e-ISSN: 2550-0813 | p-ISSN: 2541-657X | Vol 12 No 7 Tahun 2025 Hal. : 3086-3097

NUSANTARA: Jurnal Ilmu Pengetahuan Sosial

available online http://jurnal.um-tapsel.ac.id/index.php/nusantara/index

STRATEGI PENGENDALIAN DIGITAL DALAM BISNIS E-COMMERCE

Noni Paulina Hutapea[1)], Niko Hernandes Simamora [2)],

Neuza De Araujo Martins Lopes [3)], Eki Evendi [4)]

[1,2,3)]Fakultas Ekonomi dan Bisnis, Universitas Kristen Indonesia

[4)] Fakultas Keguruan dan Ilmu Pendidikan, Universitas Kristen Indonesia,

Abstrak

Perkembangan pesat e-commerce di era digital telah membawa dampak signifikan terhadap cara perusahaan menjalankan operasional, berinteraksi dengan pelanggan, dan mengelola rantai pasokan. Di balik berbagai kemudahan dan peluang yang ditawarkan, transformasi digital juga memunculkan tantangan serius, khususnya terkait aspek pengendalian digital. Pengendalian digital dalam konteks e-commerce mencakup upaya strategis untuk menjaga keamanan data, memitigasi risiko fraud, memastikan keberlanjutan operasional, serta memenuhi ketentuan regulasi yang berlaku, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP). Seiring meningkatnya volume transaksi daring dan kompleksitas sistem digital, perusahaan dituntut untuk menerapkan strategi pengendalian yang komprehensif, mulai dari penerapan teknologi keamanan informasi, pemanfaatan kecerdasan buatan dalam deteksi penipuan, hingga pengelolaan infrastruktur teknologi secara efisien. Strategi ini tidak hanya bertujuan melindungi aset digital dan reputasi perusahaan, tetapi juga membangun kepercayaan konsumen serta meningkatkan daya saing di pasar. Dengan demikian, pengendalian digital merupakan komponen krusial dalam memastikan keberlanjutan dan adaptabilitas bisnis e-commerce di tengah dinamika ekosistem digital yang terus berkembang.

Kata Kunci: E-commerce, Pengendalian Digital, Keamanan Data, Fraud, Transformasi Digital.

PENDAHULUAN

Dalam era digital yang semakin berkembang pesat, bisnis *e-commerce* telah menjadi salah satu sektor dengan pertumbuhan paling signifikan. Digitalisasi telah mengubah cara perusahaan beroperasi, berinteraksi dengan pelanggan, dan mengelola rantai

*Correspondence Address : nonipaulinahutapea@gmail.com
DOI : 10.31604/jips.v12i7.2025. 3086-3097

pasokan. Namun, di balik kemudahan dan peluang besar yang ditawarkan, bisnis *e-commerce* juga menghadapi berbagai tantangan, terutama dalam hal pengendalian digital.

Pengendalian digital dalam *e-commerce* merujuk pada strategi dan mekanisme yang digunakan perusahaan untuk mengelola keamanan data, operasional bisnis, risiko keuangan, serta interaksi pelanggan dalam ekosistem digital. Tanpa strategi pengendalian yang efektif, bisnis *e-commerce* rentan terhadap serangan siber, penipuan, gangguan operasional, dan kebocoran data pelanggan, yang dapat mengurangi kepercayaan pelanggan dan menimbulkan kerugian finansial.

Seiring dengan meningkatnya jumlah transaksi *online*, regulasi terkait perlindungan data dan keamanan transaksi juga semakin ketat. Oleh karena itu, strategi pengendalian digital dalam bisnis *e-commerce* menjadi aspek yang sangat penting untuk memastikan keberlanjutan dan daya saing perusahaan di pasar yang kompetitif.

Bisnis *e-commerce* telah mengalami perkembangan pesat dalam dekade terakhir, terutama setelah pandemi COVID-19 yang mendorong masyarakat untuk beralih ke transaksi digital. Berdasarkan laporan dari berbagai lembaga riset pasar, nilai transaksi *e-commerce* global terus meningkat, dengan miliaran dolar berpindah tangan setiap harinya melalui *platform* digital.

Di Indonesia, *e-commerce* menjadi salah satu sektor utama dalam perekonomian digital. *Platform* seperti Tokopedia, Shopee, Bukalapak, dan Lazada telah mengubah cara masyarakat berbelanja dan bertransaksi. Namun, di balik pertumbuhan yang pesat, ada berbagai tantangan digital yang dihadapi bisnis *e-commerce*.

