Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 4 No. 3 (2025) pp: 1192-1203
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Analisis Pengaruh Literasi Digital, Komitmen Manajemen, Dan Pengendalian Internal Terhadap Ukm *Cyber Preparedness*

Silfi Putri Rahmawati[1]
Fakultas Ekonomika Dan Bisnis, Universitas Negeri Surabaya
silfiputri1113@gmail.com

Abstrak

Penelitian ini bertujuan untuk menganalisis pengaruh literasi digital, komitmen manajemen, dan pengendalian internal terhadap tingkat kesiapan Usaha Kecil dan Menengah (UKM) dalam menghadapi ancaman siber (Cyber Preparedness). Dalam era digital yang semakin berkembang, UKM menjadi target potensial serangan siber karena keterbatasan sumber daya dan sistem keamanan. Penelitian ini menggunakan pendekatan kuantitatif dengan pengumpulan data melalui kuesioner yang disebarkan kepada 100 pelaku UKM yang terdaftar di Dinas Koperasi, UKM dan Perdagangan Kota Surabaya. Hasil penelitian menunjukkan bahwa literasi digital, komitmen manajemen, dan pengendalian internal berpengaruh signifikan terhadap UKM Cyber Preparedness. Temuan ini menekankan pentingnya peningkatan kemampuan digital, peran aktif manajemen, serta penerapan pengendalian internal yang efektif dalam memperkuat ketahanan UKM terhadap risiko serangan siber.

Kata kunci: *Literasi Digital, Komitmen Manajemen, Pengendalian Internal, UKM, Cyber Preparedness.*

1. Latar Belakang

Pada masa perkembangan teknologi digital saat ini, keamanan siber merupakan aspek yang harus diperhatikan oleh Usaha Kecil dan Menengah (UKM). Serangan siber dapat mengancam keutuhan data, merusak citra perusahaan, serta menimbulkan kerugian finansial yang besar D. Novita (2024). Temuan terkini dari Kapersky mengungkapkan bahwa pelaku siber terus menargetkan UKM menggunakan metode yang semakin canggih. Tercatat 43% serangan siber yang terjadi setiap tahun dialami oleh usaha kecil dan menengah (UKM), dan 46% dari serangan siber ini terjadi pada usaha kecil dengan kurang dari 1.000 pekerja (Palatty 2025). Usaha Kecil Menengah (UKM) memegang posisi penting bagi pertumbuhan perekonomi di Indonesia. Selain meningkatkan perekonomian di Indonesia UKM juga memiliki peran dalam menciptakan lapangan kerja dan memperbaiki kesejahteraan rakyat (Vinatra et al., 2023). Menurut data dari Badan Pusat Statistik (BPS), terdapat lebih dari 64 juta UKM di Indonesia yang telah berkontribusi sekitar 60% terhadap PDB nasional, namun baru sekitar 12% di antaranya yang secara optimal memanfaatkan teknologi digital (Rizkinaswara 2024). Digitalisasi merupakan elemen penting bagi pelaku Usaha Kecil dan Menengah (UKM) dalam menghadapi dan menyesuaikan diri dengan dinamika perkembangan teknologi yang semakin pesat (Dinas Perindustrian, Koperasi, dan UKM Kota Jogja, 2023).

Berbagai upaya telah dilakukan untuk mendorong digitalisasi UKM. Contohnya, beberapa UKM mulai menggunakan aplikasi pembukuan seperti BukuWarung (Basuki Putri et al., 2021) yang menyimpan data secara cloud, atau memanfaatkan platform e-market untuk memperluas jangkauan pemasaran (Azizah et al., 2023). Bahkan perusahaan besar seperti PT. Bank Negara Indonesia (BNI) telah mengadopsi sistem manajemen SDM berbasis digial melalui aplikasi DigiHC Mobile, yang mendukung kegiatan operasional secara lebih efisien (Farrel Shidqi et al., 2023). Hal ini menjadi sinyal bahwa digitalisasi telah merambat ke berbagai level usaha, termasuk UKM.

Fenomena Digitalisasi UKM merujuk pada penerapan teknologi digital dalam berbagai kegiatan operasional dan manajemen bisnis (Amartha 2024). Menurut (Fadillah et al., 2022), masih terdapat oknum yang memanfaatkan internet secara tidak semestinya untuk melakukan tindakan kejahatan yang dikenal dengan cybercrime. Dalam industri e-commerce, terdapat empat tantangan keamanan utama yaitu, keamanan transaksi, privasi, sistem

perdagangan elektronik, dan kejahatan dunia maya. Kerentanan ini dapat menyebabkan bocornya informasi sensitif, sehingga memicu pelanggaran data dan pencurian identitas.

Beberapa kasus besar menunjukkan dampak nyata dari lemahnya sistem keamanan. Contohnya, serangan ransomware yang menimpa Bank Syariah Indonesia (BSI) dan Pusat Data Nasional Sementara (PDNS) Kominfo menyebabkan gangguan operasional dan kerugian besar (A. P. Novita et al., 2023). Serangan Distributed Denial of Service (DDos) juga sempat mengacaukan sistem logistik perusahaan dan mengganggu pelayanan kepada konsumen (Yuniarti et al., 2023). Bahkan Tokopedia sebagai salah satu e-commerce terbesar di Indonesia mengalami insiden kebocoran data akibat lemahnya lapisan keamanan (Fadilla et al., 2022). Jika perusahaan besar saja bisa terdampak, UKM dengan keterbatasan SDM dan teknologi tentu lebih rentan.

