JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 3, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i3.10923

ANALISIS PERAN SERTIFIKASI PROFESIONAL CISSP DAN CISM DALAM MENDUKUNG STANDAR ETIKA PRAKTISI KEAMANAN SIBER DI INDONESIA

Naila Yustiara[1*], Evy Nurmiati[2]

[1,2]Sistem Informasi, Fakultas Sains dan Teknologi, UIN Syarif Hidayatullah Jakarta; Jl. Ir. H. Juanda No. 95, Ciputat, Kota Tangerang Selatan, Banten, 15412; Telp. (021) 740192

Keywords:
CISSP;
CISM;
Etika Profesi;
Keamanan Siber;
Sertifikasi Profesional.

Corespondent Email:
naila.yustiara24@mhs.uinjkt.ac.id

Abstrak. Berbagai insiden keamanan siber di Indonesia, termasuk kebocoran data berskala besar di sektor perpajakan dan perbankan, berulang kali menunjukkan bahwa akar persoalan tidak hanya terletak pada kelemahan teknis, tetapi juga pada lemahnya etika profesi para praktisi yang mengelola data sensitif. Penelitian ini mengkaji peran dua sertifikasi profesional yang diakui secara internasional, yaitu Certified Information Systems Security Professional (CISSP) dan Certified Information Security Manager (CISM), dalam memperkuat standar etika praktisi keamanan siber di Indonesia. Penelitian menggunakan pendekatan kualitatif berupa studi literatur terhadap publikasi nasional dan internasional serta kode etik resmi yang diterbitkan oleh (ISC)² dan ISACA, dengan analisis tematik untuk memetakan prinsip etika yang dilanggar pada kasus nyata terhadap ketentuan kode etik kedua sertifikasi. Hasil penelitian menunjukkan bahwa kedua sertifikasi memuat kode etik profesi yang mengikat dan saling melengkapi kerangka regulasi Indonesia, namun adopsinya masih terbatas akibat biaya, kesenjangan sumber daya manusia, dan belum adanya kebijakan yang mewajibkan sertifikasi dalam strategi keamanan siber nasional. Penelitian ini merekomendasikan integrasi standar etika berbasis sertifikasi ke dalam kebijakan sumber daya manusia nasional dan kurikulum pendidikan tinggi.

Abstract. *Cybersecurity incidents in Indonesia, including large-scale data leaks in the taxation and banking sectors, have repeatedly exposed weaknesses not only in technical safeguards but also in the professional ethics of practitioners who manage sensitive data. This study examines the role of two internationally recognized professional certifications, Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM), in reinforcing ethical standards among cybersecurity practitioners in Indonesia. Using a qualitative literature review of national and international publications alongside the official codes of ethics issued by (ISC)² and ISACA, and a thematic analysis mapping violated ethical principles onto both codes of conduct, this study finds that both certifications embed binding codes of professional conduct that complement Indonesia's regulatory framework, yet their adoption remains limited due to cost, human-resource gaps, and the absence of a mandatory certification policy in the national cybersecurity strategy. The study recommends closer integration of certification-based ethical standards into national workforce policy and higher-education curricula.*

1. PENDAHULUAN

Transformasi digital yang berlangsung cepat di Indonesia telah mengubah cara pemerintah, sektor swasta, dan masyarakat mengelola data serta informasi. Di satu sisi, transformasi ini mendorong efisiensi layanan publik dan pertumbuhan ekonomi digital; di sisi lain, ia memperluas permukaan serangan (attack surface) dan menghadirkan ancaman siber yang semakin kompleks [1]. Berbagai kajian menunjukkan bahwa Indonesia masih menghadapi kesenjangan kapasitas tenaga ahli yang kompeten, lemahnya koordinasi antarlembaga, keterbatasan anggaran, serta regulasi yang belum sepenuhnya adaptif terhadap perkembangan teknologi [2]. Kajian terbaru mengenai edukasi keamanan siber di Indonesia juga menemukan pola yang serupa, yaitu rendahnya kesadaran masyarakat, kesenjangan akses digital, serta belum optimalnya koordinasi kebijakan antarlembaga sebagai hambatan utama dalam mewujudkan ketahanan siber nasional [3]. Secara internasional, posisi Indonesia dalam National Cyber Security Index (NCSI) berada di peringkat 83 dari 160 negara dan peringkat keempat di kawasan Asia Tenggara dengan skor 63,64 dari 100, tertinggal dibandingkan Malaysia yang unggul dalam tata kelola dan perlindungan data [4].

Kesenjangan tersebut semakin nyata ketika ditelusuri lebih jauh ke akar penyebab berbagai insiden kebocoran data di Indonesia. Kasus kebocoran data lebih dari 20 juta wajib pajak pada awal tahun 2024 menunjukkan bahwa penyebab utama insiden bukan semata-mata kelemahan teknologi, melainkan pelanggaran terhadap prinsip etika profesi keamanan siber, yakni kerahasiaan (confidentiality), integritas (integrity), akuntabilitas (accountability), dan transparansi (transparency) oleh pihak-pihak yang memiliki akses terhadap data tersebut [5]. Pola serupa ditemukan pada kasus kebocoran data nasabah Bank Syariah Indonesia (BSI), di mana lemahnya penerapan prinsip integritas, akuntabilitas, dan tanggung jawab sosial para praktisi teknologi informasi menjadi faktor kontributor utama, di luar kecanggihan sistem keamanan yang telah diterapkan institusi [6], [7]. Temuan ini konsisten dengan pandangan bahwa keamanan informasi tidak dapat sepenuhnya diandalkan pada kontrol teknis semata, sebab faktor manusia sering menjadi celah yang paling mudah dieksploitasi sehingga diperlukan lapisan etika untuk menutup kesenjangan tersebut [8].