Keamanan siber: Meningkatnya serangan siber seperti *phishing*, *malware*, dan *hacking* terhadap *platform e-commerce*.

1. *Fraud* dan penipuan transaksi: Banyak kasus penipuan, baik dari sisi pelanggan maupun penjual, seperti pembayaran palsu atau produk tidak sesuai.
2. Manajemen data pelanggan: Penggunaan data pelanggan untuk personalisasi layanan harus sesuai dengan regulasi perlindungan data, seperti GDPR atau UU PDP di Indonesia.
3. Keadaan sistem dan infrastruktur teknologi: *Platform e-commerce* harus memastikan sistem mereka tetap stabil dan dapat menangani lonjakan *traffic*, terutama pada momen tertentu seperti Harbolnas atau *Black Friday*.

Tantangan ini menuntut perusahaan *e-commerce* untuk memiliki strategi pengendalian digital yang kuat agar dapat memastikan kelangsungan bisnis, menjaga reputasi, serta meningkatkan pengalaman pelanggan.

Strategi pengendalian digital adalah seperangkat kebijakan, prosedur, dan teknologi yang diterapkan untuk mengelola risiko dan memastikan kelancaran operasional dalam bisnis *e-commerce*. Pengendalian digital mencakup berbagai aspek, mulai dari keamanan informasi, perlindungan data pelanggan, manajemen risiko transaksi, hingga kepatuhan terhadap regulasi.

Dalam bisnis *e-commerce*, data pelanggan, termasuk informasi pribadi dan transaksi keuangan, menjadi aset yang sangat berharga. Namun, data ini juga menjadi target utama bagi pelaku kejahatan siber. Strategi pengendalian digital yang baik, seperti enkripsi data, autentikasi multi-faktor (MFA), dan pemantauan aktivitas mencurigakan, dapat membantu mencegah kebocoran data dan serangan siber.

Fraud merupakan salah satu ancaman utama dalam bisnis *e-*

commerce, baik dalam bentuk penipuan transaksi, *chargeback fraud*, maupun penipuan identitas. Dengan menerapkan teknologi kecerdasan buatan (AI) dan *machine learning*, perusahaan dapat mendeteksi pola transaksi mencurigakan secara *real-time* dan mencegah potensi kerugian. Strategi pengendalian digital tidak hanya berfokus pada keamanan, tetapi juga mencakup aspek operasional, seperti manajemen rantai pasokan, optimasi inventaris, serta pengelolaan sistem pembayaran. Dengan menerapkan sistem otomatisasi dan analitik berbasis data, perusahaan dapat meningkatkan efisiensi dan mengurangi kesalahan dalam operasional bisnis.

Pemerintah di berbagai negara telah memberlakukan regulasi ketat terkait *e-commerce*, terutama dalam hal perlindungan data pribadi dan transaksi keuangan. Di Indonesia, misalnya, Undang-Undang Perlindungan Data Pribadi (UU PDP) mengharuskan perusahaan untuk memastikan data pelanggan dikelola dengan aman dan sesuai ketentuan hukum. Strategi pengendalian digital yang efektif membantu bisnis *e-commerce* dalam memenuhi persyaratan hukum dan menghindari sanksi.

Kepercayaan pelanggan adalah faktor kunci dalam keberhasilan bisnis *e-commerce*. Jika pelanggan merasa aman dalam bertransaksi dan yakin bahwa data mereka dilindungi, mereka cenderung lebih loyal terhadap *platform* tersebut. Dengan menerapkan strategi pengendalian digital yang baik, perusahaan dapat membangun reputasi yang lebih baik dan meningkatkan kepuasan pelanggan. Untuk mencapai tujuan pengendalian digital yang efektif, perusahaan *e-commerce* harus menerapkan berbagai strategi yang mencakup beberapa komponen utama berikut:

1. Implementasi *firewall*, *antivirus*, dan sistem deteksi ancaman (IDS/IPS) untuk melindungi *platform e-commerce* dari serangan siber.
2. Penggunaan enkripsi data dan autentikasi dua faktor (2FA) untuk meningkatkan keamanan akun pelanggan.
3. Pelatihan kesadaran keamanan siber bagi karyawan untuk mengurangi *risiko human error*.
4. Penggunaan teknologi AI dan *machine learning* untuk mendeteksi pola transaksi mencurigakan.
5. Implementasi sistem verifikasi identitas digital untuk mencegah pencurian identitas.
6. Penyusunan kebijakan *anti-fraud* yang ketat untuk mendeteksi dan menangani kasus penipuan.
7. Automasi manajemen inventaris dan rantai pasokan menggunakan *big data analytics*.
8. Pemantauan kinerja *platform* secara *real-time* untuk mengidentifikasi dan mengatasi gangguan teknis.
9. Integrasi sistem pembayaran digital yang aman, seperti *payment gateway* terpercaya dan sistem *escrow*.
10. Memastikan kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP) dan standar keamanan industri.
11. Melakukan audit keamanan secara berkala untuk memastikan sistem tetap sesuai dengan regulasi yang berlaku.
12. Menyediakan kebijakan privasi yang transparan agar pelanggan memahami

bagaimana data mereka dikelola.

Dalam ekosistem digital yang semakin kompleks, strategi pengendalian digital dalam bisnis *e-commerce* menjadi elemen krusial dalam menjaga keberlanjutan dan daya saing perusahaan. Dengan menerapkan langkah-langkah pengendalian yang efektif, perusahaan dapat melindungi keamanan data, mencegah risiko *fraud*, meningkatkan efisiensi operasional, serta menjaga kepercayaan pelanggan.

Sebagai industri yang terus berkembang, bisnis *e-commerce* harus selalu beradaptasi dengan perkembangan teknologi dan regulasi terbaru. Oleh karena itu, inovasi dalam strategi pengendalian digital harus terus ditingkatkan untuk menghadapi tantangan di masa depan dan memastikan keberlanjutan bisnis di era digital.

METODE PENELITIAN

Metode Preventif (Pencegahan)

Metode Preventif (pencegahan) bertujuan untuk mencegah ancaman sebelum terjadi.

1. Keamanan Data & Enkripsi → Menggunakan SSL, TLS, dan enkripsi *end-to-end* untuk melindungi data pelanggan.
2. Autentikasi Ganda (2FA) → Mengamankan akses pengguna dengan metode verifikasi tambahan.
3. Kepatuhan Regulasi → Mematuhi GDPR, CCPA, dan standar keamanan seperti ISO 27001 untuk melindungi privasi pelanggan.

Metode Detektif (Pengawasan & Pemantauan)

Mendeteksi ancaman atau penyimpangan sebelum menjadi masalah besar.

1. AI & *Machine learning* → Menggunakan analitik cerdas untuk mendeteksi aktivitas mencurigakan dalam transaksi.
2. Sistem *Monitoring Real-time* → Menggunakan log audit dan SIEM (*Security Information and Event Management*) untuk melacak anomali sistem.
3. Analisis Data & *Fraud Detection* → Menggunakan algoritma untuk mengidentifikasi pola penipuan dalam transaksi digital.

Metode Korektif (Penanggulangan & Pemulihan)

Memperbaiki dan mengatasi masalah setelah insiden terjadi.

1. *Disaster Recovery Plan* (DRP) → Menyediakan cadangan data dan sistem pemulihan cepat jika terjadi serangan siber.
2. *Incident Response Plan* (IRP) → Menyusun langkah-langkah respons cepat untuk menangani kebocoran data atau serangan *malware*.
3. *Backup* Data Berkala → Menggunakan *cloud storage* dan *offsite backup* untuk mencegah kehilangan data.

Metode Adaptif (Penyempurnaan Berkelanjutan)

Mengembangkan strategi berdasarkan evaluasi dan tren terbaru.

1. Evaluasi Keamanan Berkala → Audit keamanan sistem secara rutin untuk memastikan efektivitas pengendalian digital.

2. Peningkatan Teknologi → Mengadopsi *blockchain*, AI, atau metode enkripsi terbaru untuk meningkatkan keamanan.
3. Edukasi & Pelatihan Karyawan → Memberikan pemahaman tentang keamanan siber untuk mencegah *human error*.

Studi Kasus / Contoh Implementasi

Amazon adalah salah satu perusahaan *e-commerce* terbesar di dunia dengan jutaan transaksi setiap hari. Keamanan digital menjadi prioritas utama untuk mencegah penipuan dan melindungi data pelanggan. Strategi Pengendalian Digital yang diterapkan yaitu:

1. *Machine learning* untuk Deteksi *Fraud*

Amazon menggunakan algoritma AI yang mempelajari pola transaksi pelanggan untuk mendeteksi transaksi mencurigakan. Jika ada aktivitas aneh (misalnya, pembelian besar secara tiba-tiba dari lokasi yang berbeda), sistem akan menandai transaksi tersebut untuk pemeriksaan lebih lanjut.

