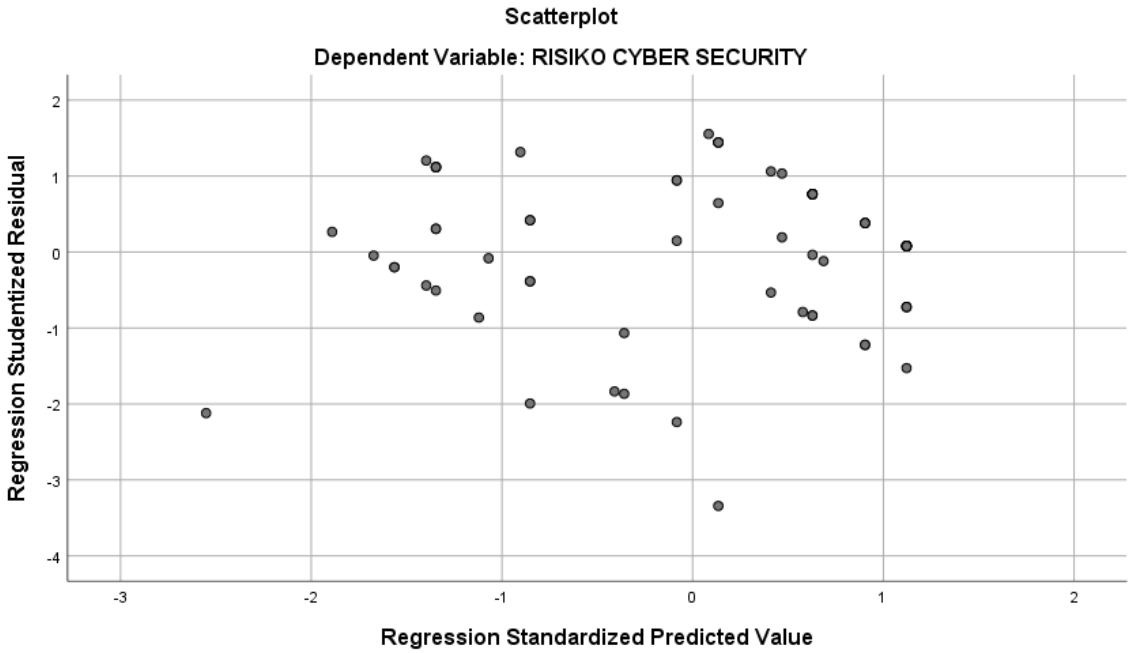
Tabel 3. Hasil Uji Multikolinearitas

Variabel	*collinearity statistics*	
	Tolerance	VIF
Peran Audit	0,998	1,002
Sistem Pengendalian Internal (SPI)	0,998	1,002

Berdasarkan data di atas, nilai tolerance untuk variabel Peran Audit (X1) sebesar 0,998 dan untuk variabel Sistem Pengendalian Internal (SPI) (X2) juga sebesar 0,998. Kedua nilai tersebut lebih besar dari 0,1 atau mendekati angka 1, yang menunjukkan tidak adanya indikasi multikolinearitas. Selain itu, nilai Variance Inflation Factor (VIF) untuk Peran Audit (X1) adalah 1,002, dan untuk SPI (X2) juga sebesar 1,002. Karena kedua nilai VIF tersebut kurang dari 10, maka dapat disimpulkan bahwa tidak terdapat multikolinearitas antar variabel independen dalam model regresi ini, sehingga variabel-variabel tersebut layak digunakan dalam penelitian.