Salah satu instrumen yang berpotensi memperkuat standar etika praktisi keamanan siber adalah sertifikasi profesional internasional. Kompetensi dan sertifikasi terbukti berkontribusi signifikan terhadap produktivitas dan profesionalisme kerja, khususnya ketika diperkuat oleh motivasi kerja sebagai variabel mediasi [9]. Di antara berbagai sertifikasi keamanan informasi yang diakui secara global, Certified Information Systems Security Professional (CISSP) yang diterbitkan oleh (ISC)² dan Certified Information Security Manager (CISM) yang diterbitkan oleh ISACA menonjol karena keduanya mensyaratkan kepatuhan mengikat terhadap kode etik profesi sebagai syarat sah dan bertahannya sertifikasi, di luar penguasaan kompetensi teknis maupun manajerial [10], [11]. Kedua kode etik tersebut secara eksplisit mengatur kewajiban melindungi kepentingan publik, bertindak jujur dan bertanggung jawab, serta menjaga kerahasiaan informasi — prinsip-prinsip yang justru menjadi titik lemah dalam berbagai kasus kebocoran data di Indonesia.

Meskipun demikian, kajian akademik yang secara khusus menghubungkan peran sertifikasi CISSP dan CISM dengan penguatan standar etika praktisi keamanan siber di Indonesia masih terbatas. Sebagian besar literatur yang tersedia membahas pelanggaran etika dan insiden kebocoran data secara terpisah dari pembahasan mengenai sertifikasi profesional sebagai salah satu instrumen mitigasinya. Oleh karena itu, penelitian ini bertujuan untuk menganalisis bagaimana sertifikasi CISSP dan CISM dapat mendukung standar etika praktisi keamanan siber di Indonesia, sejauh mana peran keduanya saling melengkapi, serta tantangan apa yang dihadapi dalam mendorong adopsinya secara lebih luas. Kebaruan penelitian ini terletak pada pemetaan langsung prinsip etika yang dilanggar pada kasus nyata di Indonesia terhadap ketentuan kode etik CISSP dan CISM, serta pada perumusan kerangka konseptual tiga lapis yang mengaitkan etika individu, tata kelola organisasi, dan regulasi nasional.

2. TINJAUAN PUSTAKA

2.1. Etika Profesi dan Sertifikasi dalam Keamanan Siber

Etika profesi keamanan siber merupakan seperangkat prinsip moral yang mengatur perilaku profesional dalam mengelola, melindungi, dan memanfaatkan informasi digital, mencakup kerahasiaan, kejujuran, tanggung jawab profesional, dan transparansi [5]. Berbeda dari hukum yang menuntut otoritas penegak dan sanksi formal, etika bersumber dari kesadaran moral individu maupun komunitas profesi sehingga mampu mengisi ruang yang tidak terjangkau regulasi, terutama ketika praktisi menghadapi dilema antara pemanfaatan teknologi dan perlindungan privasi pengguna [8], [12]. Norma etika saja tidak cukup mengubah perilaku: kajian kesenjangan etika profesional TIK di Indonesia menunjukkan bahwa kampanye moral perlu ditopang kebijakan organisasi dan mekanisme kontrol yang dapat diaudit [13].

Sertifikasi profesional berfungsi ganda, yakni sebagai bukti kompetensi sekaligus mekanisme kontrol perilaku melalui kode etik yang mengikat pemegangnya. Kompetensi dan sertifikasi terbukti berpengaruh signifikan terhadap produktivitas kerja dengan motivasi sebagai mediator [9], sementara pelatihan keamanan siber meningkatkan kesadaran personel dalam menghadapi ancaman digital [14]. Pada tingkat organisasi, kombinasi teknologi berlapis dan kompetensi sumber daya manusia memperkuat ketahanan siber [15], sejalan dengan pendekatan Plan-Do-Check-Act pada ISO/IEC 27001 [16] yang menempatkan faktor organisasional sebagai penentu keberhasilan keamanan informasi [17].

2.2. CISSP, CISM, dan Kode Etik Profesionalnya

Certified Information Systems Security Professional (CISSP) yang diterbitkan (ISC)² mencakup delapan domain Common Body of Knowledge. Pembedanya, setiap pemegang wajib mematuhi ISC2 Code of Ethics dengan empat kanon: melindungi masyarakat, kepentingan umum, kepercayaan publik, dan infrastruktur; bertindak terhormat, jujur, adil, bertanggung jawab, dan sesuai hukum; memberikan layanan yang cermat dan kompeten; serta memajukan dan melindungi profesi [10]. Pelanggaran yang disengaja dapat berujung pada pencabutan sertifikasi.

Certified Information Security Manager (CISM) dari ISACA berfokus pada fungsi manajerial melalui empat domain, yaitu tata kelola keamanan informasi, manajemen risiko, pengembangan program keamanan, serta manajemen insiden. Pemegangnya terikat Code of Professional Ethics ISACA yang mewajibkan dukungan terhadap standar tata kelola, objektivitas, serta penjagaan kerahasiaan informasi [11]. Fokus manajerial ini relevan dengan tumpang tindih otoritas dan minimnya pelaporan insiden dalam Strategi Nasional Keamanan Siber [4] serta koordinasi lintas lembaga yang masih parsial sejak pembentukan Badan Siber dan Sandi Negara (BSSN) [18].

