JURNAL MANAJEMEN TEKNOLOGI INFORMATIKA
ISSN 2988-0645 (*print*) dan 2987-8691 (*online*)
Jl. Veteran No.26B, Purus, Kec. Padang Barat, Kota Padang, Sumatera Barat 25115
Website: https://www.jentik.org | E-mail: admin@jentik.org

Integrasi Faktor Manusia dalam Tata Kelola Keamanan Siber Berbasis Cloud: Studi Pengembangan Framework

Kevin Maulana Firdaus
kevin.23100@mhs.unesa.ac.id
Universitas Negeri Surabaya

Informasi Artikel

Diterima : 01-12-2025
Direview : 12-12-2025
Disetujui : 25-12-2025

Kata Kunci

keamanan siber; tata kelola; komputasi awan; faktor manusia; framework

Abstrak

Penelitian ini bertujuan mengembangkan framework tata kelola keamanan siber berbasis cloud yang mengintegrasikan faktor manusia sebagai elemen sentral. Pendekatan kualitatif dengan desain pengembangan framework konseptual digunakan melalui studi literatur, analisis kebutuhan, perancangan model *People Process Technology*, serta simulasi implementasi. Hasil penelitian menunjukkan bahwa integrasi faktor manusia, kebijakan/prosedur, dan kontrol teknis dalam satu kerangka terpadu memberikan pendekatan tata kelola yang lebih holistik dan adaptif. Framework ini berkontribusi secara teoretis pada kajian tata kelola keamanan siber dan secara praktis sebagai acuan awal perancangan strategi keamanan siber berbasis human-centered pada lingkungan cloud.

Keywords

cybersecurity; governance; cloud computing; human factors; framework

Abstrack

This study aims to develop a cloud-based cybersecurity governance framework that integrates human factors as a central element. A qualitative approach with a conceptual framework development design was employed through literature review, needs analysis, People–Process–Technology model design, and conceptual implementation simulation. The results indicate that integrating human factors, governance processes, and technical controls into a unified framework provides a more holistic and adaptive approach to cybersecurity management in digital organizations. The proposed framework positions humans as active actors in the security system, supported by policies, standard operating procedures, and cloud security technologies. This study contributes theoretically to the development of cybersecurity governance research and practically serves as an initial reference for organizations in designing human-centered cybersecurity strategies in cloud environments.

A. Pendahuluan

Perkembangan transformasi digital dalam satu dekade terakhir telah mendorong organisasi untuk mengadopsi komputasi awan (*cloud computing*) sebagai infrastruktur utama dalam pengelolaan sistem informasi. Teknologi cloud menawarkan berbagai keunggulan, seperti efisiensi biaya, fleksibilitas, skalabilitas, serta kemudahan integrasi layanan digital lintas platform[1]. Namun, di balik manfaat tersebut, adopsi cloud juga membawa konsekuensi berupa meningkatnya kompleksitas risiko keamanan siber, terutama terkait pengelolaan akses, perlindungan data, dan ketergantungan pada pihak ketiga. Berbagai laporan industri menunjukkan bahwa insiden kebocoran data dan penyalahgunaan kredensial pada lingkungan cloud terus meningkat seiring dengan masifnya pemanfaatan layanan digital oleh organisasi modern.

Dalam konteks tersebut, keamanan siber tidak lagi dapat dipahami sebagai persoalan teknis semata, melainkan sebagai isu tata kelola (*governance*) yang melibatkan interaksi antara manusia, proses organisasi, dan teknologi. Pendekatan keamanan siber tradisional yang berfokus pada penguatan kontrol teknis seperti firewall, enkripsi, dan sistem deteksi intrusi sering kali belum mampu mengatasi akar permasalahan insiden keamanan secara menyeluruh. Hal ini disebabkan oleh fakta bahwa sebagian besar insiden keamanan siber justru dipicu oleh faktor non-teknis, seperti kelalaian pengguna, rendahnya kesadaran keamanan, kesalahan konfigurasi, serta ketidakpatuhan terhadap prosedur yang telah ditetapkan[2].