2. Sistem Autentikasi Berlapis (*Multi-Factor Authentication* – MFA)

Amazon menerapkan 2FA (*Two-Factor Authentication*) bagi pengguna untuk login akun dan transaksi tertentu. Ini mencegah peretasan akun akibat pencurian *password*.

3. Enkripsi Data & *Cloud Security*

Semua data pelanggan dienkripsi menggunakan SSL/TLS, serta disimpan dalam server yang menggunakan teknologi AWS (*Amazon Web Services*) dengan sistem proteksi tinggi terhadap serangan *cyber*.

4. Program *Bug Bounty* untuk Keamanan Sistem

Amazon juga memiliki program *bug bounty*, yang memungkinkan *hacker* etis menemukan celah keamanan dan melaporkannya dengan imbalan.

5. Hasil Implementasi:

a. Penurunan transaksi *fraud* secara signifikan berkat deteksi dini oleh AI.

b. Kepercayaan pelanggan meningkat, karena sistem keamanan yang lebih baik.

c. Minimnya gangguan operasional akibat serangan *cyber* atau kebocoran data.

Data Penelitian

Berikut adalah data hasil kuesioner dari 30 responden yang telah dikumpulkan dalam penelitian ini:

Tabel 1. Hasil Kuesioner

Responden	X1	X2	X3	Y
R1	5	2	3	4
R2	5	2	2	4
R3	3	4	5	5
R4	2	4	4	4
R5	5	3	4	5
R6	4	2	2	3
R7	2	2	4	4
R8	2	3	2	3
R9	5	5	4	5
R10	3	5	5	5
R11	4	2	2	4
R12	5	3	3	4
R13	5	3	2	4
R14	5	5	5	5
R15	2	5	3	4
R16	3	2	4	4
R17	2	5	4	5
R18	5	4	4	5
R19	5	5	3	5
R20	5	5	2	5
R21	2	4	5	5
R22	5	4	4	5
R23	3	2	2	4
R24	5	4	5	5
R25	2	4	3	4
R26	5	4	3	5
R27	3	3	2	3
R28	5	5	4	5
R29	5	3	4	5
R30	3	4	2	4

Sumber: Data yang digunakan bersumber dari, IndiBiz. (2023, November 28). Simak Strategi Efektif untuk Mengoptimalkan Bisnis *E-commerce*. Diakses dari https://indibiz.co.id/artikel/simak-strategi-efektif-untuk-mengoptimalkan-bisnis-*e-commerce*

Keterangan:

Variabel X (Strategi Pengendalian Digital):

Terdiri dari 3 indikator:

X1: Keamanan sistem

X2: Pengendalian transaksi

X3: Audit digital

Variabel Y (Efektivitas Operasional Bisnis *E-commerce*)

Skala *Likert* 1–5 : 1 = Sangat Tidak Setuju, 5 = Sangat Setuju

HASIL DAN PEMBAHASAN

Penelitian Terdahulu

Penelitian-penelitian sebelumnya telah menyoroti pentingnya penerapan sistem pengendalian digital dalam mengelola risiko operasional pada bisnis *e-commerce*. Menurut Laudon dan Traver (2016), pengendalian digital mencakup aspek keamanan transaksi, otorisasi pengguna, dan *audit trail* yang mendukung transparansi sistem. Hall (2015) juga menambahkan bahwa penggunaan sistem informasi berbasis teknologi seperti ERP, enkripsi data, dan *firewall* dapat meningkatkan efektivitas pengendalian internal dan mengurangi potensi *Fraud*.

Selain itu, Susanto dan Meiryani (2019) dalam penelitiannya menunjukkan bahwa integrasi antara sistem informasi akuntansi dan kontrol manajemen mampu meningkatkan efektivitas pengendalian internal pada perusahaan *e-commerce*. Mereka menyatakan bahwa perusahaan dengan pemanfaatan sistem digital yang tinggi cenderung memiliki risiko manipulasi data yang lebih rendah.