Uji Heteroskedastisitas

Pengujian heteroskedastisitas dapat dengan melihat grafik scatter plot dan diperkuat dengan pengujian uji park, yaitu apabila variabel independen memiliki nilai tingkat signifikansi melebihi 0,05 sehingga dapat disimpulkan tidak terjadi gejala heteroskedastisitas dalam model regresi penelitian



Gambar 2. Uji Heterokedastisitas Scatter Plot

Berdasarkan gambar scatter plot di atas, terlihat bahwa titik-titik data menyebar secara acak di atas dan di bawah garis nol pada sumbu Y, tanpa membentuk pola tertentu. Hal ini mengindikasikan bahwa tidak terjadi gejala heteroskedastisitas dalam model regresi. Temuan ini diperkuat dengan hasil uji Park, yang disajikan pada tabel berikut:

Tabel 4. Uji Park

Variabel	*Coeffisients*	
	T	Sig
Peran Audit	-1,664	0,101
Sistem Pengendalian Internal (SPI)	-0,717	0,476

Dari tabel 4 dapat di lihat bahwa variabel Peran Audit (X_1) mempunyai nilai signifikansi 0,101, Sistem Pengendalian Internal (SPI) (X_2) memiliki nilai signifikan 0,476, dan nilai signifikan lebih dari 0,05 sehingga data penelitian tidak mengandung gejala heteroskedastisitas dan dianggap memenuhi asumsi klasik.

Analisis Regresi Linier Berganda

Uji regresi linier berganda ini yaitu regresi yang digunakan untuk mengetahui seberapa besar pengaruh variabel independen terhadap variabel dependen

.

EISSN 2961-9394

Volume : 4
Nomor : 2
Bulan : July-December
Tahun : 2025
Halaman : 355-368

Tabel 5. Hasil Regresi Linier Berganda

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	-1,206	2,524		-,478	,634
	Peran Audit	,856	,078	,785	10,980	,000
	Sistem Pengendalian Internal (Spi)	,189	,078	,172	2,411	,019
a. Dependent Variable: Risiko *Cyber security*						

Berdasarkan hasil analisis data diatas, maka didapatkan persamaan regresi linier berganda sebagai berikut :

$$\boldsymbol{Y = a + \beta 1 X_1 + \beta 2 X_2 + e}$$

Y = -1,206+ 0,856 + 0,189+ e

Keterangan dari persamaan di atas yaitu :

a. Nilai a sebesar -1,206 merupakan konstanta atau keadaan saat variabel Risiko *Cyber security* belum dipengaruhi oleh variabel lainnya yaitu Peran Audit (X_1), Sistem Pengendalian Internal (SPI) (X_2). Jika variabel independen tidak ada maka variabel Risiko *Cyber security* tidak mengalami perubahan.
b. Nilai koefisien regresi X_1 sebesar 0,856 menunjukkan bahwa variabel Peran Audit mempunyai pengaruh signifikan terhadap Risiko *Cyber security* yang berarti bahwa setiap kenaikan satu satuan variabel Peran Audit, maka akan mempengaruhi pengelolaan keuangan sebesar 0,856. Dengan asumsi bahwa variabel bebas lainnya bernilai tetap.
c. Nilai koefisien regresi X_2 sebesar 0,189 menunjukkan bahwa variabel Sitem Pengendalian Internal (SPI) mempunyai pengaruh signifikan terhadap Risiko *Cyber security* yang berarti bahwa setiap kenaikan satu satuan Sitem Pengendalian Internal (SPI), maka akan mempemgaruhi kinerja Risiko *Cyber security* 0,189. Dengan asumsi bahwa variabel bebas lainnya bernilai tetap.

Pengujian Hipotesis

Uji Parsial (Uji T)

Pengujian uji t digunakan untuk mengetahui kemampuan dari masing-masing variabel dalam mempengaruhi variabel dependen (Ghozali, 2021, hal. 144). Uji t digunakan untuk mengetahui seberapa jauh pengaruh variabel independen pada penelitian ini secara individual dalam menerangkan variasi variabel dependen.

