ZONAsi Jurnal Sistem Informasi
ZONAsi VOL. 8 NO. 1 Jan 2026
Page: 23 - 33 Akreditasi Sinta 4
ISSN: 2656-7407 (Online)
2656-7393 (Print)

TINJAUAN LITERATUR SISTEMATIS BUDAYA KEAMANAN INFORMASI: DIMENSI, KERANGKA KERJA, DAN TANTANGAN DI SEKTOR PUBLIK

Ali Sofyan Abdulloh[1], Bambang Setiawan[2]
[1,2] Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember
Kampus ITS Sukolilo, Surabaya 60111
e-mail: [1]6026232009@student.its.ac.id, [2]setiawan@is.its.ac.id

Abstrak

Penerapan budaya keamanan informasi (ISC) yang positif merupakan cara efektif untuk meningkatkan perilaku dan praktik keamanan karyawan, serta mencegah ancaman siber yang masuk melalui faktor manusia. Namun, literatur yang ada saat ini masih menunjukkan inkonsistensi dalam definisi dan dimensi pembentuk ISC. Studi ini menyajikan Tinjauan Literatur Sistematis (SLR) menggunakan protokol PRISMA untuk menganalisis 27 artikel terpilih yang diterbitkan antara 2015 hingga bulan Oktober 2025. Hasil analisis mengidentifikasi pergeseran paradigma dari sekadar awareness menuju pendekatan berbasis perilaku, serta pentingnya faktor lunak (soft factor) seperti kepercayaan (trust). Meskipun studi sektor publik mendominasi secara global, ditemukan adanya urgensi spesifik bagi Indonesia yang hanya memiliki satu studi di konteks pemerintahan. Selain itu, temuan kunci menyoroti kesenjangan implementasi di sektor publik negara berkembang, yang ditandai dengan fenomena "Potemkin Village", di mana kebijakan formal gagal terinternalisasi akibat kendala budaya dan sumber daya. Guna menjembatani kesenjangan tersebut, tinjauan ini merekomendasikan penggunaan kerangka kerja komprehensif seperti STOPE atau ISCA, disertai strategi intervensi yang berfokus pada penguatan area subkultur yang masih lemah dalam lingkungan pemerintahan.

Kata kunci*:* *Budaya Keamanan Informasi, Tinjauan Literatur Sistematis, Kerangka Kerja, Faktor Manusia, Sektor Publik.*

Abstract

Fostering a positive Information Security Culture (ISC) is serves as an effective strategy to enhance employee security behaviors and practices, while mitigating cyber threats stemming from human factors. However, current literature remains inconsistent regarding the definitions and formative dimensions of ISC. This study presents a Systematic Literature Review (SLR) utilizing the PRISMA protocol to analyze 27 selected articles published between 2015 and October 2025. The analysis identifies a paradigm shift from mere awareness towards behavior-based approaches, emphasizing the importance of soft factors such as trust. While public sector studies dominate globally, the findings reveal a specific urgency for Indonesia, represented by only a single study within the government context. Furthermore, key findings highlight a significant implementation gap in the public sector of developing countries, characterized by the "Potemkin Village" phenomenon—where formal policies fail to be internalized due to cultural constraints and resource limitations. To bridge this gap, this review recommends the adoption of comprehensive frameworks such as STOPE or ISCA, accompanied by targeted intervention strategies focused on strengthening weak subcultures within government environments.

Keywords: *Information Security Culture, Systematic Literature Review, Framework, Human Factors, Public Sector.*

1. PENDAHULUAN

Dalam era digital saat ini, organisasi menghadapi tantangan keamanan informasi yang semakin kompleks. Meskipun organisasi telah berinvestasi besar pada teknologi keamanan seperti *firewall* dan sistem deteksi intrusi, insiden keamanan tetap terjadi karena jika hanya mengandalkan teknologi tidak

akan cukup untuk melindungi aset informasi [3]. Fakta di lapangan menyebutkan bahwa faktor manusia sering dianggap sebagai mata rantai terlemah (*the weakest link*) dalam rantai keamanan [19]. Selaras dengan hal ini, terdapat studi etnografis yang dilakukan oleh Greig [9] menunjukkan adanya fenomena "*Potemkin Village*" di organisasi, di mana terdapat sebuah anomali yaitu keamanan tampak kuat secara audit formal atau kebijakan tertulis, namun sebenarnya rapuh dalam praktik perilaku sehari-hari karena karyawan cenderung melanggar aturan demi efisiensi kerja.

Konsep Budaya Keamanan Informasi (*Information Security Culture* atau ISC) menjadi krusial untuk mengatasi kelemahan pada aspek manusia ini. ISC didefinisikan sebagai koleksi persepsi, sikap, nilai, asumsi, dan pengetahuan yang memandu interaksi antara manusia dengan aset informasi dalam sebuah organisasi [1]. Selain itu, penerapan budaya ini bertujuan untuk memastikan bahwa perilaku keamanan menjadi sifat kedua (*second nature*) bagi karyawan, bukan sekadar kepatuhan terpaksa terhadap aturan [1].

