

BAB II

KAJIAN LITERATUR

2.1 Informasi

Informasi merupakan hasil pengolahan data yang telah diberi makna sehingga dapat digunakan untuk memahami suatu kondisi, mengurangi ketidakpastian, dan mendukung pengambilan keputusan. Dengan demikian, informasi tidak hanya dipahami sebagai sekumpulan data, tetapi sebagai data yang telah diproses, diorganisasi, dan disajikan dalam bentuk yang lebih bermakna bagi pengguna. Dalam konteks sistem informasi, informasi memiliki peran penting karena menjadi dasar dalam pelaksanaan aktivitas operasional, pengendalian, dan pengambilan keputusan baik pada tingkat individu maupun organisasi [21].

Secara umum, data dan informasi memiliki perbedaan yang mendasar. Data merupakan fakta mentah yang belum diolah, sedangkan informasi adalah data yang telah diproses menjadi bentuk yang lebih bermakna dan berguna bagi penerima. Oleh karena itu, kualitas informasi menjadi hal yang sangat penting. Informasi yang baik umumnya harus memiliki karakteristik seperti akurasi, relevansi, kelengkapan, dan ketepatan waktu, sehingga dapat digunakan secara efektif dalam mendukung kebutuhan pengguna [22].

Dalam era digital, informasi juga dipandang sebagai aset yang bernilai karena berperan penting dalam berbagai aktivitas elektronik, termasuk transaksi digital. Informasi dapat berupa identitas pengguna, data akun, riwayat transaksi, kode autentikasi, maupun bentuk data elektronik lainnya yang memerlukan pengelolaan dan perlindungan yang baik. Pada layanan digital seperti *mobile banking*, informasi yang diproses bersifat sensitif karena berkaitan langsung dengan data pribadi dan aktivitas keuangan pengguna. Oleh karena itu, pemahaman mengenai informasi menjadi dasar yang penting sebelum membahas lebih lanjut mengenai keamanan informasi dan kesadaran keamanan informasi [23].

Berdasarkan uraian tersebut, informasi merupakan data yang telah diolah sehingga memiliki makna dan nilai guna bagi pengguna dalam mendukung pengambilan keputusan. Dalam konteks digital, informasi juga menjadi aset penting yang perlu dikelola dan dilindungi dengan baik, terutama karena berkaitan dengan data yang bersifat sensitif.

2.2 Keamanan Informasi

Keamanan informasi merupakan serangkaian tindakan yang bertujuan untuk menjaga data dari ancaman, penyalahgunaan, serta akses tidak sah sehingga aspek

kerahasiaan, keutuhan, dan ketersediaannya tetap terjamin selama proses pengolahan maupun penyimpanan data. Menurut *National Institute of Standards and Technology* (NIST) [24], keamanan informasi bertujuan untuk menjamin kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi sebagai tiga pilar utama perlindungan sistem informasi [25].

Standar internasional yang dikembangkan oleh *International Organization for Standardization* (ISO/IEC 27001) juga menegaskan bahwa keamanan informasi merupakan bagian dari sistem manajemen organisasi yang berbasis pada pendekatan risiko (*risk-based approach*), yang mencakup kebijakan, prosedur, struktur organisasi, serta kontrol teknis untuk melindungi aset informasi. Dengan demikian, keamanan informasi tidak hanya bersifat teknis, tetapi juga manajerial dan perilaku pengguna [26].

Salah satu konsep fundamental yang digunakan dalam menjelaskan keamanan informasi adalah CIA Triad, yang terdiri atas *Confidentiality*, *Integrity*, dan *Availability*. *Confidentiality* mengacu pada perlindungan informasi agar hanya dapat diakses oleh pihak yang berwenang. *Integrity* berkaitan dengan jaminan bahwa informasi tetap akurat dan tidak dimodifikasi tanpa otoritas yang sah. Sementara itu, *availability* memastikan bahwa informasi dan sistem tetap dapat diakses ketika dibutuhkan oleh pengguna yang sah. Ketiga aspek ini saling melengkapi dan menjadi dasar dalam perancangan kebijakan serta kontrol keamanan informasi [27].

Di era digital saat ini, ancaman terhadap keamanan informasi semakin kompleks. Studi yang dilakukan oleh Parsons *et al.* menunjukkan bahwa faktor manusia sering kali menjadi penyebab utama terjadinya pelanggaran keamanan informasi, meskipun sistem telah dilengkapi dengan mekanisme teknis yang memadai. Hal ini menunjukkan bahwa keamanan informasi tidak hanya bergantung pada teknologi, tetapi juga pada tingkat kesadaran dan perilaku pengguna dalam menjaga keamanan data. Dengan kata lain, pengguna menjadi salah satu komponen penting dalam sistem keamanan informasi karena tindakan yang tidak hati-hati dapat membuka celah bagi terjadinya serangan siber [8].

Dalam konteks layanan keuangan digital seperti *mobile banking*, penerapan prinsip CIA menjadi sangat penting karena melibatkan data finansial yang bersifat sensitif. Pelanggaran terhadap salah satu aspek CIA dapat menimbulkan kerugian finansial serta menurunkan kepercayaan pengguna terhadap institusi perbankan. Oleh karena itu, selain penguatan sistem teknis, diperlukan pengukuran tingkat kesadaran keamanan informasi pengguna sebagai bagian dari strategi mitigasi risiko [8,24].