Tabel 6. Hasil Uji Parsial (Uji T)

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	-1,206	2,524		-,478	,634
	Peran Audit	,856	,078	,785	10,980	,000
	Sistem Pengendalian Internal (SPI)	,189	,078	,172	2,411	,019
a. Dependent Variable: Risiko *Cyber security*						

1. Uji hipotesis 1 (H_1)
   Hasil uji hipotesis 1 dapat dilihat pada tabel diatas menunjukan bahwa nilai sginifikasi pengaruh Peran Audit (X_1) terhadap Risiko *Cyber security* adalah 0,001 < 0,05 dan nilai t hitung 10,980 > nilai t tabel 1,996. Maka H_0 ditolak dan H_1 diterima, Sehingga dapat disimpulkan bahwa variabel Peran Audit (X_1) berpengaruh signifikan terhadap Risiko *Cyber security* (Y).
2. Uji hipotesis 2 (H_2)
   Hasil uji hipotesis 2 dapat dilihat pada tabel diatas menunjukan bahwa nilai sginifikasi pengaruh Sistem Pengendalian Internal (SPI) (X_2) terhadap Risiko *Cyber security* adalah 0,003 < 0,05 dan nilai t hitung 2,411> nilai t tabel 1,996. Maka H_0 ditolak dan H_2 diterima, Sehingga dapat disimpulkan bahwa variabel Sistem Pengendalian Internal (SPI) (X_2) berpengaruh signifikan terhadap Risiko *Cyber security* (Y).

Uji Simultan (Uji F)

Uji simultan F (Uji Simultan) digunakan untuk mengetahui ada atau tidaknya pengaruh secara bersama-sama atau simultan antara variabel independen terhadap variabel dependen (Ghozali, 2021, hal. 148).

Tabel 7. Hasil Uji Simultan (Uji F)

Model		*Sum of Squares*	df	*Mean Square*	F	Sig.
1	*Regression*	207,311	2	103,655	64,567	,000[b]
	Residual	107,561	67	1,605		
	Total	314,871	69			
a. *Dependent Variable*: Risiko *Cyber security*						
b. *Predictors: (Constant),* Sistem Pengendalian Internal (SPI), Peran Audit						

Berdasarkan tabel diatas menunjukkan bahwa nilai f_{hitung} sebesar 64,567, dimana nilai ini lebih besar dari nilai f_{tabel} yang ditentukkan. Nilai signifikansinya sebesar 0,000 dimana nilai ini lebih kecil dari nilai alpha. Hal ini menunjukkan bahwa H_3 diterima atau variabel Peran Audit (X_1), dan Sistem Pengendalian Internal (SPI) (X_2) berpengaruh signifikan secara simultan terhadap Pengelolaan Keuangan (Y).

Uji Koefisien Determinasi (R2)

Menurut Agus Widarjono (2017, hal. 79), Uji koefisien determinasi (R-Squared) adalah uji untuk menjelaskan besaran proporsi variasi dari variabel dependen yang dijelaskan oleh variabel independen.

Tabel 8. Hasil Uji Koefisien Determinasi (R2)

Model Summary[b]				
Model	R	*R Square*	*Adjusted R Square*	*Std. Error of the Estimate*
1	,811[a]	,658	,648	1,267
a. *Predictors: (Constant*), Sistem Pengendalian Internal (Spi), Peran Audit				
b. *Dependent Variable*: Risiko *Cyber security*				

EISSN 2961-9394

Volume : 4
Nomor : 2
Bulan : July-December
Tahun : 2025
Halaman : 355-368

Tabel 8 menunjukan nilai koefisien determinasi sebesar 0,648. Angka tersebut memiliki arti bahwa variabel indenpenden secara bersama-sama memberikan sumbangan sebesar 64,8% dalam mempengaruhi variabel dependen, sedangkan 35,2% lainnya dipengaruhi variabel lain yang tidak diketahui oleh peneliti.