Pelatihan keamanan digital bagi karyawan juga merupakan bagian integral dari komitmen manajemen. Pelatihan rutin mengenai praktik terbaik dalam keamanan siber berperan dalam meningkatkan kesadaran dan kesiapsiagaan karyawan terhadap ancaman siber. Mereka akan lebih mampu mengenali ancaman seperti phishing atau malware, serta memahami pentingnya menjaga data perusahaan (Axios, 2024). Selain itu, investasi dalam solusi keamanan yang dapat diskalakan juga mencerminkan komitmen manajemen untuk melindungi aset organisasi dari risiko siber (ksbadmin, 2024).

Di era digital yang serba terhubung, serangan siber (cyber attack) menjadi ancaman nyata bagi organisasi dari berbagai skala, baik besar maupun kecil. Perusahaan menghadapi risiko kehilangan data penting, gangguan operasional, kerugian finansial, serta kerusakan reputasi. Dengan demikian, sistem pengendalian internal yang kuat dan komprehensif menjadi salah satu elemen krusial dalam upaya perlindungan perusahaan terhadap berbagai ancaman siber. Dalam konteks serangan siber, pengendalian internal membantu meminimalkan risiko, mendeteksi serangan dengan cepat, dan meresponsnya secara efektif.

Tingginya risiko tersebut menimbulkan urgensi untuk menyiapkan UKM menghadapi serangan siber, atau yang dikenal dengan istilah cyber preparedness. Dalam konteks ini, terdapat tiga faktor penting yang diyakini berperan besar yaitu literasi digital, komitmen manajemen dan pengendalian internal. Pertama, literasi digital menjadi aspek penting dalam keamanan siber karena kemampuan ini memungkinkan individu untuk memahami dan mengenali ancaman siber serta cara melindungi data pribadi mereka di dunia maya. Banyak orang belum menyadari risiko yang terkait dengan penggunaan internet dan perangkat digital, terutama ketika informasi dapat diakses dengan mudah. Literasi digital membantu individu mengenali ancaman siber, seperti malware, phishing, dan jenis serangan siber lainnya (Vida, 2024).

Kedua, komitmen manajemen berperan penting dalam menciptakan budaya keamanan yang kuat di dalam organisasi. Manajemen yang mendukung inisiatif keamanan siber dapat mendorong pengembangan kebijakan yang jelas dan prosedur penanganan insiden yang efektif (Palo Alto, 2023). Hal ini termasuk alokasi sumber daya untuk pelatihan karyawan dan penerapan teknologi keamanan yang memadai. Sebuah studi menunjukkan bahwa UKM yang memiliki dukungan manajemen yang kuat dalam hal keamanan informasi cenderung memiliki postur keamanan yang lebih baik dan mampu merespons ancaman dengan lebih efektif (Axios, 2024).

Ketiga, Pengendalian Internal. Dalam konteks keamanan informasi, pengendalian internal mencakup kebijakan, prosedur, dan mekanisme operasional. Tujuannya adalah untuk melindungi aset informasi serta memastikan data tetap utuh dan rahasia. Pengendalian internal yang baik dapat membantu UKM mengidentifikasi potensi risiko dan menerapkan mitigasi yang tepat. Namun, kelemahan dapat muncul ketika pengendalian tidak berjalan efektif. Bahkan, sistem yang kuat sekalipun dapat ditembus jika terdapat celah dalam pengendalian (Bowman, 2023). Salah satu risiko utama yang saat ini memengaruhi efektivitas pengendalian perusahaan adalah risiko terkait teknologi dan keamanan siber. Meningkatnya digitalisasi menyebabkan organisasi menjadi semakin rentan terhadap serangan siber dan pelanggaran data. Implementasi teknologi baru seperti cloud computing memerlukan perhatian khusus terhadap keamanan data. Menurut Budiarko (2024)pengendalian internal yang efektif harus mencakup prosedur untuk memastikan keamanan informasi dan sistem. Selain itu, kepatuhan terhadap regulasi seperti GDPR, PCI-DSS, dan undang-undang lokal lainnya sangat penting. Ketidakpatuhan dapat mengakibatkan sanksi hukum dan denda yang signifikan. (Eva, 2024) menekankan bahwa pengendalian internal juga berfungsi untuk memastikan kepatuhan terhadap peraturan perundang-undangan yang berlaku. Risiko Integritas Data, dalam proses migrasi data, terutama ke platform cloud, risiko kehilangan atau perubahan data tanpa disengaja dapat terjadi. Pengendalian yang kuat diperlukan untuk menjaga integritas data. Budiarko (2024) menekankan bahwa pengendalian internal harus memastikan akurasi dan keandalan informasi keuangan.

DOI: https://doi.org/10.31004/riggs.v4i3.2010

Meskipun beberapa penelitian telah membahas keamanan siber dan implikasinya terhadap sektor e-commerce atau perusahaan besar, penelitian yang secara eksplisit mengkaji sejauh mana literasi digital, komitmen manajemen, dan pengendalian internal mempengaruhi kesiapan UKM menghadapi serangan siber masih sangat terbatas, khususnya di konteks lokal seperti Surabaya.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif, yang berakar pada paradigma positivisme. Metode ini diterapkan untuk mengkaji populasi atau sampel tertentu dengan menggunakan alat pengumpulan data berupa instrumen penelitian. Proses analisis dilakukan secara statistik atau kuantitatif, dengan tujuan utama untuk menguji hipotesis yang telah dirumuskan sebelumnya (Sugiyono, 2019). Subjek dalam penelitian ini adalah seluruh Usaha Kecil dan Menengah (UKM) yang terdaftar di Dinas Koperasi UKM dan Perdagangan di Surabaya yang menggunakan teknologi digital dalam operasi bisnis mereka, baik dari aspek pemasaran, keuangan, atau lainnya." Dalam penelitian ini, teknik yang digunakan dalam purposive sampling, yaitu metode penentuan sampel berdasarkan kriteria tertentu, seperti UKM yang telah mengimplementasikan literasi digital, menunjukkan komitmen manajerial yang jelas serta memiliki sistem pengendalian internal. Penelitian ini menggunakan kuesioner sebagai teknik pengumpulan data. Teknik analisis data menggunakan uji validitas, reabilitas, multikolinearitas, heteroskedastisitas, autokorelasi, dan hipotesis.