Tabel 1. Perbandingan (ISC)² dan ISACA

Aspek	(ISC)² (CISSP)	ISACA (CISM)
Orientasi utama	Perlindungan masyarakat dan kepercayaan publik	Tata kelola dan akuntabilitas organisasi
Penekanan perilaku	Kejujuran, kelayakan, dan kecermatan layanan teknis	Objektivitas, kerahasiaan, dan dukungan pada standar
Lingkup penerapan	Praktik teknis lintas domain keamanan	Keputusan manajerial dan pengelolaan program
Konsekuensi pelanggaran	Peninjauan sejawat hingga pencabutan sertifikasi	Tindakan disipliner hingga pencabutan sertifikasi

3. METODE PENELITIAN

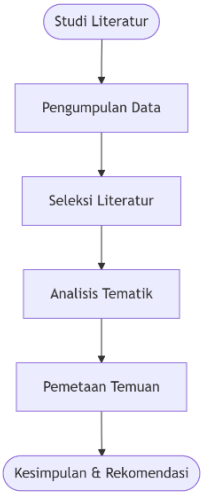
Penelitian ini menggunakan pendekatan kualitatif dengan desain studi literatur (literature review) untuk menganalisis peran sertifikasi CISSP dan CISM dalam mendukung standar etika praktisi keamanan siber di Indonesia. Pendekatan ini dipilih karena memungkinkan penelusuran mendalam terhadap kerangka konseptual etika profesi, ketentuan resmi kode etik sertifikasi, serta kasus-kasus pelanggaran etika keamanan siber

yang terdokumentasi, tanpa memerlukan interaksi langsung dengan subjek penelitian.

Sumber data dalam penelitian ini terdiri atas dua kategori. Pertama, publikasi akademik nasional dan internasional yang membahas etika profesi keamanan siber, insiden kebocoran data di Indonesia, kompetensi dan sertifikasi tenaga kerja, strategi keamanan siber nasional, serta kerangka manajemen keamanan informasi seperti ISO/IEC 27001. Kedua, dokumen resmi kode etik yang diterbitkan langsung oleh lembaga penyelenggara sertifikasi, yaitu ISC2 Code of Ethics dari (ISC)² dan Code of Professional Ethics dari ISACA, yang digunakan sebagai rujukan primer untuk memahami ketentuan etika yang mengikat pemegang sertifikasi CISSP dan CISM.

Analisis data dilakukan melalui analisis tematik, di mana data dari berbagai sumber diklasifikasikan ke dalam tema-tema utama, yaitu: (a) lanskap ancaman dan kesiapan siber Indonesia; (b) kasus pelanggaran etika profesi keamanan siber yang terdokumentasi; (c) ketentuan dan cakupan kode etik CISSP dan CISM; serta (d) tantangan implementasi sertifikasi profesional di Indonesia. Tema-tema tersebut kemudian dipetakan secara silang untuk mengidentifikasi keterkaitan antara prinsip etika yang dilanggar dalam kasus nyata dengan ketentuan kode etik yang diatur dalam CISSP dan CISM, sebagai dasar untuk merumuskan temuan dan rekomendasi kebijakan.

Pemilihan sumber dilakukan dengan kriteria inklusi berupa publikasi terbitan tahun 2019 hingga 2026, relevansi langsung dengan etika profesi, sertifikasi, atau tata kelola keamanan siber, serta ketersediaan teks lengkap; tulisan populer tanpa dasar data dan artikel yang tidak dapat ditelusuri sumber primernya dikeluarkan dari analisis. Untuk menjaga keabsahan temuan, penelitian menerapkan triangulasi sumber dengan membandingkan deskripsi kasus dari sekurang-kurangnya dua publikasi berbeda, dan setiap klaim mengenai isi kode etik diverifikasi langsung pada dokumen resmi (ISC)² dan ISACA sebagai rujukan primer, bukan pada kutipan sekunder. Sebanyak 18 sumber digunakan dalam analisis akhir, terdiri atas artikel jurnal nasional dan internasional, dokumen kode etik resmi lembaga sertifikasi, serta dokumen kebijakan dan kelembagaan keamanan siber nasional.



Gambar 1. Gambar Alur Tahapan Penelitian

4. HASIL DAN PEMBAHASAN

4.1. Pemetaan Pelanggaran Etika pada Kasus Nyata di Indonesia

Analisis terhadap dua kasus kebocoran data besar di Indonesia, yaitu kebocoran data pajak yang melibatkan lebih dari 20 juta wajib pajak [5] dan kebocoran data nasabah BSI [7], menunjukkan pola yang konsisten: pelanggaran terjadi pada empat prinsip etika utama, yaitu kerahasiaan, integritas, akuntabilitas, dan transparansi. Pada kasus kebocoran data pajak, kelalaian pegawai dalam pengelolaan data serta minimnya pengawasan pihak berwenang menjadi penyebab utama, sementara pada kasus BSI, lemahnya integritas dan akuntabilitas profesional teknologi informasi menjadi faktor kontributor meski sistem keamanan teknis telah diterapkan [6]. Kesamaan pola ini memperkuat argumen bahwa akar persoalan keamanan siber di Indonesia tidak semata teknis, melainkan berpusat pada lemahnya standar etika profesi yang terinternalisasi dan dapat diaudit.