Pembahasan

Pembahasan Variabel Peran Audit terhadap Risiko Cyber Security

Hasil penelitian menunjukkan bahwa peran audit memiliki pengaruh signifikan terhadap risiko cyber security. Temuan ini sejalan dengan teori agensi yang menyatakan bahwa keberadaan fungsi audit internal yang independen dan kompeten mampu memitigasi potensi perilaku oportunistik dalam organisasi, termasuk dalam pengelolaan sistem informasi. Auditor internal yang menjalankan fungsi risk-based auditing secara aktif dapat mengidentifikasi celah keamanan informasi, menilai kepatuhan terhadap kebijakan teknologi informasi, serta memberikan rekomendasi preventif untuk meningkatkan resiliensi siber. Di lingkungan PT Jasa Raharja Bengkulu, fungsi audit internal terbukti berperan dalam mengevaluasi kontrol akses data, pemantauan jaringan, serta kebijakan backup data, yang kesemuanya berkontribusi dalam menurunkan eksposur risiko digital.

Dari sisi statistik, hasil uji regresi linier menunjukkan bahwa peran audit memiliki nilai signifikansi di bawah 0,05, yang menandakan hubungan yang kuat dan signifikan secara parsial terhadap variabel risiko cyber security. Ini menegaskan bahwa organisasi dengan audit internal yang aktif dan terlatih dalam bidang keamanan informasi lebih siap dalam menghadapi ancaman siber yang dinamis. Selain itu, hasil ini mendukung temuan Sherina Darmawati (2022) yang menyebutkan bahwa sertifikasi dan kapasitas auditor internal berdampak langsung terhadap efektivitas perlindungan siber. Dengan demikian, pembentukan unit audit yang fokus pada aspek teknologi informasi menjadi kebutuhan mendesak, khususnya bagi entitas non-bank di daerah yang sedang beradaptasi dengan transformasi digital.

Sistem Pengendalian Internal (SPI) terhadap Risiko Cyber Security

Temuan penelitian juga menunjukkan bahwa sistem pengendalian internal (SPI) berpengaruh signifikan terhadap risiko cyber security. Dalam konteks teori COSO, SPI berfungsi sebagai kerangka kerja menyeluruh yang mencakup penilaian risiko, aktivitas pengendalian, serta pemantauan berkelanjutan atas prosedur keamanan informasi. Di PT Jasa Raharja Bengkulu, indikator SPI seperti efektivitas lingkungan pengendalian, kualitas penilaian risiko, dan kepatuhan terhadap kebijakan IT menjadi faktor utama dalam menekan ancaman digital seperti kebocoran data, ransomware, dan serangan phishing. Hal ini membuktikan bahwa penerapan SPI yang konsisten mampu meningkatkan integritas dan ketersediaan sistem digital perusahaan.

Dari analisis regresi, variabel SPI memiliki nilai signifikansi <0,05, yang menunjukkan adanya pengaruh positif dan signifikan secara parsial terhadap penurunan risiko cyber security. Hasil ini mendukung teori manajemen risiko yang menekankan pentingnya integrasi sistem kontrol internal dengan proses mitigasi risiko digital. Penelitian ini juga memperkuat hasil studi Hasanah dan Siregar (2020) yang menyatakan bahwa implementasi SPI yang baik mampu mengurangi peluang kegagalan

sistem informasi akibat serangan siber. Oleh karena itu, penting bagi perusahaan untuk terus memperbarui sistem kontrol internal, meningkatkan literasi keamanan TI di semua level, serta membangun budaya kepatuhan terhadap kebijakan keamanan digital sebagai strategi utama pertahanan siber.

Peran Audit dan SPI terhadap Risiko Cyber Security

Hasil uji simultan menunjukkan bahwa peran audit dan sistem pengendalian internal (SPI) secara bersama-sama berpengaruh signifikan terhadap risiko cyber security pada PT Jasa Raharja Bengkulu. Nilai signifikansi yang diperoleh berada di bawah 0,05 dan nilai koefisien determinasi (R^2) sebesar 65,8% menunjukkan bahwa kedua variabel ini secara kolektif mampu menjelaskan sebagian besar variasi dalam risiko siber yang dihadapi perusahaan. Hal ini memperlihatkan bahwa efektivitas pengendalian keamanan siber tidak hanya ditentukan oleh satu mekanisme pengawasan, tetapi memerlukan sinergi antara fungsi audit internal sebagai entitas evaluatif dan SPI sebagai sistem pengendali operasional. Keduanya berkontribusi menciptakan pertahanan berlapis yang mampu mendeteksi, mencegah, dan merespons ancaman digital secara proaktif.