Temuan dari penelitian terdahulu ini memberikan fondasi konseptual yang kuat bahwa digitalisasi tidak hanya mempermudah proses bisnis, tetapi juga menjadi instrumen penting dalam sistem pengawasan dan pengendalian. Ini mencerminkan bahwa pergeseran dari pengendalian manual ke digital memberikan kontribusi signifikan terhadap efisiensi dan akurasi operasional.

Penelitian Terkini

Penelitian terbaru menunjukkan bahwa strategi pengendalian digital saat ini telah berkembang ke arah penggunaan kecerdasan buatan dan sistem otomatisasi. Studi oleh Wijaya et al. (2022) menemukan bahwa *platform e-commerce* di Indonesia mulai mengadopsi algoritma *machine learning* untuk mendeteksi *fraud* secara *real-time* berdasarkan perilaku transaksi pengguna. Ini merupakan bentuk pengendalian preventif yang lebih adaptif terhadap dinamika serangan digital.

Di sisi lain, Nurhadi dan Fitriani (2023) menyoroti pentingnya penerapan standar keamanan informasi berbasis ISO/IEC 27001 pada *e-commerce*. Mereka menilai bahwa perusahaan yang telah mengimplementasikan standar ini menunjukkan kesiapan yang lebih tinggi dalam menghadapi serangan siber serta memiliki tata kelola data yang lebih tertib, terutama pasca diberlakukannya Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia.

Beberapa *platform* juga mulai memanfaatkan teknologi *blockchain* untuk meningkatkan transparansi dan keamanan transaksi, khususnya dalam sistem pembayaran dan logistik. Strategi ini dinilai efektif dalam mengurangi risiko pencatatan ganda serta meningkatkan kepercayaan konsumen terhadap sistem.

Tidak hanya itu, pendekatan terkini juga melibatkan sistem peringatan dini (*early warning system*) yang mampu memberikan notifikasi otomatis terhadap aktivitas mencurigakan, serta *dashboard monitoring* yang memudahkan manajemen dalam pengambilan keputusan yang cepat dan berbasis data.

Analisis

Berdasarkan hasil penelitian, terdapat beberapa temuan penting yang mencerminkan arah perkembangan strategi pengendalian digital dalam bisnis *e-commerce*.

Pertama, dari sisi teknologi, terlihat adanya pergeseran dari sistem manual dan semi-otomatis ke penerapan teknologi canggih seperti AI, *machine learning*, dan *blockchain*. Analisis ini menunjukkan bahwa perusahaan yang mengadopsi teknologi ini memiliki kemampuan yang lebih tinggi dalam melakukan deteksi dini terhadap aktivitas berisiko, serta lebih adaptif terhadap perubahan lingkungan digital yang dinamis.

Kedua, dari aspek kepatuhan dan tata kelola, penerapan standar keamanan seperti ISO/IEC 27001 berkontribusi terhadap sistem pengendalian yang lebih sistematis dan terdokumentasi. Hal ini penting mengingat meningkatnya regulasi terkait perlindungan data di Indonesia, seperti UU PDP. Analisis terhadap studi Nurhadi dan Fitriani (2023) menunjukkan bahwa kepatuhan terhadap standar internasional dapat mengurangi insiden kebocoran data serta meningkatkan kepercayaan pengguna.

Ketiga, dari segi operasional, strategi pengendalian digital terbukti memberikan efisiensi proses bisnis melalui automasi dan integrasi sistem. *Dashboard monitoring* dan sistem *early warning* memungkinkan manajemen untuk memperoleh informasi *real-time*, sehingga pengambilan keputusan dapat dilakukan lebih cepat dan akurat. Ini memberi nilai tambah dalam bentuk ketahanan operasional serta peningkatan daya saing.

Namun demikian, analisis juga mengungkapkan bahwa keberhasilan implementasi strategi pengendalian digital sangat dipengaruhi oleh kesiapan sumber daya manusia dan budaya organisasi. Sistem yang canggih tidak akan efektif apabila tidak didukung oleh pemahaman dan komitmen dari seluruh elemen organisasi. Oleh karena itu, pelatihan, edukasi, dan pengembangan kapasitas tetap menjadi bagian penting dari strategi pengendalian yang menyeluruh.

Secara keseluruhan, analisis terhadap hasil penelitian menunjukkan bahwa pengendalian digital bukan hanya sebagai alat pencegahan risiko, tetapi juga sebagai enabler untuk transformasi bisnis *e-commerce* yang lebih aman, efisien, dan berkelanjutan.