Meskipun pentingnya ISC telah diakui, literatur akademis mengenai topik ini masih terpecah-pecah. Sebuah tinjauan sistematis yang dilakukan oleh Nasir, Arshah, et al. [15] menemukan bahwa belum ada konsensus mengenai dimensi standar untuk konsep ISC, dengan setidaknya terdapat 48 variasi dimensi yang berbeda ditemukan dalam berbagai studi terdahulu. Hal ini tidak hanya menyulitkan pengembangan instrumen baku, tetapi juga menghambat perbandingan hasil studi dan generalisasi temuan antar konteks organisasi yang berbeda. Selain itu, sebagian besar kerangka kerja (*framework*) yang ada sering kali gagal menjelaskan hubungan internal antar komponen budaya secara menyeluruh, misalnya mengabaikan elemen pengetahuan dalam pembentukan budaya [11].

Lebih jauh lagi, terdapat kesenjangan penelitian yang signifikan terkait konteks organisasi. Mayoritas studi empiris yang sukses dilakukan di sektor swasta atau di negara maju. Sebaliknya, studi di sektor publik, khususnya di negara berkembang, menunjukkan bahwa kendala teknologi dan kurangnya pengetahuan menjadi penghambat utama dalam mewujudkan kepatuhan nyata. Selain itu, gaya manajemen yang birokratis dan pengaruh budaya lokal seperti sistem kesukuan menciptakan jarak antara kebijakan keamanan di pusat dengan implementasi praktis oleh pegawai di berbagai wilayah [13]. Indonesia sendiri menghadapi tantangan serupa sebagai negara berkembang, studi di instansi pemerintahan menemukan bahwa tingkat kesadaran keamanan pegawai masih berada pada level "cukup" hingga "buruk" pada aspek krusial seperti manajemen kata sandi [18]. Pendekatan konvensional yang hanya menekankan literasi atau peningkatan kesadaran (*awareness*) dianggap tidak memadai atau tidak cukup untuk mendorong perubahan perilaku keamanan yang berkelanjutan, sehingga pendekatan berbasis budaya dinilai lebih relevan [2]. Namun, di tengah urgensi pergeseran paradigma tersebut, literatur yang ada saat ini masih menyajikan definisi dan kerangka kerja yang terpecah-pecah, serta minimnya sintesis mendalam mengenai bagaimana budaya keamanan dapat diterapkan secara efektif dalam konteks unik birokrasi pemerintahan.

Oleh karena itu, penelitian ini bertujuan untuk melakukan Tinjauan Literatur Sistematis (*Systematic Literature Review*) terhadap studi-studi ISC yang diterbitkan antara tahun 2015 hingga 2025. Penelitian ini secara spesifik bertujuan untuk: (1) Mengidentifikasi dimensi dan faktor pembentuk ISC yang dominan dalam literatur terkini; (2) Menganalisis kerangka kerja (framework) yang digunakan untuk mengukur ISC; dan (3) Mengevaluasi tantangan serta mengidentifikasi kesenjangan implementasi ISC secara khusus di sektor publik, dengan perhatian pada konteks negara berkembang seperti Indonesia.

Melalui pencapaian tujuan tersebut, artikel ini memberikan tiga kontribusi utama bagi literatur budaya keamanan informasi yang membedakannya dari tinjauan sebelumnya. Pertama, menyajikan sintesis komprehensif yang menyoroti adanya pergeseran paradigma dalam literatur terkini, yakni transisi dari pendekatan berbasis kesadaran (*awareness*) menuju pendekatan berbasis perilaku dan faktor lunak (*soft factors*) seperti kepercayaan (*trust*). Kedua, mengungkap realitas kesenjangan implementasi di sektor publik negara berkembang yang ditandai dengan fenomena "*Potemkin Village*", di mana kebijakan formal seringkali gagal terinternalisasi akibat kendala budaya dan sumber daya. Ketiga, merumuskan rekomendasi strategis berbasis bukti guna mengatasi kesenjangan implementasi tersebut, khususnya mengusulkan transformasi dari kepatuhan administratif menuju internalisasi nilai serta optimalisasi pendekatan kepemimpinan *top-down* yang adaptif terhadap budaya hierarkis.

2. METODE PENELITIAN

Penulisan SLR ini menggunakan metode *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA), hal ini dilakukan untuk menjamin keterbukaan, validitas, serta konsistensi proses peninjauan literatur. PRISMA merupakan seperangkat pedoman berbasis bukti yang dirancang untuk meningkatkan kualitas pelaporan *systematic review* melalui prosedur yang transparan dan dapat direplikasi [17]. Adapun untuk proses peninjauan disusun melalui beberapa tahapan yang meliputi: perumusan pertanyaan penelitian sebagai dasar analisis, penyusunan strategi pencarian literatur pada basis data akademik, penetapan kriteria inklusi dan eksklusi sebelum seleksi dilakukan, serta proses pemilihan studi hingga diperoleh data final yang memenuhi kelayakan penelitian [14].

2.1 Pertanyaan Penelitian (*Research Questions*)

Berdasarkan latar belakang masalah dan kesenjangan penelitian yang telah diuraikan, penelitian ini merumuskan empat Pertanyaan Penelitian (RQ) untuk memandu proses tinjauan:

a. RQ1: Bagaimana definisi dan konsep Budaya Keamanan Informasi (ISC) digambarkan dalam literatur terkini?
b. RQ2: Apa saja faktor-faktor dan dimensi dominan yang mempengaruhi pembentukan ISC?
c. RQ3: Bagaimana kerangka kerja (*framework*) atau model yang ada digunakan untuk mengukur dan menilai ISC?
d. RQ4: Sejauh mana studi ISC telah diterapkan secara spesifik di sektor publik dan apa tantangan unik yang dihadapi?