Temuan ini secara teoritis didukung oleh kerangka COSO dan teori manajemen risiko, di mana fungsi audit dan SPI harus terintegrasi dalam siklus pengelolaan risiko untuk menjamin keberlanjutan organisasi. Audit internal berperan dalam menilai dan meningkatkan efektivitas SPI, sedangkan SPI menyediakan kontrol dan prosedur yang dijadikan objek evaluasi audit. Di PT Jasa Raharja, kolaborasi antara auditor internal dan pengelola sistem informasi membentuk sistem umpan balik yang adaptif terhadap potensi serangan siber. Dengan demikian, penguatan keduanya secara simultan bukan hanya memperkecil kemungkinan insiden keamanan, tetapi juga meningkatkan kepercayaan stakeholder terhadap tata kelola teknologi dan keamanan informasi perusahaan, terutama di tengah meningkatnya serangan digital di sektor keuangan non-bank.

Simpulan

Penelitian ini menyimpulkan bahwa peran audit dan sistem pengendalian internal (SPI) memiliki kontribusi nyata dalam menurunkan risiko cyber security, baik secara parsial maupun simultan. Temuan ini tidak hanya menunjukkan signifikansi statistik, tetapi juga menegaskan pentingnya sinergi dua pilar pengawasan organisasi dalam menghadapi kompleksitas ancaman digital yang semakin berkembang, khususnya di sektor jasa keuangan non-bank seperti PT Jasa Raharja Bengkulu. Dengan mengacu pada teori agensi, COSO framework, dan teori manajemen risiko, penelitian ini memperlihatkan bahwa tata kelola yang didukung oleh audit internal yang independen dan sistem pengendalian internal yang efektif merupakan strategi fundamental dalam menciptakan ketahanan digital perusahaan.

Secara lebih luas, hasil penelitian ini membuka ruang bagi pengembangan sistem audit berbasis risiko yang lebih adaptif terhadap dinamika keamanan informasi, serta perlunya pembaruan sistem pengendalian internal yang selaras dengan perkembangan teknologi. Ke depan, pendekatan integratif antara fungsi audit dan pengendalian internal perlu diperluas tidak hanya dalam tataran kebijakan internal, tetapi juga pada pembentukan budaya keamanan informasi di seluruh lini organisasi.

EISSN 2961-9394

Volume : 4
Nomor : 2
Bulan : July-December
Tahun : 2025
Halaman : 355-368

Penelitian ini juga memberikan dasar empirik bagi studi lanjutan dengan cakupan yang lebih luas, baik secara geografis maupun sektoral, serta dapat dikembangkan melalui pendekatan kualitatif untuk mengeksplorasi secara mendalam praktik pengendalian dan respons organisasi terhadap insiden siber. Dengan demikian, hasil penelitian ini tidak hanya bersifat teoritis, tetapi juga aplikatif dalam membangun model pengelolaan risiko cyber yang relevan, khususnya dalam konteks organisasi publik dan BUMN yang sedang bertransformasi digital.

Daftar Rujukan

Adiputra, M. A., Ruwanti, S., & Husna, A. (2018). *Universitas Maritim Raja Ali Haji | 1*. *4*(0771), 7001550. www.idx.co.id.

Agista, G.G., & Mimba, N. P. S. . (2017). Pengaruh Corporate Governance Structure Dan Konsentrasi Kepemilikan Pada Pengungkapan Enterprise Risk Management. *E-Jurnal Akuntansi Universitas Udayana*, *18*(1), 214–239.

Agus Widarjono. (2017). *Ekonometrika Pengantar dan Aplikasinya Disertai Panduan Eviews*. UPP STIM YKPN.