3. Hasil dan Diskusi

1. Hasil Uji Validitas

Tabel 4. 1 Hasil Uji Validitas

Item Variabel	Variabel	R-Hitung	R-Tabel	Keterangan
Literasi Digital	X1	0,884	0,195	Valid
		0,872	0,195	Valid
		0,855	0,195	Valid
		0,786	0,195	Valid
		0,746	0,195	Valid
		0,814	0,195	Valid
		0,831	0,195	Valid
Komitmen Manajemen	X2	0,873	0,195	Valid
		0,798	0,195	Valid
		0,801	0,195	Valid
		0,823	0,195	Valid
		0,754	0,195	Valid
		0,843	0,195	Valid
Pengendalian Internal	X3	0,782	0,195	Valid
		0,863	0,195	Valid
		8,862	0,195	Valid
		0,811	0,195	Valid
		0,806	0,195	Valid
UKM *Cyber Preparedness*	Y	0,854	0,195	Valid
		0,832	0,195	Valid
		0,891	0,195	Valid
		0,861	0,195	Valid
		0,835	0,195	Valid
		0,86	0,195	Valid
		0,779	0,195	Valid

Sumber: (Output SPSS, 2025)

DOI: https://doi.org/10.31004/riggs.v4i3.2010

Uji validitas dilakukan untuk mengetahui sejauh mana butir-butir pernyataan dalam kuesioner mampu mengukur setiap variabel penelitian secara tepat.Teknik yang digunakan adalah korelasi *Pearson (Product Moment)* antara skor masing-masing item dengan total skor variabelnya, menggunakan bantuan software SPSS versi 25. Kriteria pengujian validitas didasarkan pada nilai r tabel sebesar 0,195, dengan jumlah responden sebanyak 100 orang. Kriteria pengujian validitas adalah jika nilai r-hitung > r-tabel, maka item dinyatakan valid. Adapun nilai r-tabel untuk N = 100 dan tingkat signifikansi 5% adalah 0,195.

Berdasarkan hasil perhitungan menggunakan SPSS sebagaimana ditampilkan pada Tabel 4.6, seluruh item pernyataan pada masing-masing variabel penelitian memiliki nilai r-hitung lebih besar dari r-tabel (0,195). Hal ini menunjukkan bahwa Seluruh item pada variabel Literasi Digital (X1) memiliki nilai r-hitung antara 0,746 hingga 0,884 sehingga semuanya dinyatakan valid. Seluruh item pada variabel Komitmen Manajemen (X2) memiliki nilai r-hitung antara 0,754 hingga 0,873 sehingga semuanya dinyatakan valid. Seluruh item pada variabel Pengendalian Internal (X3) memiliki nilai r-hitung antara 0,806 hingga 0,862 sehingga semuanya dinyatakan valid. Seluruh item pada variabel UKM *Cyber Preparedness* (Y) memiliki nilai r-hitung antara 0,779 hingga 0,891 sehingga semuanya dinyatakan valid. Dengan demikian, seluruh item pernyataan pada instrumen penelitian ini telah memenuhi syarat validitas dan dapat digunakan untuk pengujian lebih lanjut.

2. Hasil Uji Reliabilitas

Tabel 4. 2 Hasil Uji Reliabilitas

No.	Variabel	Jumlah Item	Cronbach's Alpha	Keterangan
1.	Literasi Digital (X1)	7	0,922	Reliabel
2.	Komitmen Manajemen (X2)	6	0,897	Reliabel
3.	Pengendalian Internal (X3)	5	0,883	Reliabel
4.	UKM *Cyber Preparedness* (Y)	7	0,933	Reliabel

Sumber: (Output SPSS, 2025)

Uji reliabilitas dilakukan untuk mengetahui sejauh mana instrumen penelitian menghasilkan data yang konsisten dan stabil apabila diukur kembali pada waktu yang berbeda. Reliabilitas dalam penelitian ini diuji menggunakan teknik *Cronbach's Alpha* dengan bantuan *software SPSS*. Suatu instrumen dikatakan reliabel apabila nilai *Cronbach's Alpha* lebih besar dari 0,60. Pada Tabel 4.5.2 seluruh nilai *Cronbach's Alpha* tersebut lebih besar dari 0,60 yang berarti bahwa seluruh item pernyataan pada masing-masing variabel dinyatakan reliabel. Artinya instrumen yang digunakan dalam penelitian ini telah memenuhi kriteria keandalan dan dapat dipercaya untuk mengukur variabel diatas.

3. Hasil Asumsi Klasik

Hasil Uji Normalitas

Tabel 4. 3 Hasil Uji Normalitas

One-Sample Kolmogorov-Smirnov Test

		Unstandardized Residual
N		100
Normal Parameters[a,b]	Mean	,0000000
	Std. Deviation	2,26336709

DOI: https://doi.org/10.31004/riggs.v4i3.2010

Most Extreme Differences	Absolute	,081
	Positive	,081
	Negative	-,065
Test Statistic		,081
Asymp. Sig. (2-tailed)		,103[c]

a. Test distribution is Normal.

b. Calculated from data.

c. Lilliefors Significance Correction.