Tabel 2. Pemetaan pelanggaran prinsip etika pada siklus pengelolaan data

Tahap siklus data	Prinsip dilanggar	Bentuk kegagalan
Penyimpanan dan akses	Kerahasiaan	Data pribadi terambil pihak tidak berwenang tanpa terdeteksi

Pemrosesan	Integritas	Pemegang hak akses istimewa tidak menjalankan kewajiban profesional
Pascainsiden	Akuntabilitas	Tidak ada pihak yang menjelaskan rantai kelalaian secara terbuka
Komunikasi publik	Transparansi	Pengungkapan insiden berjalan lambat dan tidak lengkap

Tabel 2 menjawab pertanyaan mengapa kontrol teknis yang telah tersedia tetap gagal mencegah insiden: kontrol tersebut dioperasikan oleh personel yang tidak terikat pada standar etika yang dapat ditegakkan dan diaudit. Sebaran pelanggaran pada seluruh tahap siklus juga menunjukkan bahwa titik kritis perlindungan data tidak berhenti pada tahap penyimpanan, melainkan berlanjut sampai tahap pengungkapan kepada pemilik data. Dengan demikian, evaluasi kesiapan organisasi tidak cukup diarahkan pada kekuatan kontrol akses semata, tetapi perlu mencakup kesiapan dalam mempertanggungjawabkan keputusan profesionalnya pada setiap tahapannya.

Pola tersebut juga memperlihatkan bahwa kegagalan etika bersifat berlapis dan berurutan, bukan berdiri sendiri pada satu titik. Kelalaian pada tahap awal, misalnya klasifikasi data yang tidak tegas, memperbesar dampak kelalaian pada tahap berikutnya, sementara ketiadaan akuntabilitas pascainsiden menghilangkan umpan balik yang seharusnya memperbaiki proses. Dalam kedua kasus, tidak ditemukan mekanisme profesi yang dapat menuntut pertanggungjawaban personal di luar jalur hukum pidana, sehingga konsekuensi pelanggaran nyaris seluruhnya ditanggung institusi, bukan individu yang menjalankan kewenangan teknis. Kondisi inilah yang menjadikan standar etika bersertifikasi relevan, karena ia menempatkan tanggung jawab pada individu yang memegang akses istimewa.

4.2. Kontribusi CISSP terhadap Penguatan Etika Praktisi

Kontribusi CISSP terhadap penguatan etika praktisi keamanan siber dapat ditelusuri dari keterkaitan langsung antara empat kanon ISC2 Code of Ethics dengan prinsip-prinsip yang terbukti dilanggar dalam kasus-kasus nyata di Indonesia. Kanon pertama, melindungi masyarakat, kepentingan umum, kepercayaan publik, dan infrastruktur, secara langsung merespons persoalan kerahasiaan data yang menjadi akar kebocoran data pajak, di mana data pribadi lebih dari 20 juta wajib pajak seharusnya dilindungi sebagai bagian dari kepercayaan publik terhadap institusi pemerintah [5]. Kanon kedua, bertindak terhormat, jujur, adil, bertanggung jawab, dan sesuai hukum, menekankan pentingnya integritas personel yang memiliki akses terhadap data sensitif, sejalan dengan temuan bahwa lemahnya integritas menjadi faktor kontributor dalam kasus kebocoran data BSI [6], [7].

Kanon ketiga dan keempat, yakni memberikan layanan yang cermat dan kompeten serta memajukan dan melindungi profesi, menegaskan bahwa kompetensi teknis semata tidak cukup tanpa disertai kesungguhan profesional dalam menjalankan tugas, gagasan yang selaras dengan pandangan bahwa etika berperan mengisi celah yang tidak mampu dijangkau oleh kontrol teknis maupun hukum [8]. Cakupan delapan domain teknis CISSP memastikan bahwa pemegang sertifikasi memiliki kompetensi luas untuk menerapkan prinsip-prinsip etika tersebut secara konkret, bukan sekadar memahaminya secara normatif.

Selain kanon etik, delapan domain CISSP memberikan jalur konkret untuk menerjemahkan etika menjadi praktik. Domain manajemen risiko keamanan menuntut pemegang sertifikasi menilai risiko privasi sebelum sistem dioperasikan; domain keamanan aset mewajibkan klasifikasi dan penanganan data sesuai tingkat kerahasiaannya; sedangkan domain keamanan operasi menuntut pencatatan aktivitas akses istimewa yang dapat diaudit. Ketiga domain tersebut menyasar langsung titik kegagalan yang teridentifikasi pada kasus kebocoran data pajak dan BSI, yaitu penilaian risiko yang tidak dilakukan,

klasifikasi data yang tidak tegas, serta jejak audit yang tidak memadai [5], [7].

Dibandingkan dengan penelitian terdahulu yang menempatkan etika sebagai variabel normatif tanpa mekanisme penegakan [8], [12], temuan ini menunjukkan kebaruan pada aspek keterikatan administratif. Kode etik CISSP tidak berhenti sebagai pernyataan nilai, melainkan melekat pada status sertifikasi yang dapat ditinjau dan dicabut oleh panel sejawat, sehingga pelanggaran memiliki konsekuensi karier yang nyata. Dengan demikian, CISSP menghadirkan apa yang belum disediakan oleh imbauan moral maupun regulasi yang berorientasi sanksi pidana, yaitu sanksi profesi yang bekerja pada tingkat individu dan berlaku lintas yurisdiksi.