Anathasya Angelia Zeta Junus, Amelia Vernanda, Vanessa Gabriella, & Carmel Meiden. (2022). Audit Operasional Dan Pengendalian Internal Pada Masa Pandemi Terhadap Efektivitas Dan Efisiensi Pengendalian Kinerja Manajemen Di Pt Belvamas Maritim Indontama. *Juremi: Jurnal Riset Ekonomi*, *2*(2), 181–192. https://doi.org/10.53625/juremi.v2i2.3294

Ben Ahmed, D., & Khelil-Rhouma, Z. (2020). The determinants of employee stock ownership: French case. *Corporate Ownership and Control*, *17*(4), 110–116. https://doi.org/10.22495/cocv17i4art9

BSSN. (2024). Laporan Tahunan Keamanan Siber Indonesia 2023. *Badan Siber Dan Sandi Negara.*

Dinata, A., Sutabri, T., Bina, U., Palembang, D., Yani, J. A., Palembang, P., Informatika, M. T., & Darma, U. B. (2019). *Analisis Efektivitas Pengendalian Internal IT Berdasarkan Metode Cobit 2019 1,2,3*. 261–269.

Fatrizia, S., & Arliana, S. A. (2023). SLR : SPI Dan Kecurangan Akuntansi Terhadap Keamanan Data Dalam SIA Di Era BIG DATA. *Jurnal Ilmiah Raflesia Akuntansi*, *9*(2), 47–56. https://doi.org/10.53494/jira.v9i2.234

Ghozali, I. (2021). Aplikasi Analisis Multivariate Dengan Program IBM SPSS 26 Edisi 10. *Badan Penerbit Universitas Diponegoro.*

Hidayat, R., & Sari, D. P. (2019). Peran Audit dalam Meningkatkan Transparansi dan Akuntabilitas Laporan Keuangan. *Jurnal Akuntansi Dan Manajemen*, *11*(2), 123–135.

Hidayat, R. (2020). Peran Sistem Pengendalian Internal dalam Meningkatkan Kinerja Organisasi. *Jurnal Akuntansi Dan Keuangan*, *12*(1), 45–60.

Kirana, A. P. (2017). Pengaruh Komite Manajemen Risiko dan Konsentrasi Kepemilikan Terhadap Enterprise Risk Management. *Universitas Lampung*.

Kurniadi, A. (2019). Audit Dan Norma Pemeriksaan Akuntan. *OSF Preprints*, 8.

Martono, N. (2016). Metode Penelitian Kuantitatif: Analisis Isi Dan Analisis Data Sekunder. *Rajawali Pers.*, *2*.

Ngamal, Y., & Maximus Ali Perajaka. (2021). Penerapan Model Manajemen Risiko

Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia. *Jurnal Manajemen Risiko*, *2*(2), 59–74. https://doi.org/10.33541/mr.v2iiv.4099

Ningsih, R. Y. (2024). Peran dan Potensi Implementasi Audit TI dalam Transformasi Digital Berkelanjutan pada Keuangan Sektor Publik di Indonesia. *Indonesian Journal of Auditing and Accounting*, *1*(1). http://jurnal.iapi.or.id/index.php/ijaa/article/view/45%0Ahttp://jurnal.iapi.or.id/index.php/ijaa/article/download/45/16

Prasetyo, A., & Wibowo, S. (2021). Peran Sistem Pengendalian Internal dalam Mengelola Risiko *Cyber security*. *Jurnal Teknologi Informasi Dan Komunikasi*, *15*(2), 123–135.

Prasetyo, A., & Sanjaya, A. (2020). Analisis Prospek Bisnis BUMN yang Tergabung di IDX BUMN 20 Pasca Kasus Korupsi (Studi Kasus pada PT Waskita Karya, Tbk dan PT Wijaya Karya, Tbk. *Buletin IAMI*, 51–57.

Putra, A. R., & Sari, D. P. (2020). Pengertian dan Pentingnya *Cyber security* dalam Era Digital. *Urnal Teknologi Informasi Dan Komunikasi*, *14*(1), 55–70.