2.2 Strategi Pencarian

Proses pencarian literatur dilakukan pada tanggal 1-15 November 2025 yang dilakukan secara menyeluruh pada tujuh basis data elektronik utama yang relevan dengan bidang sistem informasi dan keamanan, yaitu: *Science Direct, Scopus, Emerald Insight, Springer Nature, IEEE Xplore, Taylor & Francis,* dan *Google Scholar*.

Kata kunci pencarian disusun menggunakan operator Boolean (AND, OR) untuk mencakup variasi istilah yang relevan. Agar strategi pencarian dapat direplikasi, berikut adalah contoh sintaks pencarian yang diterapkan pada Google Scholar:

("*information security culture*" OR "*security culture*") AND (*framework* OR *model* OR *assessment* OR *measurement* OR *factors* OR *dimensions* OR "*case study*").

Pencarian dibatasi pada artikel yang relevan dan difilter menggunakan fitur "Rentang Khusus" (*Custom Range*) untuk tahun penerbitan 2015–2025 guna mendapatkan literatur terkini dalam satu dekade terakhir.

2.3 Kriteria Seleksi Studi

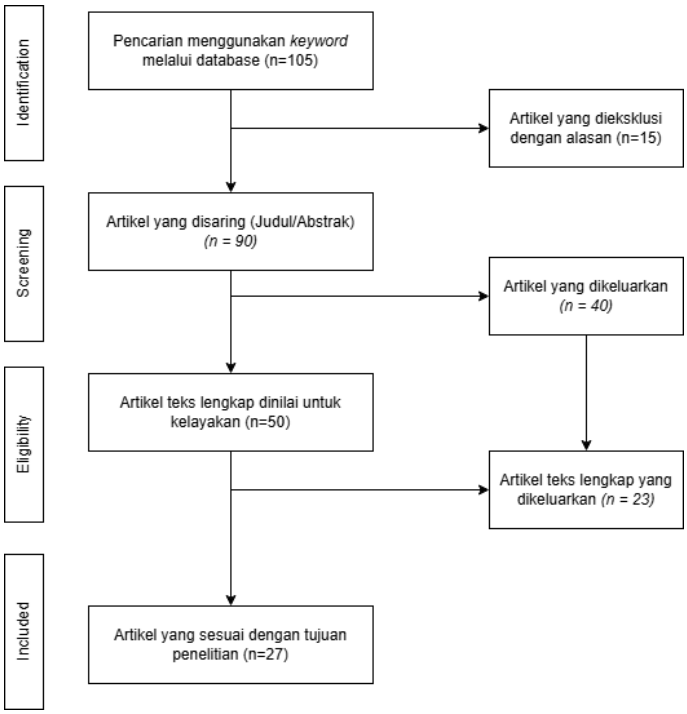
Untuk memastikan relevansi dan kualitas literatur yang dipilih, penelitian ini menerapkan kriteria inklusi dan eksklusi yang ketat. Kriteria tersebut dirangkum dalam Tabel berikut:

Tabel 1. Kriteria Inklusi dan Eksklusi

Kriteria	Kriteria Inklusi	Kriteria Eksklusi
Waktu	Diterbitkan antara 1 Januari 2015 hingga 31 Oktober 2025. Pencarian literatur dilaksanakan pada periode 1-15 November, sehingga artikel yang terbit setelah tanggal tersebut tidak termasuk.	Diterbitkan sebelum tahun 2015.
Bahasa	Ditulis dalam Bahasa Inggris atau Bahasa Indonesia.	Ditulis dalam bahasa selain Inggris atau Indonesia.
Jenis Publikasi	Merupakan Artikel Jurnal Ilmiah, Prosiding Konferensi yang telah melalui proses *peer-review*, ataupun dalam bentuk thesis dan disertasi.	Berupa editorial, abstrak saja, poster, *white paper*, artikel berita, postingan blog, atau bab buku (*book chapter*).

Fokus Topik	Fokus utamanya adalah membahas, menganalisis, atau mengusulkan faktor, model, atau *framework* Budaya Keamanan Informasi (ISC).	Hanya menyebutkan ISC sepintas dan bukan menjadi fokus utama pembahasan.
Konteks	Membahas ISC dalam konteks organisasi (swasta, pendidikan, kesehatan, atau pemerintahan).	Fokus murni pada individu di luar konteks organisasi atau aspek teknis murni (misal: algoritma kriptografi) tanpa kaitan ke budaya/manusia.

2.4 Proses Seleksi Studi (PRISMA *Flow*)



Gambar 1. Diagram Alur Prisma

Proses seleksi literatur dilakukan mengikuti empat tahapan diagram alir PRISMA (Gambar 1).

a. Identifikasi (*Identification*): Pada tahap ini, pencarian awal dilakukan pada tujuh basis data menghasilkan total 105 artikel. Setelah dilakukan pemeriksaan duplikasi, sebanyak 15 artikel yang sama dihapus, menyisakan 90 artikel untuk diproses lebih lanjut.
b. Penyaringan (*Screening*): Pada tahap ini, sebanyak 90 artikel disaring berdasarkan relevansi judul dan abstrak. Hasilnya, 40 artikel dikeluarkan karena tidak memenuhi kriteria dasar, seperti pembahasan yang murni teknis (misalnya algoritma enkripsi) tanpa menyentuh aspek budaya atau manusia.
c. Kelayakan (*Eligibility*): Pada tahap ini tersisa 50 artikel yang kemudian dibaca secara lengkap (*full-text*). Selain itu, penilaian menyeluruh dilakukan terhadap isi artikel. Sebanyak 23 artikel dieksklusi dengan alasan: (a) Fokus studi di luar konteks organisasi; atau (b) Tidak menawarkan kerangka kerja atau faktor yang jelas.
d. Inklusi (*Excluded*): Hasil akhirnya, sebanyak 27 artikel dinilai memenuhi seluruh kriteria inklusi dan memiliki kualitas data yang memadai untuk diekstraksi ke dalam sintesis kualitatif.