4.3. Kontribusi CISM terhadap Penguatan Etika dan Tata Kelola

Sementara CISSP menekankan keluasan teknis, CISM memperkuat dimensi tata kelola dan akuntabilitas institusional yang menjadi titik lemah berulang dalam kasus-kasus keamanan siber di Indonesia. Ketentuan dalam Code of Professional Ethics ISACA yang mewajibkan pemegang sertifikasi untuk mendukung tata kelola sistem informasi perusahaan, bertindak objektif dan cermat, serta menjaga kerahasiaan informasi [11], secara langsung relevan dengan persoalan akuntabilitas yang muncul ketika pihak berwenang dalam kasus kebocoran data pajak tidak dapat menjelaskan kelalaian yang terjadi [5]. Empat domain CISM juga sejalan dengan rekomendasi kebijakan yang mendesak pembentukan lembaga independen lintas sektor dan kewajiban pelaporan insiden dalam Strategi Nasional Keamanan Siber [4]. Dengan kata lain, kompetensi manajerial yang disyaratkan CISM berpotensi menjembatani kesenjangan kelembagaan yang telah lama diidentifikasi sejak awal pembentukan BSSN, di mana penanganan keamanan siber di Indonesia masih bersifat parsial dan sektoral [18].

Perbedaan orientasi ini menjelaskan mengapa kedua sertifikasi tidak dapat saling menggantikan. Kasus kebocoran data di Indonesia memperlihatkan kegagalan ganda: kegagalan pada tingkat pelaksana teknis yang menjadi ranah CISSP, dan kegagalan pada tingkat pengambil keputusan yang menjadi ranah CISM. Ketika organisasi hanya memiliki personel teknis bersertifikasi tanpa manajemen yang terikat kode etik tata kelola, keputusan mengenai alokasi sumber daya, pelaporan insiden, dan komunikasi publik tetap berada di luar kerangka etika profesi. Sebaliknya, kepemimpinan bersertifikasi tanpa pelaksana yang kompeten hanya menghasilkan kebijakan yang tidak terimplementasi.

Domain manajemen insiden pada CISM juga menjawab persoalan transparansi yang menonjol pada kedua kasus. Standar kompetensi CISM mensyaratkan adanya rencana respons insiden yang mencakup prosedur komunikasi kepada pemangku kepentingan, termasuk pemilik data. Apabila prosedur semacam ini melekat pada kompetensi wajib manajemen keamanan, keterlambatan dan ketidaklengkapan pengungkapan insiden dapat ditekan, karena pengungkapan tidak lagi bergantung pada pertimbangan reputasi jangka pendek organisasi, melainkan pada kewajiban profesional yang telah disepakati.

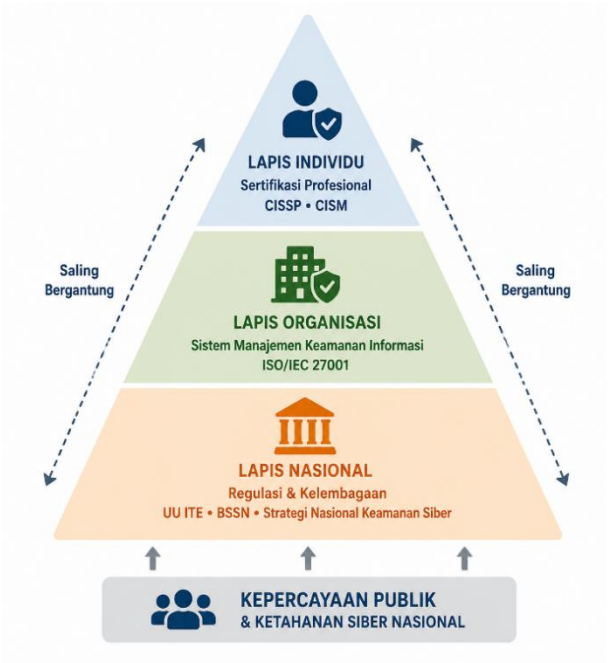
4.4. Kerangka Konseptual: Sertifikasi sebagai Lapisan Etika dalam Ekosistem Keamanan Siber

Untuk merangkum keterkaitan antara sertifikasi profesional, manajemen organisasi, dan regulasi nasional, penelitian ini mengusulkan kerangka konseptual tiga lapis sebagaimana digambarkan pada Gambar 2. Pada lapis individu, kode etik CISSP dan CISM menjadi pengikat perilaku personel. Pada lapis organisasi, standar seperti ISO/IEC 27001 menerjemahkan komitmen etika individu ke dalam sistem manajemen keamanan informasi yang terstruktur [16]. Pada lapis nasional, regulasi seperti UU ITE [1] dan kelembagaan seperti BSSN serta Strategi Nasional Keamanan Siber menetapkan kerangka hukum dan kelembagaan yang menaungi keseluruhan ekosistem [4], [18].

Ketiga lapis ini saling bergantung: lemahnya salah satu lapis, sebagaimana terlihat pada kasus kebocoran data pajak dan BSI, dapat menggerus kepercayaan publik terhadap keseluruhan sistem. Struktur berlapis ini sejalan dengan temuan [3], yang menyimpulkan bahwa ketahanan siber nasional bertumpu pada

keterpaduan pilar sosial, regulatif, dan teknis. Perbedaannya, kerangka yang diusulkan dalam penelitian ini menempatkan etika profesi bersertifikasi sebagai perekat yang menghubungkan ketiga lapis tersebut, sehingga penguatan kapasitas individu tidak berhenti pada aspek literasi, melainkan terikat pada kode etik yang dapat ditegakkan.