Sumber: (Output SPSS, 2025)

Uji normalitas dilakukan untuk mengetahui apakah data residual berdistribusi normal, yang merupakan salah satu asumsi dasar analisis statistik parametrik. Pengujian normalitas dilakukan menggunakan *One-Sample Kolmogorov-Smirnov Test* terhadap data residual yang telah distandarisasi. Berdasarkan output uji, diperoleh nilai signifikansi (*Asymp. Sig. 2-tailed*) sebesar 0,103. Karena nilai tersebut lebih besar dari taraf signifikansi yang digunakan (= 0,05), maka dapat disimpulkan bahwa bahwa data residual berdistribusi normal

4. Uji Multikolinearitas

Berikut adalah hasil uji multikolinearitas yang telah ditampilkan dalam tabel berikut.

Tabel 4. 1 Hasil Uji Multikolinearitas

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	,119	,846		,140	,889		
	LITERASI	,603	,091	,584	6,628	,000	,128	7,817
	KOMITMEN_2	,229	,103	,190	2,217	,029	,136	7,349
	PENGENDALIAN	,301	,095	,209	3,172	,002	,229	4,364

a. Dependent Variable: UKM

Sumber: (Output SPSS, 2025)

Berdasarkan tabel 4.9 dapat diketahui bahwa variabel Literasi Digital (X1) memiliki nilai *tolerance* 0,128 > 0,10 dan nilai VIF 7,817 < 10. Variabel Komitmen Manajemen (X2) nilai *tolerance* 0,136 > 0,10 dan nilai VIF 7,349 < 10. Dan variabel Pengendalian Internal (X3) nilai *tolerance* 0,229 > 0,10 dan nilai VIF 4,364 < 10. Oleh karena itu dapat disimpulkan bahwa setiap variabel independent tidak terjadi multikolinieritas.

DOI: https://doi.org/10.31004/riggs.v4i3.2010

5. Uji Heteroskedastisitas

Tabel 4. 4 Hasil Uji Heteroskedastisitas

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	1,000	,595		1,682	,096
	LITERASI	-,068	,063	-,293	-1,068	,288
	KOMITMEN_2	,014	,072	,051	,191	,849
	PENGENDALIAN_2	,119	,061	,379	1,960	,053

a. Dependent Variable: Abs_RES

Sumber: (Output SPSS, 2025)

Untuk mengetahui apakah dalam model regresi terjadi heteroskedastisitas, dilakukan uji *Glejser* dengan cara meregresikan nilai residual *absolut (Abs_REF)* terhadap variabel independen: literasi digital, komitmen manajemen, dan pengendalian internal. Hasil pengujian menunjukkan nilai signifikansi (*Sig.)* untuk masing-masing variabel berikut ini, Literasi digital 0,288, Komitmen manajemen 0,849, dan pengendalian internal 0,053. Berdasarkan kriteria pengambilan keputusan jika nilai signifikansi > 0,05, maka tidak terdapat gejala heteroskedastisitas.

Dari hasil tersebut, dapat disimpulkan bahwa:

- Variabel literasi digital dan komitmen manajemen memiliki nilai signifikansi jauh di atas 0,05, sehingga tidak terdapat indikasi heteroskedastisitas
- Variabel pengendalian internal memiliki nilai signifikansi sebesar 0,053, yang masih sedikit di atas ambang batas 0,05, sehingga masih dapat dikatakan tidak terdapat gejala heteroskedastisitas secara signifikan.

Secara keseluruhan, hasil uji *Glejser* menunjukkan bahwa model regresi tidak mengandung gejala heteroskedastisitas, sehingga asumsi klasik mengenai homogenitas varians terpenuhi. Oleh karena itu, model regresi yang digunakan layak untuk dianalisis lebih lanjut secara statistik.

6. Uji Autokorelasi

Tabel 4. 5 Hasil Uji Autokorelasi

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	,947[a]	,896	,893	2,398	1,845

a. Predictors: (Constant), PENGENDALIAN_2, KOMITMEN_2, LITERASI

b. Dependent Variable: UKM

DOI: https://doi.org/10.31004/riggs.v4i3.2010

Sumber: (Output SPSS, 2025)

Syarat tidak terjadi gejala Autokorelasi = dU<dW<4-dU
Diketahui:
N = 100
K (Variabel Independen) = 4
Nilai dL = 1,6131
Nilai dU = 1,7364
Nilai 4-dU = 2,2636
Jadi, 1,7364 < 1,845 < 2,2636 (dU<dW<4-dU)

Berdasarkan hasil uji autokorelasi dengan menggunakan uji *Durbin-Watson*, diperoleh nilai *Durbin-Watson* sebesar 1,845. Nilai ini berada di antara batas atas (dU = 1,7364) dan batas atas komplementer (4-dU = 2,2636). Oleh karena itu, dapat disimpulkan bahwa tidak terdapat gejala autokorelasi dalam model regresi yang digunakan. Hal ini menunjukkan bahwa asumsi klasik mengenai tidak adanya autokorelasi pada residual terpenuhi, sehingga model regresi layak untuk digunakan dalam analisis lebih lanjut.