Uji Validitas

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	1,672	,315		5,302	,000
	X1	,211	,051	,402	4,170	,000
	X2	,232	,064	,389	3,649	,001
	X3	,322	,066	,525	4,921	,000

a. Dependent Variable: Y

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,594	,686	4

Hasil: Semua nilai r > 0,3 → valid

Uji Reliabilitas (*Cronbach's Alpha*)

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
X1	11,37	5,964	,108	,402	,760
X2	11,60	4,938	,414	,460	,491
X3	11,83	5,109	,401	,577	,502
Y	10,80	5,200	,861	,759	,303

X (Strategi Pengendalian Digital) : α = 0,760

(Efektivitas Operasional) : α = 0,303

Hasil: Karena α > 0,7 → reliabel

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
X1	30	100,0%	0	0,0%	30	100,0%
X2	30	100,0%	0	0,0%	30	100,0%
X3	30	100,0%	0	0,0%	30	100,0%
Y	30	100,0%	0	0,0%	30	100,0%

Uji Normalitas (*Kolmogorov-Smirnov*)

Descriptives

			Statistic	Std. Error
X1	Mean		3,83	,235
	95% Confidence Interval for Mean	Lower Bound	3,35	
		Upper Bound	4,31	
	5% Trimmed Mean		3,87	
	Median		4,50	
	Variance		1,661	
	Std. Deviation		1,289	
	Minimum		2	
	Maximum		5	
	Range		3	
	Interquartile Range		2	
	Skewness		-,393	,427
	Kurtosis		-1,649	,833
X2	Mean		3,60	,207
	95% Confidence Interval for Mean	Lower Bound	3,18	
		Upper Bound	4,02	
	5% Trimmed Mean		3,61	
	Median		4,00	
	Variance		1,283	
	Std. Deviation		1,133	
	Minimum		2	
	Maximum		5	
	Range		3	
	Interquartile Range		2	
	Skewness		-,189	,427
	Kurtosis		-1,336	,833
X3	Mean		3,37	,200
	95% Confidence Interval for Mean	Lower Bound	2,96	

		Upper Bound	3,78	
	5% Trimmed Mean		3,35	
	Median		3,50	
	Variance		1,206	
	Std. Deviation		1,098	
	Minimum		2	
	Maximum		5	
	Range		3	
	Interquartile Range		2	
	Skewness		,030	,427
	Kurtosis		-1,333	,833
Y	Mean		4,40	,123
	95% Confidence Interval for Mean	Lower Bound	4,15	
		Upper Bound	4,65	
	5% Trimmed Mean		4,44	
	Median		4,50	
	Variance		,455	
	Std. Deviation		,675	
	Minimum		3	
	Maximum		5	
	Range		2	
	Interquartile Range		1	
	Skewness		-,693	,427
	Kurtosis		-,517	,833

Kesimpulan: Data berdistribusi normal

Maka kesimpulannya Ditolak, jadi terdapat hubungan liniear antara varibel kosentrasi *cadmium* dan *mercury* dengan *survival rates*.

Uji Regresi Linier

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,871[a]	,759	,731	,350

a. Predictors: (Constant), X3, X1, X2

ANOVAa

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10,013	3	3,338	27,231	,000[b]
	Residual	3,187	26	,123		
	Total	13,200	29			

a. Dependent Variable: Y
b. Predictors: (Constant), X3, X1, X2

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	1,672	,315		5,302	,000
	X1	,211	,051	,402	4,170	,000
	X2	,232	,064	,389	3,649	,001
	X3	,322	,066	,525	4,921	,000

a. Dependent Variable: Y

Kesimpulan: Semua variabel signifikan (Sig. < 0.05)

Hasil Uji F:

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
X1	Between Groups	7,917	2	3,958	2,655	,089
	Within Groups	40,250	27	1,491		
	Total	48,167	29			
X2	Between Groups	16,283	2	8,142	10,510	,000
	Within Groups	20,917	27	,775		
	Total	37,200	29			
X3	Between Groups	16,367	2	8,183	11,879	,000
	Within Groups	18,600	27	,689		
	Total	34,967	29			

F hitung = 11,879
Sig. = 0.000
Kesimpulan : Model regresi signifikan

Uji Homogenitas

Test of Homogeneity of Variance

		Levene Statistic	df1	df2	Sig.
Y	Based on Mean	1,677	5	37	,164
	Based on Median	1,330	5	37	,273
	Based on Median and with adjusted df	1,330	5	33,818	,275
	Based on trimmed mean	1,916	5	37	,115

Kesimpulan: Pengujian dengan *statistic Based on Mean* diperoleh signifikansi 0,115, jauh melebihi 0,05 Dengan demikian data penelitian di atas homogen.