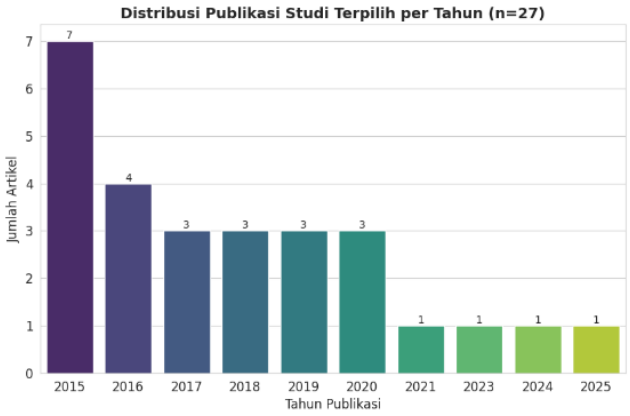
2.5 Prosedur Ekstraksi dan Sintesis Data

Setelah studi final terpilih (n=27), data diekstraksi ke dalam template terstruktur yang mencakup: identitas studi (penulis, tahun, negara), konteks organisasi, definisi ISC yang digunakan, dimensi atau faktor kunci, kerangka kerja pengukuran, temuan utama, dan tantangan yang diidentifikasi. Sintesis data dilakukan secara kualitatif menggunakan pendekatan analisis tematik (*thematic analysis*). Selanjutnya, temuan dikelompokkan dan dianalisis berdasarkan pertanyaan penelitian (RQ1-RQ4) untuk mengidentifikasi pola, persamaan, perbedaan, dan kesenjangan dalam literatur.

3. HASIL DAN PEMBAHASAN

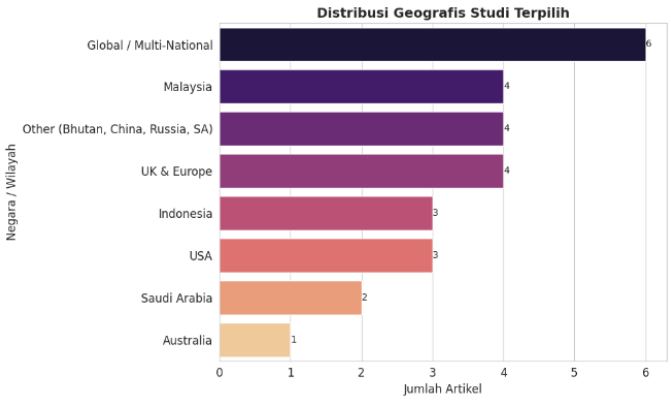
Bagian ini menyajikan hasil sintesis dari tinjauan sistematis terhadap 27 artikel yang relevan. Pembahasan disusun ke dalam empat fokus utama: (1) pemetaan tren publikasi dan demografi penelitian (Sub-bab 3.1), (2) penjelasan tentang perkembangan definisi serta dimensi kunci Budaya Keamanan Informasi (Sub-bab 3.2), (3) penjelasan tentang kerangka kerja pengukuran ISC (Sub-bab 3.3), dan (4) penjelasan tentang tantangan Implementasi ISC di Sektor Publik (Sub-bab 3.4).

3.1 Tren dan Demografi Penelitian



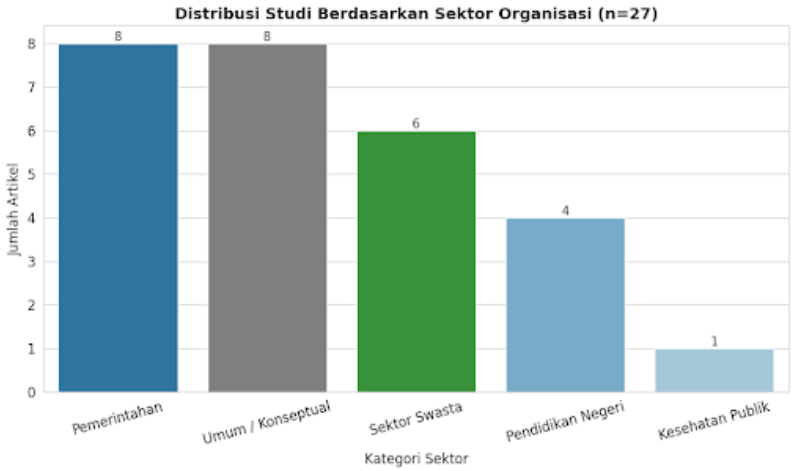
Gambar 2. Distribusi Publikasi Pertahun

Sebanyak 27 artikel yang memenuhi kriteria inklusi dianalisis untuk mengidentifikasi tren publikasi dan konteks geografis. Seperti terlihat pada Gambar 2, minat penelitian terhadap Budaya Keamanan Informasi (*Information Security Culture/ISC*) menunjukkan konsistensi dalam satu dekade terakhir, dengan lonjakan signifikan pada tahun-tahun tertentu yang mengindikasikan relevansi topik ini di tengah meningkatnya ancaman siber global.