3. Metode Analisis Regresi Linear Berganda

Tabel 4. 6 Hasil Uji Regresi Linear Berganda

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error
1	(Constant)	,777	,880
	LITERASI	,752	,094
	KOMITMEN	,362	,107
	PENGENDALIAN	-,108	,090

a. Dependent Variable: UKM

Sumber: (Output SPSS, 2025)

Berdasarkan Tabel 4.12 menunjukkan bahwa persamaan regresi linear berganda adalah:
$Y = a + b_1X_1 + b_2X_2 + b_3X_3 + e$
$Y = 0,777 + 0,752\ X_1 + 0,362\ X_2 - 0,108\ X_3 + e$

Berdasarkan hasil dari persamaan regresi linear di atas, maka dapat diinterprestasikan sebagai berikut:

a. Nilai dari konstanta (a) memiliki nilai positif yaitu sebesar 0,777. Tanda positif pada nilai konstanta menunjukkan adanya pengaruh searah dasar antara variabel independen terhadap variabel dependen. Artinya, apabila seluruh variabel independen yaitu Literasi Digital (X1), Komitmen Manajemen (X2), dan Pengendalian Internal (X3), diasumsikan bernilai nol atau tidak mengalami perubahan, maka nilai UKM *Cyber Preparedness* (Y) tetap berada pada nilai dasar sebesar 0,777.
b. Nilai Koefisien regresi untuk Literasi Digital (X1) adalah sebesar 0,752. Nilai tersebut menunjukkan adanya pengaruh positif dan signifikan antara variabel Literasi Digital terhadap UKM *Cyber Preparedness*. Artinya, jika Literasi Digital mengalami peningkatan sebesar 1%, maka nilai UKM *Cyber Preparedness* akan meningkat sebesar 0,752, dengan asumsi bahwa variabel lainnya tetap. Hal ini menunjukkan bahwa semakin tinggi tingkat literasi digital pelaku UKM, maka semakin tinggi pula tingkat kesiapan UKM dalam menghadapi ancaman siber.

DOI: https://doi.org/10.31004/riggs.v4i3.2010

c. Nilai Koefisien regresi untuk Komitmen Manajemen (X2) adalah sebesar 0,362. Nilai ini menunjukkan bahwa terdapat pengaruh positif dan signifikan antara Komitmen Manajemen terhadap UKM *Cyber Preparedness*. Dengan kata lain, jika Komitmen Manajemen meningkat 1%, maka nilai UKM *Cyber Preparedness* akan meningkat sebesar 0,362, dengan asumsi variabel lain tetap. Ini berarti bahwa komitmen manajemen UKM berperan penting dalam meningkatkan kesiapan siber organisasi.

d. Nilai Koefisien regresi untuk Pengendalian Internal (X3) adalah sebesar -0,108. Tanda negatif menunjukkan bahwa Pengendalian Internal berpengaruh negatif, meskipun tidak signifikan secara statistik, terhadap UKM *Cyber Preparedness*. Artinya, jika nilai Pengendalian Internal meningkat sebesar 1%, maka nilai UKM *Cyber Preparedness* akan menurun 0,108, dengan asumsi variabel lain tetap. Namun karena nilai signifikansi (Sig.) sebesar 0,233 > 0,05, maka pengaruh tersebut tidak dapat disimpulkan secara meyakinkan

4. Hasil Uji Hipotesis

1. Hasil Uji t

Tabel 4. 7 Hasil Uji t

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	,777	,880		,884	,379
	LITERASI	,752	,094	,728	8,022	,000
	KOMITMEN	,362	,107	,300	3,386	,001
	PENGENDALIAN	-,108	,090	-,077	-1,201	,233

a. Dependent Variable: UKM

Sumber: (Output SPSS, 2025)

Berdasarkan Tabel 4.13 diatas dapat diinterpretasikan sebagai berikut:

1) Diketahui nilai signifikansi untuk variabel Literasi Digital (X1), terhadap UKM *Cyber Preparedness* (Y) adalah sebesar 0,000 < 0,05 dan nilai dari t hitung adalah 8,022 > t tabel 1,984, sehingga dapat disimpulkan bahwa H_1 diterima dan H_{01} ditolak, yang artinya terdapat pengaruh signifikan secara parsial antara Literasi Digital terhadap UKM *Cyber Preparedness*. Dengan demikian, semakin tinggi tingkat literasi digital pelaku UKM, maka akan semakin meningkatkan kesiapan UKM dalam menghadapi ancaman siber.
2) Diketahui nilai signifikansi untuk variabel Komitmen Manajemen (X2) terhadap UKM *Cyber Preparedness* (Y) adalah sebesar 0,001 < 0,05 dan nilai dari t hitung adalah 3,386 > t tabel 1,984, sehingga dapat disimpulkan bahwa H_2 diterima dan H_{02} ditolak, yang artinya terdapat pengaruh signifikan secara parsial antara Komitmen Manajemen terhadap *Cyber Preparedness*. Artinya, semakin tinggi komitmen manajemen dalam pengelolaan UKM, maka akan semakin meningkatkan kesiapan siber yang dimiliki

DOI: https://doi.org/10.31004/riggs.v4i3.2010

3) Diketahui nilai signifikansi untuk variabel Pengendalian Internal (X3) terhadap UKM *Cyber Preparedness* (Y) adalah sebesar 0,233 > 0,05 dan nilai dari t hitung adalah -1,201 < t tabel 1,984, sehingga dapat disimpulkan bahwa H_{03} diterima dan H_3 ditolak, yang artinya tidak terdapat pengaruh signifikan secara parsial antara Pengendalian Internal terhadap UKM *Cyber Preparedness*. Hal ini menunjukkan bahwa perubahan pada sistem pengendalian internal tidak memberikan dampak yang berarti terhadap tingkat kesiapan siber UKM dalam konteks penelitian ini.