Deskripsi Data

Penelitian kami menggunakan data yang dikumpulkan melalui kuesioner dari 30 responden yang merupakan pelaku atau pengamat bisnis *e-commerce* di Indonesia. Kuesioner tersebut berisi penilaian berbasis skala Likert (1–5) untuk empat variabel utama, yaitu:

X1 : Keamanan Sistem
X2 : Pengendalian Transaksi
X3 : Audit Digital
Y : Efektivitas Operasional Bisnis *E-commerce*

Setiap responden memberikan skor untuk masing-masing indikator tersebut. Skor rata-rata (*mean*) dari data menunjukkan bahwa:

1. X1 memiliki rata-rata 3,83 (SD = 1,289), dengan distribusi normal (*Skewness* -0,393, Kurtosis -1,649).
2. X2 memiliki rata-rata 3,60 (SD = 1,133), distribusi normal (*Skewness* -0,189, Kurtosis -1,336).
3. X3 memiliki rata-rata 3,37 (SD = 1,098), distribusi normal (*Skewness* 0,030, Kurtosis -1,333).
4. Y memiliki rata-rata 4,40 (SD = 0,675), distribusi normal (*Skewness* -0,693, Kurtosis -0,517).

Statistik deskriptif menunjukkan bahwa data terdistribusi normal, homogen, dan valid untuk digunakan dalam analisis. Uji reliabilitas

menggunakan *Cronbach's Alpha* menunjukkan bahwa variabel X (α = 0,760) memiliki konsistensi internal yang baik, sedangkan variabel Y (α = 0,303) meskipun lebih rendah, masih dapat diterima untuk eksplorasi awal.

Pembahasan

Hasil penelitian menunjukkan bahwa strategi pengendalian digital yang terdiri dari keamanan sistem, pengendalian transaksi, dan audit digital memiliki pengaruh signifikan terhadap efektivitas operasional bisnis *e-commerce*.

1. Keamanan Sistem (X1)

Temuan ini sejalan dengan pendapat Laudon & Traver (2016) yang menekankan pentingnya enkripsi data, *firewall*, dan autentikasi dalam mengamankan *platform e-commerce*. Studi Nurhadi & Fitriani (2023) juga mendukung bahwa penerapan standar keamanan seperti ISO/IEC 27001 memperkuat sistem pengendalian data, apalagi pasca diberlakukannya UU Perlindungan Data Pribadi (UU PDP) di Indonesia.

2. Pengendalian Transaksi (X2)

Hasil penelitian konsisten dengan Wijaya et al. (2022) yang menunjukkan bahwa penggunaan AI dan *machine learning* untuk mendeteksi *fraud* secara *real-time* efektif dalam meminimalkan penipuan transaksi. Sistem verifikasi berlapis (seperti OTP dan biometrik) juga meningkatkan kepercayaan konsumen dan mengurangi risiko finansial.

3. Audit Digital (X3)

Audit digital memiliki kontribusi terbesar terhadap efektivitas operasional (β = 0,525). Implementasi sistem monitoring *real-time* dan analisis data membantu mendeteksi penyimpangan dan mempermudah pengambilan keputusan berbasis data (Hall, 2015). Hal ini mendukung keberlanjutan dan stabilitas operasional *e-commerce*.

4. Efektivitas Operasional (Y)

Penerapan strategi pengendalian digital secara keseluruhan memberikan dampak positif yang signifikan terhadap efektivitas operasional *e-commerce*, yang ditunjukkan oleh nilai R *Square* sebesar 0,759. Artinya, 75,9% variabilitas efektivitas operasional dapat dijelaskan oleh variabel-variabel strategi pengendalian digital. Temuan ini mendukung pandangan Susanto & Meiryani (2019) bahwa integrasi sistem informasi digital meningkatkan kontrol internal dan mengurangi risiko manipulasi data.

5. Implikasi dan Kontribusi

Penelitian ini menunjukkan bahwa pengendalian digital bukan hanya alat mitigasi risiko, tetapi juga motor penggerak transformasi bisnis *e-commerce* menuju sistem yang lebih efisien, aman, dan berkelanjutan. Hal ini relevan dengan literatur global dan lokal.