Berdasarkan uraian tersebut, keamanan informasi dalam penelitian ini menjadi landasan konseptual untuk memahami pentingnya pengukuran *Information Security Awareness* pada pengguna *mobile banking*, khususnya dalam menjaga kerahasiaan kredensial, keutuhan transaksi, dan ketersediaan layanan keuangan digital.

2.3 Mobile Banking BCA

Mobile banking merupakan layanan perbankan berbasis teknologi yang memungkinkan nasabah untuk melakukan berbagai transaksi keuangan melalui perangkat *mobile* seperti *smartphone* secara *real-time* tanpa harus mengunjungi kantor bank. Layanan ini hadir sebagai bagian dari transformasi digital di sektor perbankan yang bertujuan untuk meningkatkan kemudahan, efisiensi, dan aksesibilitas layanan keuangan bagi masyarakat. Melalui *mobile banking*, nasabah dapat melakukan berbagai aktivitas seperti transfer dana, pembayaran tagihan, pembelian produk digital, serta pengecekan saldo dan mutasi rekening dengan lebih praktis dan cepat [28,29].

Salah satu bank yang menyediakan layanan *mobile banking* di Indonesia adalah Bank Central Asia. Layanan *mobile banking* memberikan kemudahan bagi nasabah dalam mengakses layanan perbankan secara digital kapan saja dan di mana saja. Fitur yang tersedia meliputi transfer antar rekening, transfer antar bank, pembayaran berbagai tagihan, pembelian pulsa dan paket data, serta akses informasi rekening secara *real-time*. Kehadiran *mobile banking* BCA menjadi salah satu bentuk inovasi layanan digital yang banyak dimanfaatkan oleh masyarakat dalam mendukung aktivitas keuangan sehari-hari [28,29].

Dalam mendukung keamanan transaksi, layanan *mobile banking* juga dilengkapi dengan berbagai fitur keamanan yang dirancang untuk melindungi data dan aktivitas pengguna. Beberapa fitur keamanan tersebut antara lain penggunaan PIN (*Personal Identification Number*) sebagai autentikasi utama dalam setiap transaksi, sistem *One-Time Password* (OTP) sebagai verifikasi tambahan, serta penerapan enkripsi data untuk menjaga kerahasiaan informasi selama proses transaksi. Selain itu, BCA juga menyediakan fitur keamanan tambahan seperti autentikasi biometrik (sidik jari atau pengenalan wajah) serta mekanisme pengamanan berlapis untuk mencegah akses tidak sah. Penerapan fitur keamanan ini bertujuan untuk meminimalkan risiko penyalahgunaan akun serta meningkatkan kepercayaan pengguna dalam menggunakan layanan *mobile banking* [28,29].

Meskipun demikian, penggunaan layanan *mobile banking* tetap memiliki risiko keamanan informasi, terutama karena layanan ini melibatkan data yang bersifat sensitif seperti identitas pengguna, nomor rekening, PIN, serta kode autentikasi. Berbagai ancaman

keamanan seperti *phishing*, *smishing*, dan *social engineering* sering kali menargetkan pengguna *mobile banking* untuk memperoleh data tersebut secara ilegal. Oleh karena itu, pengguna dituntut untuk memiliki tingkat kesadaran keamanan informasi yang baik agar dapat menggunakan layanan *mobile banking* secara aman dan terhindar dari risiko penyalahgunaan data. Dengan demikian, *mobile banking* BCA menjadi objek yang relevan dalam penelitian ini untuk menganalisis tingkat kesadaran keamanan informasi pengguna [4,30].

Berdasarkan uraian tersebut, *mobile banking* BCA merupakan layanan perbankan digital yang memberikan kemudahan dalam melakukan transaksi keuangan sekaligus dilengkapi dengan berbagai fitur keamanan untuk melindungi data pengguna. Namun demikian, tingginya risiko ancaman keamanan digital menuntut pengguna untuk memiliki tingkat kesadaran keamanan informasi yang baik agar dapat menggunakan layanan *mobile banking* secara aman dan terhindar dari potensi penyalahgunaan data [28,31].

2.4 Information Security Awareness (ISA)

2.4.1 Pengertian Information Security Awareness (ISA)

Information Security Awareness (ISA) merupakan konsep yang berfokus pada tingkat pemahaman, sikap, dan perilaku individu dalam menjaga keamanan informasi. ISA mencakup kemampuan pengguna dalam memahami ancaman keamanan informasi serta menerapkan praktik keamanan yang tepat dalam aktivitas digital sehari-hari. Parsons *et al.* menjelaskan bahwa kesadaran keamanan informasi berkaitan dengan kemampuan individu untuk mengenali potensi ancaman serta mengambil tindakan yang tepat untuk melindungi informasi dari berbagai risiko keamanan [8].