Gambar 3. Distribusi jumlah artikel pernegara

Dari segi konteks geografis (Gambar 3), terdapat variasi yang menarik. Penelitian tidak lagi didominasi oleh negara-negara maju (Global/Multi-National dan USA/Eropa), tetapi juga mulai banyak dilakukan di negara berkembang, khususnya di kawasan Asia Tenggara seperti Malaysia (4 studi) dan Indonesia (3 studi). Hal ini memperkuat urgensi penelitian ini untuk memetakan tantangan spesifik yang dihadapi oleh sektor publik di negara berkembang yang mungkin tidak terpotret dalam studi global. Selain itu terdapat analisis distribusi sektor penelitian sebagai berikut;



Gambar 4. Distribusi jumlah penelitian perjenis organisasi

Analisis pada Gambar 4 menunjukkan pola distribusi studi berdasarkan sektor organisasi. Sektor Pemerintahan menempati porsi terbesar dengan 8 studi, diikuti oleh kategori Umum/Konseptual dengan jumlah yang sama (8 studi). Berikutnya, terdapat sektor Swasta berada dengan 6 studi, disusul oleh Pendidikan Negeri (4 studi) dan Kesehatan Publik (1 studi). Jika sektor-sektor yang berorientasi layanan publik digabungkan (Pemerintahan, Pendidikan Negeri, dan Kesehatan Publik), tercatat total 13 studi, yang secara proporsional melampaui penelitian pada sektor swasta (6 studi).

Namun, temuan yang lebih signifikan muncul ketika meninjau konteks penelitian dalam kategori Pemerintahan. Dari 8 studi tersebut, hanya satu yang secara spesifik meneliti instansi pemerintah di Indonesia (penelitian oleh; Parlindungan, 2024) [18]. Jumlah ini jauh lebih sedikit dibandingkan studi serupa di negara berkembang lain seperti Malaysia dan Arab Saudi. Lebih lanjut, temuan ini menggarisbawahi kelangkaan bukti empiris spesifik untuk konteks birokrasi Indonesia, yang justru sedang dalam proses transformasi digital yang cepat, sehingga menciptakan urgensi penelitian mendatang di area ini.

3.2. Perkembangan Definisi Serta Dimensi Kunci Budaya Keamanan Informasi

Walaupun penelitian mengenai budaya keamanan informasi telah berkembang cukup luas, kajian literatur masih menunjukkan tidak adanya kesepakatan yang jelas terkait definisi maupun dimensi pembentuk budaya keamanan informasi (ISC) [16]. Adapun hasil analisis tematik terhadap studi yang tersedia memperlihatkan adanya pergeseran fokus konseptual: dari pendekatan yang menitikberatkan pada kepatuhan teknis menuju perspektif yang menempatkan perilaku manusia sebagai inti penguatan budaya keamanan.

a. Evolusi Definisi.
   Terdapat evolusi definisi dari ISC, di mana saat ini tidak lagi dipahami hanya sebagai program peningkatan kesadaran keamanan informasi, melainkan sebagai seperangkat nilai, keyakinan, dan asumsi dasar yang secara tidak langsung membentuk perilaku keamanan dan menjadikannya bagian dari kebiasaan kerja sehari-hari atau *second nature* bagi individu dalam organisasi [1].
b. Dimensi-Dimensi Utama.
   Berdasarkan sintesis kajian terdahulu, terdapat beberapa konstruk yang secara konsisten muncul sebagai fondasi pembentuk ISC, yakni:
   1. Dukungan Manajemen dan Kebijakan.

Faktor ini menjadi komponen fundamental di hampir seluruh model konseptual yang dikembangkan [10] [15] [20].

2. Pengetahuan dan Kesadaran (SETA).
   Program pelatihan dan edukasi terbukti memiliki kontribusi signifikan dalam pembentukan budaya keamanan organisasi [3] [19].
3. Faktor "Lunak" (*Soft Factors*).
   Pada penelitian terbaru mengindikasikan bahwa elemen *interpersonal* dan psikologis, seperti *interpersonal trust* [23] *job satisfaction*, serta kepribadian [24], berperan sebagai prediktor yang lebih kuat terhadap kepatuhan keamanan dibandingkan penerapan aturan yang bersifat prosedural semata.

3.3. Kerangka Kerja Pengukuran ISC

Berbagai kerangka kerja (*framework*) telah dikembangkan untuk mengukur tingkat kematangan budaya keamanan. Tiga model yang paling dominan dalam literatur terpilih disajikan pada tabel berikut:

Tabel 2 Kerangka kerja pengukuran ISC

Kerangka Kerja (Framework)	Pengembang Utama (Studi Terkait)	Fokus & Dimensi Utama	Keunggulan & Karakteristik
STOPE (*Strategy, Technology, Organization, People, Environment*)	AlHogail [1]	Mengintegrasikan 5 dimensi utama dengan Manajemen Perubahan. Selain itu, menekankan keseimbangan aspek teknis dan manusia.	Telah menyeluruh karena memasukkan faktor Lingkungan Eksternal. Selain itu, validitas telah teruji lintas sektor (Pemerintahan Arab Saudi hingga Universitas di AS).
ISCA (*Information Security Culture Assessment*)	Da Veiga [4]; Da Veiga & Martins [6] [7]	Fokus pada asesmen berkelanjutan (*monitoring*) untuk melihat tren perubahan budaya dari waktu ke waktu.	Unggul dalam mendeteksi Subkultur dalam organisasi (misal: kesenjangan budaya antara staf IT vs non-IT) dan sangat efektif untuk studi jangka panjang.
KAB / HAIS-Q (*Knowledge-Attitude-Behavior*)	Parlindungan,[18]; Parsons et al. [19]	Fokus pada aspek Psikologis pengambilan keputusan: Pengetahuan, Sikap, dan Perilaku.	Sangat efektif untuk diagnosis spesifik di area teknis (misal: kelemahan manajemen *password*, email, internet). Banyak diadopsi di studi sektor publik Indonesia.

3.4. Tantangan Implementasi di Sektor Publik

Temuan paling signifikan dari tinjauan ini adalah adanya kesenjangan (*gap*) implementasi yang nyata antara sektor publik di negara berkembang dibandingkan sektor swasta di negara maju. Tantangan tersebut dapat dikategorikan ke dalam empat aspek utama:

a. Fenomena "*Potemkin Village*" (Kesenjangan Persepsi vs Realita).
   Studi di sektor swasta negara maju cenderung menunjukkan kematangan budaya di mana tingkat kepatuhan berbanding lurus dengan kebijakan. Sebaliknya, studi di sektor publik seringkali menemukan fenomena "*Potemkin Village*", di mana organisasi memiliki kebijakan keamanan yang

lengkap di atas kertas, namun praktik sehari-hari karyawan justru melanggar aturan tersebut demi efisiensi kerja [9]. Hal ini selaras dengan kondisi di sektor publik Arab Saudi yang dijelaskan oleh AlGhamdi, Win, & Vlahu-Gjorgievska, 2022 [13]. Meskipun investasi keamanan di wilayah tersebut terus meningkat hingga mencapai $1.7 miliar, namun organisasi tetap menghadapi tantangan besar dalam kepatuhan karyawan. Temuan dalam penelitian mereka menunjukkan adanya kegagalan pada pendekatan hukuman konvensional (*punishment severity*) yang terbukti tidak berpengaruh signifikan secara statistik (p=0.153) terhadap niat patuh karyawan. Sebaliknya, perilaku nyata di lapangan lebih banyak dipengaruhi oleh sikap personal dan budaya organisasi, yang menunjukkan bahwa kebijakan di atas kertas belum terinternalisasi menjadi tindakan nyata. Fenomena ini memperkuat argumen bahwa pendekatan konvensional berbasis kepatuhan (*compliance*) semata telah gagal, dan menyiratkan perlunya strategi transformatif yang berfokus pada internalisasi nilai, seperti yang akan direkomendasikan pada bagian kesimpulan.

b. Kendala Sumber Daya dan Infrastruktur.
   Berbeda dengan institusi keuangan global yang memiliki sumber daya memadai untuk pelatihan dan *monitoring* berkelanjutan [6] organisasi publik seringkali terhambat oleh keterbatasan anggaran dan teknologi yang telah usang. Syauqina et al., 2019 [21] secara spesifik menemukan bahwa di Puskesmas (sektor kesehatan publik Indonesia), faktor ketersediaan anggaran dan teknologi memiliki pengaruh signifikan, namun seringkali menjadi penghambat utama terbentuknya budaya keamanan yang matang.
c. Faktor Budaya dan Kepemimpinan (*Top-Down Approach*).
   Di negara dengan budaya hierarkis yang kuat seperti China dan Indonesia, peran pimpinan (*Top Management*) menjadi faktor penentu yang jauh lebih dominan dibandingkan kesadaran individu. Studi di BUMN China [22] dan Universitas di Indonesia [10] menunjukkan bahwa budaya organisasi yang "ketat" dan dukungan manajemen puncak memiliki korelasi positif yang lebih kuat terhadap kepatuhan dibandingkan sekadar program edukasi. Temuan ini berbeda dengan studi di Amerika Serikat yang menunjukkan bahwa *awareness* individu (melalui program SETA) bisa lebih efektif daripada sekadar kebijakan formal [3].
d. Kesenjangan Kompetensi (IT vs Non-IT).
   Selain itu, terdapat tantangan spesifik lain di sektor publik yaitu adanya kesenjangan budaya yang tajam antara staf teknis (IT) dan staf administratif (non-IT). Penelitian yang dilakukan oleh Glaspie, 2018 [8] serta Da Veiga & Martins, 2017 [7] menemukan bahwa subkultur karyawan IT memiliki skor budaya keamanan yang jauh lebih tinggi, sementara karyawan non-IT seringkali tidak menyadari keberadaan kebijakan atau prosedur pelaporan insiden, yang menjadi celah keamanan signifikan dalam birokrasi.