2. Hasil Uji F

Tabel 4. 8 Hasil Uji F

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	4760,167	3	1586,722	275,940	,000[b]
	Residual	552,023	96	5,750		
	Total	5312,190	99			

a. Dependent Variable: UKM

b. Predictors: (Constant), PENGENDALIAN, KOMITMEN, LITERASI

Sumber: (Output SPSS, 2025)

Berdasarkan Tabel 4.14 diatas menunjukkan bahwa nilai signifikansi untuk variabel Literasi Digital (X1), Komitmen Manajemen (X2), dan Pengendalian Internal (X3) terhadap UKM *Cyber Preparedness* adalah sebesar 0,000 < 0,05 dan nilai F hitung sebesar 275,940 > F tabel sebesar 2,699. Dengan demikian, dapat disimpulkan bahwa H_4 diterima dan H_{04} ditolak, yang berarti terdapat pengaruh yang signifikan secara simultan antara variabel Literasi Digital, Komitmen Manajemen dan Pengendalian Internal terhadap UKM *Cyber Preparedness*. Artinya, secara bersama-sama ketiga variabel independent tersebut berkontribusi dalam menjelaskan variabel dependen, yaitu UKM *Cyber Preparedness*

3. Koefisien Determinasi (R^2)

Tabel 4. 9 Hasil Uji Koefisien Determinasi (R^2)

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,947[a]	,896	,893	2,398

a. Predictors: (Constant), PENGENDALIAN, KOMITMEN, LITERASI

Sumber: (Output SPSS, 2025)

Berdasarkan hasil analisis pada Tabel 4.15 diatas, dapat diketahui bahwa nilai koefisien determinasi (R Square) sebesar 0,896 atau 89,6%. Hal ini menunjukkan bahwa variabel independen yaitu Literasi Digital (X1), Komitmen Manajemen (X2), dan Pengendalian Internal (X3) secara simultan memberikan kontribusi pengaruh sebesar 89,6% terhadap variabel dependen, yaitu UKM *Cyber Preparedness*. Sementara sisanya 10,4% dijelaskan oleh variabel lain yang tidak dimasukkan

DOI: https://doi.org/10.31004/riggs.v4i3.2010

dalam model penelitian ini. Dengan demikian, model regresi ini memiliki kemampuan prediksi yang sangat kuat terhadap variabel dependen, karena nilai R Square yang mendekati 1.

Pembahasan

Pengaruh Literasi Digital Terhadap UKM Cyber Preparedness, Berdasarkan hasil uji t diketahui bahwa variabel Literasi Digital (X1) memiliki nilai t hitung sebesar 8,022 dengan nilai signifikansi 0,000. Nilai ini lebih besar dari t tabel sebesar 1,984, dan signifikansinya berada di bawah 0,05. Dengan demikian, H_1 diterima dan H_{01} ditolak, yang berarti terdapat pengaruh signifikan secara parsial antara literasi digital terhadap UKM Cyber Preparedness. 2. Pengaruh Komitmen Manajemen terhadap UKM Cyber Preparedness "Hasil uji t menunjukkan bahwa variabel Komitmen Manajemen (X2) memiliki t hitung sebesar 3,386 dan nilai signifikansi 0,001. Karena t hitung > t tabel (1,984) dan signifikansi < 0,05, maka H_2 diterima dan H_{02} ditolak. Artinya, terdapat pengaruh signifikan secara parsial antara komitmen manajemen terhadap UKM Cyber Preparedness. 3. Pengaruh Pengendalian Internal terhadap UKM Cyber Preparedness "Berdasarkan uji t, diperoleh nilai t hitung untuk Pengendalian Internal (X3) sebesar -1,201 dengan signifikansi 0,232. Nilai ini lebih kecil dari t tabel (1,984) dan signifikansi lebih besar dari 0,05 sehingga H_3 ditolak dan H_{03} diterima. Artinya secara parsial, pengendalian internal tidak berpengaruh signifikan terhadap UKM Cyber Preparedness. Padahal, secara teoritis, pengendalian internal merupakan mekanisme penting dalam manajemen risiko.

Pengaruh Literasi Digital, Komitmen Manajemen dan Pengendalian Internal terhadap UKM Cyber Preparedness "Berdasarkan hasil uji F, diketahui bahwa nilai F hitung sebesar 275,940 lebih besar dari F tabel sebesar 2,699 dengan signifikansi 0,000 < 0,05. Dengan demikian H_4 diterima dan H_{04} ditolak, yang berarti bahwa Literasi Digital, Komitmen Manajemen dan Pengendalian Internal secara simultan berpengaruh signifikan terhadap UKM Cyber Preparedness.

4. Kesimpulan

Berdasarkan hasil analisis data dan pembahasan yang telah dilakukan, maka dapat disimpulkan beberapa hal sebagai berikut, Literasi Digital berpengaruh secara positif dan signifikan terhadap UKM Cyber Preparedness. Semakin tinggi literasi digital yang dimiliki oleh pelaku UKM, maka semakin tinggi pula kesiapan siber yang dimiliki. Literasi Digital membantu pelaku UKM memahami risiko siber, menggunakan teknologi dengan aman dan menerapkan langkah-langkah mitigasi secara tepat." Komitmen Manajemen berpengaruh positif dan signifikan terhadap UKM Cyber Preparedness. Komitmen manajemen yang kuat dalam mendukung dan memprioritaskan keamanan digital berkontribusi nyata terhadap Kesiapan siber UKM. Komitmen ini dapat berupa dukungan kebijakan, pelatihan karyawan, serta alokasi sumber daya untuk perlindungan siber." Pengendalian Internal tidak berpengaruh signifikan terhadap UKM Cyber Preparedness. Pengendalian internal belum mampu memberikan kontribusi yang berarti terhadap kesiapan siber. Hal ini bisa disebabkan oleh belum optimalnya penerapan kontrol internal atau kurangnya integrasi antara kontrol internal dan sistem keamanan digital. Berdasarkan hasil uji yang telah dilakukan pada semua variabel, hanya pada variabel pengendalian internal yang berpengaruh negatif atau tidak terdapat pengaruh terhadap UKM Cyber Preparedness, sedangkan pada variabel Literasi Digital dan Komitmen manajemen berpengaruh secara positif dan signifikan terhadap UKM Cyber Preparedness