Berbagai standar dan kerangka kerja keamanan informasi, seperti ISO/IEC 27001 dan NIST *Cybersecurity Framework*, telah memberikan panduan normatif mengenai pengelolaan risiko dan penerapan kontrol keamanan. Meskipun demikian, penerapan standar tersebut dalam praktik sering kali menghadapi kendala pada aspek implementasi, khususnya terkait perilaku dan budaya pengguna dalam organisasi. Sejumlah penelitian menunjukkan bahwa keberhasilan implementasi kebijakan keamanan siber sangat dipengaruhi oleh tingkat pemahaman, sikap, dan komitmen pengguna terhadap kebijakan tersebut[3]. Kondisi ini mengindikasikan adanya kesenjangan antara kerangka tata kelola keamanan yang bersifat normatif dengan realitas operasional organisasi digital.

Pendekatan *human centered security* muncul sebagai respons terhadap keterbatasan pendekatan keamanan siber yang terlalu berorientasi teknis. Pendekatan ini menempatkan manusia sebagai elemen sentral dalam sistem keamanan dengan menekankan aspek kesadaran, perilaku, budaya organisasi, serta kejelasan peran dan tanggung jawab pengguna. Dalam pendekatan ini, manusia tidak lagi dipandang semata-mata sebagai "mata rantai terlemah", melainkan sebagai komponen strategis yang dapat memperkuat ketahanan keamanan siber apabila dikelola secara sistematis dan berkelanjutan[4]. Pendekatan ini sejalan dengan pandangan keamanan siber sebagai sistem sosio-teknis, di mana interaksi antara manusia dan teknologi menjadi faktor penentu keberhasilan pengelolaan keamanan.

Dalam lingkungan berbasis cloud, pendekatan human-centered menjadi semakin relevan karena adanya model *shared responsibility*, di mana tanggung jawab keamanan dibagi antara penyedia layanan cloud dan organisasi pengguna. Model ini menuntut keterlibatan aktif organisasi dalam mengelola perilaku pengguna, kebijakan internal, serta proses operasional keamanan, di samping

penerapan kontrol teknis yang disediakan oleh penyedia layanan cloud[5]. Namun demikian, kajian mengenai integrasi faktor manusia dalam tata kelola keamanan siber berbasis cloud masih relatif terbatas, terutama dalam bentuk pengembangan framework yang bersifat konseptual, terintegrasi, dan aplikatif.

Sebagian besar penelitian terdahulu cenderung berfokus pada pengukuran risiko secara kuantitatif atau pengembangan solusi teknis tertentu, sementara panduan tata kelola yang mengintegrasikan faktor manusia, proses organisasi, dan teknologi cloud dalam satu kerangka yang utuh masih belum banyak dikembangkan. Keterbatasan ini menunjukkan adanya peluang penelitian untuk mengembangkan sebuah framework tata kelola keamanan siber yang tidak hanya memenuhi aspek teknis, tetapi juga mampu menjawab tantangan perilaku dan budaya keamanan dalam organisasi digital.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengembangkan sebuah framework tata kelola keamanan siber berbasis cloud yang mengintegrasikan faktor manusia sebagai elemen utama melalui pendekatan *People Process Technology*. Framework yang dikembangkan diharapkan dapat menjadi model konseptual yang membantu organisasi digital dalam merancang kebijakan, prosedur, dan mekanisme keamanan siber yang lebih holistik, adaptif, dan berkelanjutan. Secara teoretis, penelitian ini diharapkan memperkaya kajian tata kelola keamanan siber dengan perspektif human-centered, sementara secara praktis memberikan acuan awal bagi organisasi dalam meningkatkan efektivitas pengelolaan keamanan sistem informasi berbasis cloud.