Implikasi teoretis dari kerangka ini adalah bahwa etika profesi perlu diposisikan sebagai variabel penghubung, bukan sebagai atribut individual yang berdiri sendiri. Kerangka tiga lapis juga memberi cara membaca kegagalan sistem secara diagnostik: setiap insiden dapat ditelusuri untuk menentukan lapis mana yang tidak berfungsi, sehingga intervensi kebijakan dapat diarahkan secara lebih tepat sasaran daripada sekadar menambah kontrol teknis.



Gambar 2. Kerangka konseptual tiga lapis etika keamanan siber

4.5. Perbandingan Peran CISSP dan CISM

CISSP dan CISM tidak berada dalam posisi saling menggantikan, melainkan saling melengkapi pada dua lapis yang berbeda dalam ekosistem keamanan siber. CISSP berfokus pada implementasi kontrol keamanan dari sisi teknis, sedangkan CISM menekankan pengelolaan keamanan informasi melalui tata kelola dan pengambilan keputusan strategis.

Tabel 3. Peran perbandingan CISSP dan CISM dalam mendukung standar etika praktisi keamanan siber

Aspek	CISSP	CISM
Fokus	Teknis dan operasional	Manajerial dan strategis
Peran	Implementasi kontrol keamanan	Tata kelola dan manajemen keamanan
Kode etik	ISC² Code of Ethics	ISACA Code of Professional Ethics
Kontribusi etika	Menjaga kepatuhan pada praktik teknis	Menjamin akuntabilitas organisasi

Tabel 3 memperlihatkan bahwa perbedaan keduanya bersifat komplementer, bukan hierarkis. CISSP menyediakan kedalaman pada tataran pelaksanaan kontrol, sedangkan CISM menyediakan legitimasi pada tataran pengambilan keputusan. Pada organisasi pengelola infrastruktur informasi kritis, kombinasi keduanya membentuk rantai pertanggungjawaban yang utuh, mulai dari personel yang mengonfigurasi kontrol keamanan hingga pimpinan yang menetapkan kebijakan dan bertanggung jawab atas pengungkapan insiden. Ketiadaan salah satu sisi menyebabkan rantai tersebut terputus, dan pada titik itulah pelanggaran etika paling sering terjadi tanpa ada pihak yang dapat dimintai tanggung jawab secara profesional. Implikasinya, kebutuhan sertifikasi pada organisasi di Indonesia tidak dapat dinilai semata dari jumlah personel bersertifikat, melainkan dari sebaran perannya pada posisi teknis maupun tata kelola.

4.6. Tantangan Implementasi CISSP dan CISM di Indonesia

Meskipun secara konseptual CISSP dan CISM menawarkan kerangka etika yang kuat, penerapannya di Indonesia masih menghadapi sedikitnya lima tantangan struktural yang saling berkaitan. Pertama, jumlah tenaga ahli keamanan siber yang kompeten dan bersertifikasi masih jauh dari kebutuhan, sehingga organisasi kerap menempatkan personel tanpa latar kompetensi yang memadai pada posisi dengan hak akses istimewa [2].

Kedua, jenjang pelatihan yang tersedia umumnya berhenti pada tingkat pengenalan dasar dan belum menyambung ke tingkat sertifikasi internasional, sehingga peserta pelatihan tidak memiliki jalur lanjutan yang jelas [14]. Ketiga, prioritas investasi organisasi masih condong pada pengadaan perangkat keamanan dibandingkan penguatan kompetensi dan etika sumber daya manusia [15]. Keempat, belum terdapat kebijakan yang mewajibkan kepemilikan sertifikasi bagi pengelola infrastruktur informasi kritis [4]. Kelima, biaya pemeliharaan status sertifikasi melalui kewajiban pendidikan profesional berkelanjutan menyulitkan praktisi mempertahankan sertifikasinya dalam jangka panjang.

Kelima tantangan tersebut tidak berdiri sendiri, melainkan membentuk lingkaran yang saling menguatkan: keterbatasan anggaran menekan jumlah personel bersertifikasi, jumlah yang terbatas membuat sertifikasi tidak dapat dijadikan prasyarat jabatan, dan ketiadaan prasyarat membuat organisasi tidak terdorong menganggarkan pembiayaannya. Kondisi ini beresonansi dengan temuan pada isu etika profesional TIK lainnya di Indonesia, yaitu bahwa norma dan kampanye etika semata tidak cukup mengubah perilaku tanpa dukungan kebijakan organisasi dan mekanisme kontrol yang dapat diaudit [13]. Memutus lingkaran tersebut karenanya menuntut intervensi kebijakan pada beberapa titik sekaligus, bukan pada satu tantangan secara terpisah.

Jika dibandingkan dengan praktik di sejumlah negara yang telah menetapkan kualifikasi minimum bagi pengelola infrastruktur informasi kritis, Indonesia belum memiliki instrumen serupa yang mengikat, sehingga kepemilikan sertifikasi masih diperlakukan sebagai keunggulan kompetitif individu, bukan sebagai prasyarat jabatan. Ketiadaan prasyarat tersebut menyulitkan organisasi menilai kesiapan etika calon personel karena tidak tersedia tolok ukur yang seragam dan dapat diverifikasi.

4.7. Implikasi dan Rekomendasi Kebijakan

Berdasarkan temuan tersebut, penelitian ini mengajukan empat rekomendasi kebijakan. Pertama, lembaga seperti BSSN maupun regulator sektoral dapat mempertimbangkan untuk mensyaratkan atau memberi insentif kepemilikan sertifikasi CISSP dan/atau CISM bagi personel yang mengelola data sensitif pada sektor infrastruktur informasi kritis, khususnya perpajakan dan perbankan, mengingat kedua sektor tersebut telah mengalami insiden kebocoran data berskala besar [5], [7]. Kedua, konten Common Body of Knowledge CISSP dan domain CISM, khususnya bagian kode etiknya, dapat diintegrasikan ke dalam kurikulum pendidikan tinggi bidang teknologi informasi di Indonesia, mengingat kompetensi dan sertifikasi terbukti berkontribusi terhadap produktivitas dan profesionalisme kerja [9].