3.5 Sintesis dan Implikasi Awal

Sintesis terhadap 27 studi yang dianalisis menunjukkan bahwa kajian mengenai Budaya Keamanan Informasi (ISC) tidak lagi berhenti pada ranah teknis, tetapi telah bergerak menuju pemahaman atas perilaku manusia dalam organisasi. Meskipun kerangka seperti STOPE dan ISCA telah menyediakan fondasi konseptual untuk memetakan dimensi budaya, temuan ini mengungkap perbandingan bertolak belakang yang menarik: di mana kematangan teori ternyata belum mampu menjamin keberhasilan implementasi, terutama pada organisasi publik di negara berkembang yang masih terpaku pada pola kepatuhan administratif. Selain itu, temuan ini secara lebih tajam menekankan bahwa persoalan mendasar pada sektor publik bukan terletak pada ketiadaan regulasi, melainkan pada kegagalan menghidupkan regulasi tersebut sebagai norma sosial. Fenomena "*Potemkin Village*" menggambarkan kondisi tersebut dengan tepat: di mana audit keamanan hanya menampilkan citra kepatuhan prosedural, sementara praktik sehari-hari cenderung melanggar aturan demi tuntutan efisiensi dan karena kuatnya struktur hierarki yang kaku. Dengan demikian, implikasi penting dari tinjauan ini menegaskan bahwa perbaikan ISC di sektor publik tidak cukup dilakukan melalui penyempurnaan audit dan daftar periksa. Tantangan utamanya berada pada bagaimana organisasi mengurangi jurang antara aturan dan perilaku nyata melalui intervensi yang kontekstual, terutama dengan menyasar subkultur yang rawan (misalnya

staf non-IT) serta membangun rasa percaya untuk menggantikan budaya takut dan sekadar memenuhi kewajiban.

3.6 Pembahasan

Tinjauan ini mengungkap temuan krusial mengenai lanskap budaya keamanan informasi di sektor publik negara berkembang, yang menghadapi tantangan unik dibandingkan sektor swasta.

3.6.1 Fenomena "*Potemkin Village*" dan Kesenjangan Implementasi

Berbeda dengan sektor swasta yang cenderung matang, organisasi publik di negara berkembang (seperti Indonesia dan Malaysia) terindikasi mengalami kesenjangan implementasi yang serius. Fenomena ini dikenal sebagai "*Potemkin Village*" [9], di mana kebijakan keamanan tersedia secara formal dan lengkap di atas kertas, namun gagal terinternalisasi dalam praktik operasional sehari-hari. Hal ini diperburuk oleh temuan Orehek & Petrič, 2021 [12] yang menyoroti adanya risiko *social desirability* bias, di mana pegawai cenderung melaporkan tingkat kepatuhan yang tinggi dalam survei formal untuk memenuhi ekspektasi organisasi, padahal korelasi terhadap perilaku nyata di lapangan masih sangat lemah. Kondisi ini membuktikan bahwa pendekatan kepatuhan administratif semata sering kali menciptakan rasa aman yang semu dan tidak cukup untuk membangun budaya keamanan yang tangguh.

3.6.2 Strategi Transformasi Budaya Keamanan Informasi

Merespons tantangan tersebut, sintesis literatur menyarankan tiga strategi intervensi utama bagi sektor publik:

a. Transformasi Menuju *Trust-Based Approach*: Mengingat kegagalan pendekatan kepatuhan formal, fokus harus beralih pada pembangunan kepercayaan (*trust*) dan keterikatan pegawai. Pendekatan berbasis nilai ini secara empiris terbukti lebih efektif membentuk perilaku berkelanjutan dibandingkan ancaman sanksi semata [5] [19].
b. Intervensi Berbasis Subkultur: Organisasi pemerintah bukanlah entitas monolitik. Terdapat kesenjangan tajam antara subkultur staf teknis (IT) dengan staf administratif (non-IT) [7] [8]. Oleh karena itu, pendekatan *'one-size-fits-all'* tidak akan efektif; intervensi harus disesuaikan dengan kerentanan spesifik masing-masing subkultur.
c. Optimalisasi Kepemimpinan *Top-Down*: Dalam budaya kolektivis dan hierarkis (seperti Indonesia), keteladanan pimpinan adalah kunci. Dukungan manajemen puncak memiliki pengaruh yang jauh lebih dominan terhadap kepatuhan di Asia dibandingkan di Barat [3] [22]. Pimpinan harus berfungsi sebagai *social proof* untuk memvalidasi norma keamanan.

3.6.3 Implikasi Teoritis

Secara teoritis literatur ini mengonfirmasi bahwa model kepatuhan tradisional kurang memadai untuk menangkap kompleksitas budaya keamanan informasi. Berdasarkan hasil sintesis dari peneliti terdahulu, kerangka kerja komprehensif seperti STOPE dan ISCA, yang mengintegrasikan faktor "lunak" (*soft factors*) seperti norma sosial dan kepuasan kerja, terbukti lebih efektif sebagai prediktor perilaku budaya keamanan informasi.

4. KESIMPULAN

Tinjauan sistematis terhadap 27 artikel terpilih ini menyimpulkan bahwa lanskap penelitian budaya keamanan informasi (ISC) sedang mengalami pergeseran paradigma dari pendekatan berbasis kesadaran (*awareness*) menuju pendekatan berbasis perilaku dan nilai. Temuan utama studi ini menyoroti adanya kesenjangan implementasi kritis di sektor publik negara berkembang, yang ditandai dengan fenomena "*Potemkin Village*" yaitu kondisi di mana kebijakan formal tersedia namun terpisah dari praktik nyata.