Referensi

1. Aditya Arie Hanggono, Siti Ragil Handayani, & Heru susilo. (n.d.). ANALISIS ATAS PRAKTEK TAM (TECHNOLOGY ACCEPTANCE MODEL) DALAM MENDUKUNG BISNIS ONLINE DENGAN MEMANFAATKAN JEJARING SOSIAL INSTAGRAM. In Jurnal Administrasi Bisnis (JAB)|Vol (Vol. 26, Issue 1).
2. Ainul Khatimah Sulmi, A., Awaluddin, M., Gani, I., Kara, M., & Islam Negeri Alauddin Makassar, U. (2021). (Studi Empiris pada Mahasiswa Fakultas Ekonomi dan Bisnis Islam. Economic and Financial Journal, 1(2), 59–73.
3. Alivia, L., Hartono, J., Ali, S., & Nurhayati, R. (2020). Information Disclosure Readability, Cognitive Style, and Investment Decision Making: A Web Experimental Study.
4. Amartha, B. (2024). Apa Itu Digitalisasi UMKM? Ini Pengertian dan Strateginya. Amartha.
5. Angsori, M. L. (2018). Manfaat Teknologi Informasi Dalam Meningkatkan Kinerja Karyawan.

DOI: https://doi.org/10.31004/riggs.v4i3.2010

6. Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. Journal of Cybersecurity and Privacy, 1(2), 219–238. https://doi.org/10.3390/jcp1020012
7. Argianto, R. (2014). 78530-ID-analisis-sistem-akuntansi-penggajian-dan.
8. Axios. (2024). Pelatihan Keamanan Digital: Kunci Perlindungan UMKM dari Ancaman Siber. AXIOS.
9. A'yun. (2021). Didaktika Pendidikan Dasar.
10. A'yuni, Q. (2015). LITERASI DIGITAL REMAJA DI KOTA SURABAYA.
11. Azizah, S. N., Ikhsanudin, R. M., & Solichin, R. (2023). Peningkatan Usaha dan Digitalisasi Pemasaran UKM Produk Minyak Klentik (VCO) di Desa Karangrejo Kebumen (Vol. 3, Issue 3).
12. Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: an empirical evidence from the Pakistani banking sector. Information and Computer Security, 31(5), 635–654. https://doi.org/10.1108/ICS-11-2022-0179
13. Basuki Putri, P. K., Yudhanegara, D., & Fadilah, R. (2021). DIGITALISASI KEUANGAN UKM (Studi Kasus CV. Madu Mekar Purwakarta). Jurnal Riset Entrepreneurship, 4(2), 1. https://doi.org/10.30587/jre.v4i2.2530
14. Bowman, K. (2023). Apa itu Kontrol Internal? Panduan Praktis untuk Kepatuhan.
15. Budiarko, A. (2024). Pengendalian Internal: Pengertian, Tujuan, Jenis & Komponen.
16. COSO (2013). (2013).
17. Da, F., Layla, N., Studi Akuntansi, P., & Ekonomi, F. (2022). PENGARUH KOMITMEN MANAJEMEN TERHADAP PENERAPAN TRANSPARANSI PELAPORAN KEUANGAN (Studi Pada Pemerintah Daerah Kota Baubau). http://ejournal.lppmunidayan.ac.id/index.php/akuntansi
18. Fadilla, Z., Ketut Ngurah Ardiawan, M., Eka Sari Karimuddin Abdullah, M., Jannah Ummul Aiman, M., & Hasda, S. (2022). METODOLOGI PENELITIAN KUANTITATIF. http://penerbitzaini.com
19. Fadillah, F., Khanif, H. N., & Shahira, R. (2022). Dampak Cyber Attack Bagi Ekonomi Perdagangan Elektronik : Studi Pada Bocornya Data di Platform Tokopedia. 122–136.
20. Farrel Shidqi, M., Darmastuti, I., & Suryo Wicaksono, B. (n.d.). PENGARUH DIGITALISASI SISTEM PERUSAHAAN TERHADAP KINERJA KARYAWAN MELALUI KEPUASAN KERJA SEBAGAU VARIABEL INTERVENING (STUDI PADA PT. BANK NEGARA INDONESIA KANTOR WILAYAH SEMARANG). DIPONEGORO JOURNAL OF MANAGEMENT, 12(1). http://ejournal-s1.undip.ac.id/index.php/dbr
21. Ghozali. (2018). ghozali spss 25.
22. ksbadmin. (2024). Keamanan Siber untuk Usaha Kecil dan Menengah (UKM): Panduan Praktis Melindungi Bisnis Anda. INSTITUT BISNIS DAN INFORMATIKA KWIK KIANG GIE.
23. Kurniawan, Y., & Mulyawan, A. N. (2023). The Role of External Auditors in Improving Cybersecurity of the Companies through Internal Control in Financial Reporting. Journal of System and Management Sciences, 13(1), 485–510. https://doi.org/10.33168/JSMS.2023.0126
24. Lin, T. C. W. (2016). Financial Weapons of War. http://ssrn.com/abstract=2765010
25. Luthfah, D. (2021). Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia (Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law). TerAs Law Review : Jurnal Hukum Humaniter Dan HAM, 3(1), 11–22. https://doi.org/10.25105/teras-lrev.v3i1.10742
26. Maulana Murad. (2015). Definisi, Manfaat dan Elemen Penting LIterasi Digital. www.muradmaulana.com-1
27. Meilani, I. (2022). ANALISIS PENGARUH MANAJEMEN KOMITMEN UNTUK KUALITAS. In Jurnal Manajemen Dirgantara (Vol. 15, Issue 2).
28. Novita, A. P., Fatmanegara, F., Runtuwene, J. J., Samuela, J. T., Syahbani, M. F., Studi, P., Informasi, S., & Kunci, K. (n.d.). CYBER SECURITY THREATS; ANALISIS DAN MITIGASI RESIKO RANSOMWARE DI INDONESIA. Jurnal Simasi : Jurnal Ilmiah Sistem Informasi, 3(1), 160–169. https://doi.org/10.46306/sm.v3i1
29. Novita, D. (2024). Panduan Keamanan Cyber untuk UMKM: Langkah-Langkah Praktis untuk Melindungi Bisnis Anda.
30. Noviyanti, S., Putri, A., Afifah, N., Khaerunisa, A., Arya Pratama, R., & Bhayangkara Jakarta Raya Informatika, U. (2025). Pengaruh Literasi Digital Terhadap Perilaku Mahasiswa Dalam Melindungi Data Pribadi Dari Ancaman Siber. Jurnal Pustaka Nusantara Multidisplin, 3(1).
31. Palatty, J. (2025). 51 Statistik Serangan Siber pada Usaha Kecil Tahun 2025 (dan Apa yang Dapat Anda Lakukan Mengenainya). Astra.
32. Palo Alto. (2023). Palo Alto komitmen bantu keamanan siber UKM di Indonesia. ANTARA.