Ketiga, pemerintah dapat memperluas skema pelatihan bersubsidi yang telah dirintis pada tingkat kepolisian daerah [14] menjadi jenjang berkelanjutan menuju sertifikasi internasional, guna mengurangi hambatan biaya yang selama ini membatasi partisipasi tenaga kerja Indonesia dalam sertifikasi CISSP dan CISM. Keempat, penguatan sertifikasi individu perlu diselaraskan dengan kerja sama regional, termasuk integrasi kebijakan dengan Kerangka Kerja Sama Keamanan Siber ASEAN 2025 yang menekankan penguatan sumber daya manusia siber sebagai salah satu pilar utama [4].

Rekomendasi tersebut dapat diterapkan secara bertahap, dimulai dari pemetaan kebutuhan kompetensi pada sektor infrastruktur informasi kritis oleh regulator, penetapan target jumlah personel bersertifikasi beserta skema pembiayaannya, pengikatan kode etik profesi ke dalam perjanjian kerja dan prosedur operasional organisasi, hingga evaluasi berkala terhadap kepatuhan etika sebagai bagian dari audit keamanan informasi. Kemajuannya dapat dipantau melalui rasio personel bersertifikasi pada posisi dengan hak akses istimewa, ketersediaan prosedur penanganan pelanggaran etika, serta ketepatan waktu pengungkapan insiden kepada pemilik data, dengan lembaga sertifikasi dan perguruan tinggi berperan menyediakan jalur pelatihan yang menyambungkan tingkat dasar dengan tingkat sertifikasi internasional. Dengan pembagian peran yang eksplisit, penguatan etika menjadi terukur dan dapat diaudit, bukan sekadar pernyataan komitmen dalam dokumen kebijakan.

Secara teoretis, temuan ini memperluas kajian etika profesi keamanan siber yang selama ini didominasi pendekatan normatif, dengan menunjukkan bahwa sertifikasi berfungsi sebagai mekanisme institusionalisasi etika yang menghubungkan nilai individu dengan tata kelola organisasi dan regulasi nasional. Secara praktis, kerangka tiga lapis yang diusulkan dapat digunakan organisasi sebagai instrumen evaluasi mandiri untuk menilai apakah kepatuhan etika telah tertanam pada setiap lapis, tidak hanya pada dokumen kebijakan.

Penelitian ini memiliki keterbatasan. Analisis bersifat kualitatif dan bertumpu pada sumber sekunder yang tersedia secara publik, sehingga belum dapat mengukur secara kuantitatif besarnya pengaruh kepemilikan sertifikasi terhadap penurunan insiden. Kasus yang dianalisis juga terbatas pada dua insiden berskala besar sehingga generalisasi temuan perlu dilakukan secara hati-hati.

5. KESIMPULAN

1) Sertifikasi CISSP dan CISM berperan saling melengkapi dalam mendukung standar etika praktisi keamanan siber di Indonesia. CISSP memperkuat dimensi teknis dan kepatuhan individual melalui empat kanon ISC2 Code of Ethics, sedangkan CISM memperkuat dimensi tata kelola dan akuntabilitas institusional melalui Code of Professional Ethics ISACA.
2) Pemetaan terhadap dua kasus kebocoran data berskala besar di Indonesia menunjukkan bahwa pelanggaran prinsip kerahasiaan, integritas, akuntabilitas, dan transparansi telah tercakup secara eksplisit dalam ketentuan kode etik kedua sertifikasi, sehingga adopsinya berpotensi menjadi instrumen mitigasi risiko serupa pada masa mendatang.
3) Kerangka konseptual tiga lapis yang diusulkan menempatkan etika profesi bersertifikasi sebagai penghubung antara lapis individu, organisasi, dan nasional, sekaligus menjadi alat diagnostik untuk menelusuri lapis mana yang tidak berfungsi ketika insiden terjadi.
4) Pendekatan berbasis sertifikasi memiliki keunggulan berupa penegakan sanksi profesi lintas yurisdiksi. Namun, penerapannya masih terbatas karena bersifat sukarela, terkendala biaya dan ketersediaan SDM, serta belum diwajibkan pada sektor infrastruktur informasi kritis.
5) Pengembangan selanjutnya disarankan berupa kajian empiris kuantitatif untuk menguji korelasi antara kepemilikan sertifikasi CISSP dan CISM dengan tingkat kepatuhan etika dan insiden keamanan, serta perumusan kebijakan yang mengintegrasikan standar etika bersertifikasi ke dalam kebijakan sumber daya manusia nasional dan kurikulum pendidikan tinggi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, UIN Syarif Hidayatullah Jakarta atas dukungan akademik selama penyusunan artikel ini, serta kepada para reviewer atas masukan yang membangun.

DAFTAR PUSTAKA

[1] R. Hikmatulloh and E. Nurmiati, “Analisis Strategi Pencegahan Cybercrime Berdasarkan UU ITE Di Indonesia (Studi Kasus: Penipuan Pelanggan Gojek),” *Kosmik Hukum*, vol. 20, no. 2, pp. 121–127, Jul. 2020, doi: 10.30595/kosmikhukum.v20i2.6449.