B. Metode Penelitian

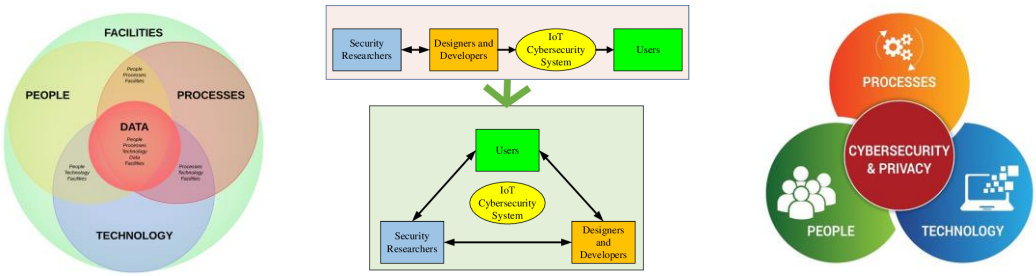
Penelitian ini menggunakan pendekatan kualitatif dengan desain pengembangan framework konseptual (*conceptual framework development*). Pendekatan ini dipilih karena tujuan penelitian tidak berfokus pada pengujian hipotesis atau pengukuran kuantitatif, melainkan pada pengembangan model tata kelola keamanan siber yang bersifat integratif dan aplikatif. Pendekatan kualitatif memungkinkan peneliti untuk melakukan sintesis teori, praktik terbaik, serta temuan penelitian sebelumnya menjadi sebuah kerangka kerja konseptual yang relevan dengan konteks organisasi digital berbasis cloud. Data dianalisis dengan menggunakan analisis deskriptif kualitatif. Data yang diperoleh dari studi literatur dan dokumentasi dianalisis dengan cara mengelompokkan, membandingkan, dan mensintesis konsep, teori, serta temuan penelitian sebelumnya yang relevan dengan tata kelola keamanan siber, faktor manusia, dan komputasi awan. Analisis ini bertujuan untuk mengidentifikasi pola, keterkaitan antar konsep, serta kesenjangan pendekatan keamanan siber yang ada. Hasil analisis selanjutnya digunakan sebagai dasar dalam perancangan framework tata kelola keamanan siber berbasis cloud yang mengintegrasikan faktor manusia sebagai elemen sentral, serta untuk mengevaluasi keterpaduan dan konsistensi antar komponen framework yang dikembangkan.

C. Hasil dan Pembahasan

Hasil utama penelitian ini adalah tersusunnya sebuah framework tata kelola keamanan siber berbasis cloud yang mengintegrasikan faktor manusia sebagai elemen sentral melalui pendekatan *People Process Technology*. Framework ini

dikembangkan untuk menjawab kebutuhan pengelolaan keamanan siber yang tidak hanya berfokus pada penguatan kontrol teknis, tetapi juga memperhatikan aspek perilaku pengguna, struktur tata kelola, dan dinamika organisasi digital. Hasil pengembangan framework menunjukkan bahwa integrasi ketiga pilar tersebut menghasilkan pendekatan pengelolaan keamanan siber yang lebih holistik dan adaptif terhadap kompleksitas lingkungan cloud.

1. Hasil Pengembangan *Framework People Process Technology*



Gambar 1. Simulasi Implementasi Framework Tata Kelola Keamanan Siber Berbasis Cloud Berbasis *People Process Technology*

Secara konseptual, framework yang dihasilkan memposisikan faktor manusia (*People*) sebagai inti dari tata kelola keamanan siber. Pilar ini mencakup kesadaran keamanan, perilaku pengguna, kompetensi, serta budaya keamanan dalam organisasi. Hasil penelitian menunjukkan bahwa tanpa adanya pengelolaan faktor manusia yang sistematis, penerapan kebijakan dan kontrol teknis cenderung tidak efektif dalam jangka panjang. Temuan ini memperkuat pandangan bahwa manusia tidak semata-mata merupakan "mata rantai terlemah" dalam keamanan siber, melainkan aktor kunci yang dapat memperkuat atau melemahkan sistem keamanan tergantung pada bagaimana perilaku dan kesadarannya dikelola[6].

Pilar Process berfungsi sebagai pengikat antara faktor manusia dan teknologi melalui tata kelola yang jelas. Pada pilar ini, dikembangkan kebijakan dan prosedur operasional standar (SOP) yang mencakup kesadaran dan pelatihan keamanan, manajemen akses pengguna, penanganan insiden keamanan siber, serta monitoring dan evaluasi keamanan. Hasil pengembangan menunjukkan bahwa keberadaan SOP yang terstruktur mampu memberikan kejelasan peran dan tanggung jawab bagi setiap pihak yang terlibat, sehingga mengurangi potensi kesalahan akibat ketidakjelasan alur kerja. Hal ini sejalan dengan prinsip tata kelola teknologi informasi yang menekankan pentingnya struktur, akuntabilitas, dan mekanisme pengendalian risiko[7].