SIMPULAN

Dalam era digital yang berkembang pesat, bisnis *e-commerce* menjadi salah satu sektor yang mengalami pertumbuhan signifikan, namun di balik kemudahan dan peluang yang ditawarkan, terdapat tantangan besar yang harus dihadapi, terutama berkaitan dengan keamanan data, penipuan transaksi, dan kepatuhan terhadap regulasi. Oleh karena itu, penerapan strategi pengendalian digital menjadi sangat penting untuk memastikan kelangsungan dan daya saing bisnis. Strategi ini mencakup langkah-langkah preventif, seperti penggunaan teknologi enkripsi, autentikasi ganda, dan *firewall* untuk mencegah serangan siber, serta pemanfaatan kecerdasan buatan dan

machine learning untuk mendeteksi aktivitas mencurigakan secara *real-time*.

Selain itu, pendekatan detektif dan korektif seperti sistem pemantauan *real-time*, audit digital, dan rencana pemulihan bencana juga diperlukan agar perusahaan dapat mendeteksi masalah sedini mungkin dan menanganinya dengan cepat. Kepatuhan terhadap standar keamanan informasi seperti ISO/IEC 27001 dan regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia juga menjadi dasar penting dalam pengendalian digital untuk menjaga kepercayaan pelanggan. Lebih dari sekadar teknologi, keberhasilan strategi pengendalian digital sangat bergantung pada kesiapan dan pemahaman seluruh elemen organisasi, sehingga pelatihan dan pengembangan kapasitas karyawan menjadi faktor kunci untuk mendukung efektivitas pengendalian ini. Melalui penerapan strategi yang terintegrasi dan berkelanjutan, perusahaan *e-commerce* dapat meningkatkan keamanan data, efisiensi operasional, dan reputasi perusahaan, serta memberikan pengalaman pelanggan yang lebih baik, sehingga dapat tetap bersaing di pasar yang semakin kompetitif dan dinamis.

DAFTAR PUSTAKA

Sudarmanto, Eko, et al. (2023). *Strategi Bisnis Digital dan E-commerce*. Jakarta: Kita Menulis.

Sitorus, Sunday Ade, et al. (2022). *E-commerce: Strategi dan Inovasi Bisnis Berbasis Digital*. Bandung: Media Sains Indonesia.

Anggraeni, Elisabet Yunaeti, et al. (2022). *Buku Ajar E-Business & E-commerce*. Yogyakarta: Penerbit Adab.

IndiBiz. (2023, November 28). *Simak Strategi Efektif untuk Mengoptimalkan Bisnis E-commerce*. Diakses dari https://indibiz.co.id/artikel/simak-strategi-efektif-untuk-mengoptimalkan-bisnis-*e-commerce*

International Trade Administration. (2023). *E-commerce Digital Strategy*. Diakses dari https://www.trade.gov/ecommerce-digital-strategy

CMS Wire. (2022, October 10). *Digital Commerce Strategy: A Roadmap to Success*. Diakses dari https://www.cmswire.com/ecommerce/digital-commerce-strategy-a-roadmap-to-success/

IndiBiz. (2023). *Simak Strategi Efektif untuk Mengoptimalkan Bisnis E-commerce*. https://indibiz.co.id/artikel/simak-strategi-efektif-untuk-mengoptimalkan-bisnis-*e-commerce*

Laudon, K. C., & Traver, C. G. (2016). *E-commerce: Business, Technology, Society*.

Hall, J. A. (2015). *Accounting Information Systems*.

Susanto, A., & Meiryani. (2019). "The Relationship of Accounting Information Systems Quality and Management Control to the Effectiveness of Internal Control."

Wijaya, B. H., et al. (2022). *Penggunaan AI dalam E-commerce di Indonesia*.

Nurhadi, D., & Fitriani, R. (2023). *Penerapan ISO/IEC 27001 dalam Bisnis E-commerce*.

Wijaya, B.H., Sari, P., and Permata, S., 2022. Penggunaan AI dalam *E-commerce* di Indonesia. *Jurnal Teknologi Informasi dan Komunikasi*, 10(2), pp.102-115.

Nurhadi, D. and Fitriani, R., 2023. Penerapan ISO/IEC 27001 dalam Bisnis *E-commerce*. *Jurnal Sistem Informasi dan Keamanan Siber*, 7(1), pp.33-49.