Untuk mengatasi kesenjangan tersebut, penelitian ini merekomendasikan pergeseran strategi dari kepatuhan administratif menuju internalisasi nilai berbasis kepercayaan (*trust*). Selain itu, intervensi budaya harus bersifat adaptif dengan mengakomodasi perbedaan subkultur (IT vs Non-IT) serta memanfaatkan struktur hierarki birokrasi melalui keteladanan manajemen puncak (*top-down leadership*).

4.1. Keterbatasan dan Saran Penelitian Masa Depan

Penelitian ini memiliki keterbatasan pada jumlah literatur dan cakupan bahasa. Untuk penelitian selanjutnya, disarankan untuk: (1) Melakukan studi jangka panjang di sektor publik Indonesia untuk mengukur efektivitas intervensi budaya dalam rentang waktu yang lebih luas; dan (2) Mengembangkan dan memvalidasi instrumen pengukuran ISC yang terkontekstualisasi secara budaya (*culturally-contextualized*). Instrumen ini harus mengakomodasi nilai-nilai lokal (seperti gotong royong, sungkan atau hubungan hierarkis) sebagai variabel moderating atau bahkan dimensi pembentuk ISC itu sendiri, sehingga meningkatkan relevansi dan validitas pengukurannya di Indonesia.

Daftar Pustaka

[1] AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575. doi.org/10.1016/j.chb.2015.03.054.

[2] Astakhova, L. V. (2020). Issues of the culture of information security under the conditions of the digital economy. *Scientific and Technical Information Processing*, *47*(1), 56–64. doi.org/10.3103/S0147688220010062.

[3] Chen, Y. A. N., Ramamurthy, K., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11–19. doi.org/10.1080/08874417.2015.11645767.

[4] Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security*, *24*(2), 139–151. doi.org/10.1108/ICS-12-2015-0048.

[5] Da Veiga, A., Astakhova, L. V, Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. doi.org/10.1016/j.cose.2020.101713.

[6] Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162–176. doi.org/10.1016/j.cose.2014.12.006.

[7] Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, *70*, 72–94. doi.org/10.1016/j.cose.2017.05.002.

[8] Glaspie, Henry, "Assessment of Information Security Culture in Higher Education" (2018). Electronic Theses and Dissertations. 6009. https://stars.library.ucf.edu/etd/6009.

[9] Greig, A., Renaud, K., & Flowerday, S. (2015). An ethnographic study to assess the enactment of information security culture in a retail store. *2015 World Congress on Internet Security (WorldCIS)*, 61–66. doi.org/10.1109/WorldCIS.2015.7359415.

[10] Julfiana, E., Ransi, N., & Rahman, G. A. (2023). Analysis of Information Security Culture at FMIPA Halu Oleo University Using Partial Least Squares-Structural Equation Modeling Method. *IAIC International Conference Series*, *4*(1), 153–164. doi.org/10.34306/conferenceseries.v4i1.647.

[11] Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A systematic literature review: Information security culture. *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 1–6. doi.org/10.1109/ICRIIS.2017.8002442.

[12] Orehek, Š., & Petrič, G. (2021). A systematic review of scales for measuring information security culture. Information & Computer Security, 29(1), 133–158. doi.org/10.1108/ICS-12-2019-0140.

[13] AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2022). Employees' intentions toward complying with information security controls in Saudi Arabia's public organisations. Government Information Quarterly, 39(4), 101721. doi.org/10.1016/j.giq.2022.101721.

[14] Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Bmj*, *339*. doi.org/10.1371/journal.pmed.1000097.

[15] Nasir, A., Abdullah Arshah, R., & Ab Hamid, M. R. (2019). A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. *Information Security Journal: A Global Perspective*, *28*(3), 55–80. doi.org/10.1080/19393555.2019.1643956,

[16] Nasir, A., Arshah, R. A., Ab Hamid, M. R., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications*, *44*, 12–22. \doi.org/10.1016/j.jisa.2018.11.003.

[17] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., & Brennan, S. E. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *Bmj*, *372*. doi.org/10.1136/bmj.n71.

[18] Parlindungan, M. (2024). Eksplorasi Kesadaran dan Faktor Budaya Keamanan Terhadap Keamanan Informasi Dinas Komunikasi dan Informatika Kabupaten XYZ. *The Indonesian Journal of Computer Science*, *13*(6). doi.org/10.33022/ijcs.v13i6.4536.

[19] Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117–129. doi.org/10.1177/1555343415575152.

[20] Sherif, E., Furnell, S., & Clarke, N. (2015). An identification of variables influencing the establishment of information security culture. *Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015. Proceedings 3*, 436–448. doi.org/10.1007/978-3-319-20376-8_39.

[21] Syauqina, S., Sari, P. K., Prasetio, A., & Candiwan, C. (2019). Analisis Budaya Keamanan Informasi Di Puskesmas Kota Bandung. *Jurnal Kesehatan Vokasional*, *4*(2), 70–79. doi.org/10.22146/jkesvo.44409.

[22] Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, *17*(2), 179–186. doi.org/10.1007/s10799-015-0252-2.

[23] Tenzin, S., McGill, T., & Dixon, M. (2024). An Investigation of the Factors That Influence Information Security Culture in Government Organizations in Bhutan. *Journal of Global Information Technology Management*, *27*(1), 37–62. doi.org/10.1080/1097198X.2023.2297634.

[24] Tolah, A., Furnell, S. M., & Papadaki, M. (2021). An empirical analysis of the information security culture key factors framework. Computers & Security, 108, 102354. doi.org/10.1016/j.cose.2021.102354.