[2] I. I. Megasari and Y. H. Azzahra, “Tantangan dan Kesiapan Indonesia Menghadapi Ancaman Siber,” *Civic Education Perspective Journal*, vol. 5, no. 2, pp. 53–66, 2025.

[3] R. Wijaya and D. Juardi, “Edukasi Masyarakat Tentang Keamanan Siber Dalam Tantangan Dan Solusi Di Era Digital,” *JITET (Jurnal Informatika dan Teknik Elektro Terapan)*, vol. 14, no. 1, pp. 298–305, 2026, doi: 10.23960/jitet.v14i1.8336.

[4] I. Aryasatya, S. Riyanta, and E. Daryanto, “Analisis Kebijakan Keamanan Siber Indonesia dalam Strategi Nasional Keamanan Siber,” *Jurnal Impresi Indonesia (JII)*, vol. 5, no. 3, pp. 1411–1427, 2026.

[5] F. Pritama, E. R. D. Leluni, Yovita, and J. Parhusip, “Analisis Pelanggaran Etika Profesi Keamanan Siber (Studi Kasus Kebocoran Data Pajak di Indonesia),” *Teknik: Jurnal Ilmu*

Teknik dan Informatika, vol. 4, no. 2, pp. 53–56, Oct. 2024, doi: 10.51903/teknik.

[6] S. Anugrah, N. Raihana Qalby, M. Z. Himawan, and E. Nurmiati, "Pengaruh Etika Profesi Terhadap Keamanan Informasi dalam Konteks Kebocoran Data BSI (Bank Syariah Indonesia): Studi Literatur Sistematis," *JTK3TI: Jurnal Tata Kelola dan Kerangka Kerja Teknologi Informasi*, vol. 11, no. 2, pp. 106–112, 2025.

[7] A. Permana, A. B. Ayogi, A. L. Bagaskara, and R. M. Saputra, "Pengaruh Etika Profesi Terhadap Keamanan Informasi dalam Konteks Kebocoran Data BSI (Bank Syariah Indonesia): Studi Literatur Sistematis," *TEKNOBIS : Teknologi, Bisnis Dan Pendidikan*, vol. 3, no. 2, pp. 348–354, 2025, [Online]. Available: https://jurnalmahasiswa.com/index.php/teknobis

[8] T. Aşuroğlu and C. Gemci, "Role of Ethics in Information Security," *International Conference on Advanced Technology & Sciences (ICAT'16)*, vol. 1, no. 3, Sep. 2016.

[9] A. Afif, Reniati, and A. A. Nugroho, "The Effect of Competency and Certification on Work Productivity: The Mediating Role of Motivation," *International Journal of Economics, Business, and Entrepreneurship* |, vol. 8, no. 1, p. 100, 2025.

[10] ISC2, "ISC2 Code of Ethics." Accessed: Jul. 15, 2026. [Online]. Available: https://www.isc2.org/ethics

[11] ISACA, "Code of Professional Ethics." Accessed: Jul. 15, 2026. [Online]. Available: https://www.isaca.org/code-of-professional-ethics

[12] D. Y. Zebua and A. P. Zebua, "TANTANGAN ETIKA DALAM PROFESI TEKNOLOGI INFORMASI," *IDENTIK: Jurnal Ilmu Ekonomi, Pendidikan dan Teknik*, vol. 2, no. 1, pp. 35–44, Jan. 2025.

[13] Hendrawan, L. S. Udi, I. G. Prayogo, Abdul, and A. Cahyadi, "Kesenjangan Etika Profesional TIK dan Perangkat Lunak Bajakan: Kajian Literatur Kontekstual Indonesia," *Jurnal Teknik Informatika dan Teknologi Informasi*, vol. 5, no. 3, pp. 18–28, Oct. 2025, doi: 10.55606/jutiti.v5i3.6072.

[14] M. M. Alamin, A. S. Editya, N. Kurniati, A. L. Pramana, and A. Lisdiyanto, "Peningkatan Kualitas SDM Melalui Pelatihan Cyber Security Pada Anggota Polisi Daerah Jawa Timur," *PARTA: Jurnal Pengabdian Kepada Masyarakat*, vol. 4, no. 2, pp. 150–155, Dec. 2023, [Online]. Available: http://journal.undiknas.ac.id/index.php/parta.

[15] M. F. Aska, D. pratama Putta, and C. J. M. Sinambela, "Strategi Efektif Untuk Implementasi Keamanan Siber di Era Digital," *Journal of Information and Information Security (JIFORTY)*, vol. 5, no. 2, pp. 187–200, Jan. 2025, [Online]. Available: http://ejurnal.ubharajaya.ac.id/index.php/jiforty

[16] Nurbojatmiko, M. S. K. Karimiyah, N. M. Asnadi, and R. Anisyah, "ISO 27001 as Information Security Solution in Society 5.0 Era: Systematic Literature Review," *Sinkron: Jurnal dan Penelitian Teknik Informatika*, vol. 9, no. 1, pp. 484–492, Feb. 2025, doi: 10.33395/sinkron.v9i1.14448.

[17] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," Mar. 16, 2021, *Emerald Group Holdings Ltd.* doi: 10.1108/TQM-09-2020-0202.

[18] D. A. Sudarmadi and A. J. S. Runturambi, "Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia," *Jurnal Kajian Stratejik Ketahanan Nasional*, vol. 2, no. 2, pp. 163–183, Dec. 2019, doi: 10.7454/jkskn.v2i2.10028.