Pilar Technology dalam framework berperan sebagai pendukung implementasi tata kelola keamanan siber berbasis cloud. Kontrol teknis yang diidentifikasi meliputi manajemen identitas dan akses (*identity and access management*), pencatatan aktivitas (*logging*), pemantauan keamanan, serta mekanisme pencadangan dan pemulihan data. Namun, hasil penelitian menegaskan bahwa teknologi dalam framework ini tidak diposisikan sebagai solusi tunggal, melainkan sebagai *enabler* yang mendukung efektivitas

pengelolaan faktor manusia dan proses tata kelola. Interpretasi ini mengonfirmasi pandangan bahwa ketergantungan berlebihan pada teknologi tanpa pengelolaan perilaku dan kebijakan yang memadai berpotensi menimbulkan rasa aman semu (*false sense of security*)[8].

2. Implementasi Rancangan Sistem melalui Simulasi Konseptual

Sebagai bentuk implementasi dari rancangan sistem yang dikembangkan, penelitian ini dilengkapi dengan simulasi implementasi konseptual framework. Simulasi dilakukan melalui pemodelan alur proses keamanan siber, mulai dari aktivitas pengguna, deteksi anomali, respon insiden, hingga evaluasi dan perbaikan kebijakan. Simulasi ini bertujuan untuk menggambarkan bagaimana framework dapat diterapkan secara sistematis dalam lingkungan organisasi *digital berbasis cloud.*

Hasil simulasi menunjukkan bahwa pendekatan human-centered memberikan kejelasan yang lebih baik pada setiap tahap pengelolaan insiden keamanan siber. Pada tahap awal, aktivitas pengguna dipantau melalui mekanisme *logging* dan monitoring, yang memungkinkan deteksi dini terhadap aktivitas tidak wajar. Ketika anomali terdeteksi, proses respon insiden tidak hanya berfokus pada tindakan teknis, tetapi juga melibatkan komunikasi, koordinasi, dan evaluasi perilaku pengguna. Tahap evaluasi pascainsiden kemudian digunakan untuk memperbarui kebijakan dan prosedur, serta meningkatkan kesadaran pengguna melalui edukasi ulang.

Pendekatan ini menunjukkan bahwa pengelolaan keamanan siber tidak berhenti pada penyelesaian insiden secara teknis, melainkan berlanjut pada pembelajaran organisasi (*organizational learning*). Dengan demikian, framework yang dikembangkan mendorong terciptanya siklus perbaikan berkelanjutan dalam tata kelola keamanan siber.

Gambar 4.2 Diagram Step-by-Step Implementasi Rancangan Sistem melalui Simulasi Konseptual

3. Analisis Perbandingan dengan Pendekatan Keamanan Konvensional

Untuk memperdalam pembahasan, dilakukan analisis perbandingan konseptual antara framework yang dikembangkan dan pendekatan keamanan siber konvensional. Pendekatan konvensional umumnya menempatkan teknologi sebagai fokus utama pengamanan sistem informasi, sementara faktor manusia dan proses organisasi sering kali diperlakukan sebagai aspek pendukung. Sebaliknya, framework yang dikembangkan dalam penelitian ini

menempatkan ketiga pilar manusia, proses, dan teknologi dalam posisi yang setara dan saling melengkapi.

Perbandingan ini menunjukkan bahwa pendekatan human-centered lebih adaptif dalam menghadapi dinamika ancaman keamanan siber yang terus berkembang. Dengan melibatkan pengguna sebagai aktor aktif dalam sistem keamanan, framework ini berpotensi meningkatkan kepatuhan terhadap kebijakan keamanan dan mengurangi risiko kesalahan operasional. Temuan ini sejalan dengan kajian tata kelola keamanan siber yang menekankan pentingnya integrasi aspek manusia dalam strategi keamanan organisasi[9].

4. Konfirmasi Temuan dengan Teori dan Penelitian Sebelumnya

Hasil penelitian ini mengonfirmasi sejumlah temuan dan teori sebelumnya yang menyatakan bahwa faktor manusia merupakan salah satu penyebab dominan insiden keamanan siber. Penelitian tentang *human aspects of information security* menunjukkan bahwa rendahnya kesadaran dan kepatuhan pengguna berkontribusi signifikan terhadap terjadinya pelanggaran keamanan[10]. Selain itu, kajian mengenai evolusi konsep keamanan dari *information security* menuju *cybersecurity governance* menekankan perlunya pendekatan yang lebih holistik dan berorientasi tata kelola dalam menghadapi kompleksitas ancaman siber modern[11].