DOI: https://doi.org/10.31004/riggs.v4i3.2010

33. Perinkin/Kop UKM Kota Jogja. (2023). Transformasi Digital Meningkatkan Daya Saing Pelaku UKM Di Era Modern. Dinas Perindustrian Koperasi Usaha Kecil Dan Menengah. https://perinkopukm.jogjakota.go.id/detail/index/30307
34. Rahmawati, S., Irwan, M., & Nasution, P. (2024). Evaluasi Implementasi Sistem Informasi Manajemen Berbasis Teknologi Cloud Computing pada Usaha Kecil dan Menengah (UKM). In Journal Of Informatics And Busisnes (Vol. 02, Issue 01).
35. Restianty. (2018). GUNAHUMAS.
36. Rizkinaswara, L. (2024). Coba Atasi Kesenjangan Digital, Kominfo Luncurkan Program Adopsi Teknologi Digital UMKM 2024.
37. Saputra, D. F. (n.d.). LITERASI DIGITAL UNTUK PERLINDUNGAN DATA PRIBADI.
38. Sherina. (2022). PENGARUH AUDITOR INTERNAL DAN KEBIJAKAN MANAJEMEN.
39. Silvia. (2008). PENGARUH KETERBATASAN SISTEM INFORMASI.
40. Sugiyono. (2019). METODE PENELITIAN KUANTITATIF KUALITATIF DAN R&D (2nd ed.).
41. UNIKOM. (n.d.). jbptunikompp-gdl-alfinfredi-26839-6-unikom_a-i.
42. Vinatra, S., Bisnis, A., Veteran, U., & Timur, J. (2023). Peran Usaha Mikro, Kecil, dan Menengah (UMKM) dalam Kesejahteraan Perekonomian Negara dan Masyarakat. Jurnal Akuntan Publik, 1(3), 1–08. https://doi.org/10.59581/jap-widyakarya.v1i1.832
43. Widiyati, D., & Erliana. (2024). PENGARUH LITERASI KEUANGAN, PERLINDUNGAN DATA, DAN CYBERSECURITY TERHADAP PENGGUNAAN FINANCIAL TECHNOLOGY. JAE (JURNAL AKUNTANSI DAN EKONOMI), 9(1), 130–141. https://doi.org/10.29407/jae.v9i1.21945
44. Winarto, S. R., & Bisma, R. (2021). Studi Literatur: Analisis Persepsi UMKM di Indonesia Terhadap Cyber Security Menggunakan Model Protection Motivation Theory (PMT). Journal of Informatics and Computer Science, 03.
45. Wirawan, S., Djajadikerta, H., & Setiawan, A. (2021). Penerapan Pengendalian Intern pada 13 UMKM di Bandung. Jurnal Administrasi Bisnis, 10(1), 33–44. https://doi.org/10.14710/jab.v10i1.34009
46. Yuniarti, D. R., Alfarizy, H. F., Siallagan, Z., & Rizkyanfi, M. W. (2023). ANALISIS POTENSI DAN STRATEGI PENCEGAHAN CYBER CRIM DALAM SISTEM LOGISTIK DI ERA DIGITAL. Jurnal Bisnis, Logistik Dan Supply Chain (BLOGCHAIN), 3(1), 23–32. https://doi.org/10.55122/blogchain.v3i1.714
47. Zhuang, R., Bardas, A. G., DeLoach, S. A., & Ou, X. (2015). A theory of cyber attacks: A step towards analyzing mtd systems. MTD 2015 - Proceedings of the 2nd ACM Workshop on Moving Target Defense, Co-Located with: CCS 2015, 11–20. https://doi.org/10.1145/2808475.2808478
48. Zulfa Ar Rahman. (2024). Pemanfaatan Teknologi Informasi dalam Edukasi Literasi Digital untuk Peningkatan Keamanan Data dan Pencegahan Kejahatan Siber di Masyarakat Rawang Panca Arga. Merkurius : Jurnal Riset Sistem Informasi Dan Teknik Informatika, 2(6), 82–90. https://doi.org/10.61132/merkurius.v2i6.399

DOI: https://doi.org/10.31004/riggs.v4i3.2010