Rani, E. H., & Triani, N. N. A. (2021). Audit Delay of Listed Companies On The IDX. *Jurnal ASET (Akuntansi Riset)*, *13*(1), 12–25. https://doi.org/10.17509/jaset.v13i1.32824

Roussy, M., & Perron, A. (2018). Internal auditors' roles: From watchdogs to helpers and protectors of the top manager. *Critical Perspectives on Accounting*, *49*, 37–52.

Saputra, T. S., & Ismandra, I. (2023). Studi Kualitatif Fungsi Internal Audit dan Manajemen Risiko Dalam Tata Kelola Perguruan Tinggi Swasta. *Mbia*, *21*(3), 334–344. https://doi.org/10.33557/mbia.v21i3.1955

Sari, D. P., & Hidayat, R. (2020). Penerapan Standar Audit Internasional dalam Audit Laporan Keuangan di Indonesia. *Jurnal Akuntansi Dan Keuangan*, *12*(1), 45–60.

Sari, M., Hanum, S., & Rahmayati, R. (2022). Analisis Manajemen Resiko Dalam Penerapan Good Corporate Governance : Studi pada Perusahaan Perbankan di Indonesia. *Owner*, *6*(2), 1540–1554. https://doi.org/10.33395/owner.v6i2.804

Sherina Darmawati. (2020). Audit Internal Berbasis TI dan Efektivitas Pengendalian Keamanan Data. *Jurnal Sistem Informasi Dan Keamanan*, *10*(1), 22–30.

Sherina Darmawati, D. (2022). Pengaruh Auditor Internal dan Kebijakan Manajeman Terhadap Efektivitas Keamanan Siber. *Jurnal Ekonomi Trisakti*, *2*(2), 515–528. https://www.trijurnal.trisakti.ac.id/index.php/jet

Sudarmanto, E., & Utami, C. K. (2021). Pencegahan Fraud Dengan Pengendalian Internal Dalam Perspektif Alquran. *Jurnal Ilmiah Ekonomi Islam*, *7*(1), 195.Adiputra, M. A., Ruwanti, S., & Husna, A. (2018). *Universitas Maritim Raja Ali Haji | 1*. *4*(0771), 7001550. www.idx.co.id.

BSSN. (2024). Laporan Tahunan Keamanan Siber Indonesia 2023. *Badan Siber Dan Sandi Negara*.

Kirana, A. P. (2017). Pengaruh Komite Manajemen Risiko dan Konsentrasi Kepemilikan Terhadap Enterprise Risk Management. *Universitas Lampung*.

Ningsih, R. Y. (2024). Peran dan Potensi Implementasi Audit TI dalam Transformasi Digital Berkelanjutan pada Keuangan Sektor Publik di Indonesia. *Indonesian Journal of Auditing and Accounting*, *1*(1). http://jurnal.iapi.or.id/index.php/ijaa/article/view/45%0Ahttp://jurnal.iapi.or.id/ind

EISSN 2961-9394

Volume : 4
Nomor : 2
Bulan : July-December
Tahun : 2025
Halaman : 355-368

ex.php/ijaa/article/download/45/16

Prasetyo, A., & Sanjaya, A. (2020). Analisis Prospek Bisnis BUMN yang Tergabung di IDX BUMN 20 Pasca Kasus Korupsi (Studi Kasus pada PT Waskita Karya, Tbk dan PT Wijaya Karya, Tbk. *Buletin IAMI*, 51–57.

Putra, A. R., & Sari, D. P. (2020). Pengertian dan Pentingnya Cyber Security dalam Era Digital. *Urnal Teknologi Informasi Dan Komunikasi*, *14*(1), 55–70.

Sudarmanto, E., & Utami, C. K. (2021). Pencegahan Fraud Dengan Pengendalian Internal Dalam Perspektif Alquran. *Jurnal Ilmiah Ekonomi Islam*, *7*(1), 195. https://doi.org/10.29040/jiei.v7i1.1593