Tabel 1 Konfirmasi Temuan dengan Teori dan Penelitian Sebelumnya

No	Aspek yang Dianalisis	Temuan Studi Independen	Teori / Penelitian Sebelumnya	Kesesuaian
1	Peran faktor manusia	Faktor manusia ditempatkan sebagai elemen sentral dalam tata kelola keamanan siber berbasis cloud	Teori *Human-Centered Security* menyatakan manusia merupakan aktor kunci dalam sistem keamanan informasi	Sesuai
2	Penyebab insiden keamanan	Insiden keamanan tidak hanya disebabkan oleh kelemahan teknis, tetapi juga oleh perilaku dan kesadaran pengguna	Penelitian keamanan siber menunjukkan human error sebagai penyebab dominan insiden keamanan	Sesuai
3	Pendekatan tata kelola	Keamanan siber dikelola melalui integrasi People, Process, dan Technology	Teori tata kelola TI menekankan integrasi kebijakan, proses, dan teknologi	Sesuai
4	Ketergantungan pada teknologi	Kontrol teknis tidak cukup tanpa dukungan proses dan perilaku pengguna	Konsep *socio-technical* system dalam keamanan informasi	Sesuai
5	Konteks cloud computing	Pengelolaan keamanan berbasis cloud memerlukan tata kelola internal yang kuat	Teori *shared* responsibility *model* pada cloud computing	Sesuai
6	Keberlanjutan keamanan	Evaluasi dan perbaikan berkelanjutan menjadi bagian dari tata kelola keamanan	Konsep *continuous improvement* dalam manajemen keamanan informasi	Sesuai

Framework yang dikembangkan dalam penelitian ini memperkuat temuan tersebut dengan menyajikan model konseptual yang mengintegrasikan

faktor manusia ke dalam tata kelola keamanan siber berbasis cloud. Dengan demikian, penelitian ini tidak hanya mengonfirmasi temuan sebelumnya, tetapi juga memperluas diskursus mengenai peran faktor manusia dalam konteks lingkungan cloud yang memiliki karakteristik risiko dan tanggung jawab yang berbeda.

5. Implikasi Teoretis dan Praktis

   Secara teoretis, penelitian ini memberikan kontribusi pada pengembangan kajian tata kelola keamanan siber dengan menghadirkan framework konseptual yang menempatkan faktor manusia sebagai elemen inti. Framework ini memperkaya perspektif keamanan siber sebagai sistem sosio-teknis, di mana interaksi antara manusia, proses, dan teknologi menjadi fokus utama analisis.

   Secara praktis, framework ini dapat dijadikan acuan awal bagi organisasi digital dalam merancang kebijakan dan strategi keamanan siber berbasis cloud yang lebih adaptif dan berkelanjutan. Pendekatan human-centered memungkinkan organisasi untuk mengelola risiko keamanan tidak hanya melalui investasi teknologi, tetapi juga melalui penguatan kesadaran dan budaya keamanan pengguna.

6. Keterbatasan dan Arah Penelitian Lanjutan

   Meskipun hasil penelitian menunjukkan relevansi dan kontribusi framework yang dikembangkan, penelitian ini memiliki keterbatasan pada aspek evaluasi. Implementasi framework dilakukan dalam bentuk simulasi konseptual, sehingga belum memberikan pengukuran kuantitatif mengenai efektivitas atau penurunan risiko keamanan siber secara empiris. Oleh karena itu, penelitian lanjutan disarankan untuk menguji penerapan framework ini pada organisasi nyata dengan karakteristik yang berbeda, serta mengukur dampaknya secara lebih terukur.

D. Simpulan

Penelitian ini menghasilkan sebuah framework tata kelola keamanan siber berbasis cloud yang mengintegrasikan faktor manusia sebagai elemen sentral melalui pendekatan *People Process Technology*. Framework yang dikembangkan berangkat dari pemahaman bahwa keamanan siber tidak dapat dikelola secara efektif apabila hanya bertumpu pada kontrol teknis, melainkan memerlukan keterpaduan antara kesadaran dan perilaku pengguna, tata kelola organisasi, serta dukungan teknologi keamanan yang memadai.

Hasil penelitian menunjukkan bahwa penempatan faktor manusia sebagai inti dalam tata kelola keamanan siber memberikan pendekatan yang lebih holistik dan adaptif terhadap kompleksitas lingkungan cloud. Melalui pengintegrasian kebijakan, prosedur operasional standar, dan kontrol teknis dalam satu kerangka konseptual, framework ini mampu menggambarkan alur pengelolaan keamanan siber yang sistematis, termasuk dalam penanganan insiden dan proses evaluasi berkelanjutan. Simulasi implementasi konseptual yang dilakukan memperlihatkan bahwa pendekatan human-centered membantu memperjelas peran dan tanggung jawab setiap pihak yang terlibat, serta mendorong pembelajaran organisasi dalam pengelolaan keamanan siber.

Secara teoretis, penelitian ini berkontribusi pada pengembangan kajian tata kelola keamanan siber dengan memperkuat perspektif keamanan sebagai sistem sosio-teknis yang menekankan interaksi antara manusia, proses, dan teknologi. Secara praktis, framework yang dihasilkan dapat dijadikan acuan awal bagi organisasi digital dalam merancang strategi keamanan siber berbasis cloud yang lebih berkelanjutan, khususnya bagi organisasi dengan tingkat literasi keamanan yang beragam dan keterbatasan sumber daya.

Penelitian ini memiliki keterbatasan karena evaluasi framework dilakukan dalam bentuk simulasi konseptual tanpa pengujian empiris. Oleh karena itu, penelitian lanjutan disarankan untuk mengimplementasikan framework ini pada organisasi nyata serta melakukan pengukuran kuantitatif terhadap efektivitasnya dalam mengurangi risiko keamanan siber. Meskipun demikian, framework yang dikembangkan dalam penelitian ini memberikan landasan konseptual yang relevan dan dapat menjadi titik awal bagi pengembangan tata kelola keamanan siber berbasis human-centered di lingkungan cloud.

E. Referensi

[1] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97–102, 2013.

[2] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link': A human/computer interaction approach to usable and effective security," *BT Technology Journal*, vol. 19, no. 3, pp. 122–131, 2001.

[3] Setya Hadi, H. (2025). INTERNET OF THING (IOT): PRINSIP DAN IMPLEMENTASINYA.

[4] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "The human aspects of information security questionnaire (HAIS-Q): Two further validation studies," *Computers & Security*, vol. 66, pp. 40–51, 2017.

[5] Setya Hadi, H., & AZIZAH, M. (2024). PERANCANGAN SISTEM ANTRIAN DENGAN SPEECH RECOGNITION BERBASIS WEB PADA PUSKESMAS GASAN GADANG KAB. PADANG PARIAMAN. *Jurnal Manajemen Teknologi Informatika*, *2*(3), 154-160.

[6] ISO/IEC 27001:2022, *Information Security, Cybersecurity and Privacy Protection Information Security Management Systems Requirements*, International Organization for Standardization, 2022.

[7] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, NIST, Gaithersburg, MD, USA, 2018.

[8] B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, New York, NY, USA: W. W. Norton & Company, 2015.

[9] Hadi, H. S., Yahyan, W., & Sabriani, M. (2025). Penerapan UML dan Metode Waterfall pada Sistem Pelacakan Sertifikat Tanah Berbasis Web. *Journal of Informatics Management and Information Technology*, *5*(3), 292-301.

[10] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing*, v4.0, Cloud Security Alliance, 2017.

[11] Verizon, *2023 Data Breach Investigations Report*, Verizon Enterprise, 2023.

A. Behl and K. Behl, *Cyberwar: The Next Threat to National Security and What to Do About It*, Oxford, UK: Oxford University Press, 2017.

[12] P. P. Tallon, "Do you see what I see? The search for consensus among executives' perceptions of IT business value," *European Journal of Information Systems*, vol. 17, no. 4, pp. 306–325, 2008.

[13] S. Flowerday and R. von Solms, "Trust: An element of information security," *Information Management & Computer Security*, vol. 13, no. 4, pp. 288–297, 2005.

[14] D. McLeod and R. Schell, *Management Information Systems*, 12th ed., Boston, MA, USA: Pearson Education, 2014.

[15] rahul vandra and H. S. Hadi, "WEB-BASED TOURISM INFORMATION SYSTEM IN BUNGUS TELUK KABUNG SUB-DISTRICT OFFICE", *JENTIK*, vol. 2, no. 2, pp. 109-116, Aug. 2024.

[16] Mulawarman Munsyir, S. E., SI, S., Kom, M., Hadi, H. S., Kom, S., Kom, M., ... & Vandika, A. Y. (2024). Algoritma dan Pemrograman: Pendekatan Komprehensif. *YPAD Penerbit*.