2.4.2 Pentingnya Information Security Awareness pada Pengguna Mobile banking

Tingkat kesadaran keamanan informasi memiliki peran yang sangat penting bagi pengguna dalam menggunakan teknologi digital secara aman dan bertanggung jawab. Kesadaran ini membantu pengguna memahami berbagai ancaman seperti *phishing*, pencurian data, *malware*, *social engineering*, serta berbagai bentuk penipuan digital lainnya. [32].

Selain itu, tingkat kesadaran keamanan informasi juga berpengaruh terhadap sikap dan perilaku pengguna dalam menerapkan praktik keamanan digital. Pengguna yang memiliki tingkat kesadaran keamanan informasi yang baik cenderung lebih berhati-hati dalam menggunakan kata sandi, menjaga kerahasiaan kode autentikasi, serta tidak mudah

mempercayai tautan atau informasi yang mencurigakan. Sebaliknya, rendahnya tingkat kesadaran keamanan informasi dapat meningkatkan risiko terjadinya kesalahan penggunaan teknologi yang berpotensi menyebabkan kebocoran data, penyalahgunaan akun, maupun kerugian finansial [33].

Dalam konteks penggunaan layanan *mobile banking*, tingkat kesadaran keamanan informasi menjadi sangat penting karena aktivitas transaksi melibatkan data yang bersifat sensitif, seperti identitas pengguna, data akun, kode autentikasi, dan riwayat transaksi keuangan. Pengguna yang memiliki tingkat kesadaran keamanan informasi yang baik akan lebih mampu menjaga keamanan akun dan transaksi digitalnya, sehingga dapat meminimalkan risiko terjadinya penyalahgunaan data maupun penipuan digital. Oleh karena itu, pengukuran tingkat kesadaran keamanan informasi pengguna menjadi penting untuk mengetahui sejauh mana kesiapan pengguna dalam menghadapi ancaman keamanan informasi saat menggunakan layanan *mobile banking* [15].

2.4.3 Pengukuran Skor *Information Security Awareness* (ISA)

Pengukuran tingkat *Information Security Awareness* dalam penelitian ini dilakukan menggunakan pendekatan *Knowledge, Attitude, and Behavior* (KAB), yang menilai hubungan antara pengetahuan, sikap, dan perilaku pengguna terhadap keamanan informasi. Untuk mengukur ketiga dimensi tersebut, digunakan instrumen *Human Aspects of Information Security Questionnaire* (HAIS-Q) yang dikembangkan oleh Parsons *et al.* Instrumen ini digunakan untuk mengevaluasi tingkat kesadaran keamanan informasi pengguna berdasarkan berbagai praktik keamanan dalam aktivitas digital [8,9].

Pengukuran Skor ISA dalam penelitian ini tidak dilakukan secara menyeluruh, melainkan dikasifikasikan ke dalam sembilan fokus area keamanan informasi. Hal ini bertujuan untuk menghasilkan pemetaan kesadaran yang lebih detail dan akurat pada setiap kategori keamanan yang diukur. Dengan memecah pengukuran ke dalam sembilan fokus area, peneliti dapat mengidentifikasi area mana yang memiliki tingkat kerentanan paling tinggi dan area mana yang sudah memiliki tingkat kesadaran yang baik. Penjelasan mendalam mengenai kesembilan fokus area tersebut akan dipaparkan pada subbab 2.6 mengenai instrumen HAIS-Q.

Secara teoretis, data yang diperoleh melalui instrumen ini akan merefleksikan pemetaan tingkat kesadaran pengguna yang terbagi ke dalam kategori tertentu. Hasil pengukuran ini memberikan gambaran objektif mengenai sejauh mana pengguna memahami risiko keamanan informasi serta kecenderungan mereka dalam menerapkan perilaku yang aman saat menggunakan layanan perbankan digital.

2.5 Model *Knowledge, Attitude, and Behavior* (KAB)

Model *Knowledge, Attitude, and Behavior* (KAB) merupakan pendekatan yang banyak digunakan dalam penelitian perilaku untuk menjelaskan hubungan antara pengetahuan, sikap, dan perilaku individu terhadap suatu isu tertentu. Dalam konteks keamanan informasi, model ini digunakan untuk memahami bagaimana tingkat pengetahuan dan sikap pengguna terhadap keamanan informasi dapat mempengaruhi perilaku mereka dalam menjaga keamanan data dan sistem informasi. Kruger dan Kearney menjelaskan bahwa kesadaran keamanan informasi dapat diukur melalui tiga komponen utama, yaitu pengetahuan (*knowledge*), sikap (*attitude*), dan perilaku (*behavior*), yang saling berkaitan dalam membentuk tingkat kesadaran keamanan informasi pengguna [7].

Model KAB menjelaskan bahwa peningkatan pengetahuan pengguna mengenai ancaman keamanan informasi dapat mempengaruhi sikap mereka terhadap pentingnya keamanan informasi. Sikap yang positif terhadap keamanan informasi selanjutnya akan mendorong terbentuknya perilaku yang lebih aman dalam penggunaan teknologi informasi. Dengan demikian, hubungan antara ketiga dimensi tersebut menjadi dasar dalam menilai tingkat kesadaran keamanan informasi pengguna [31,34].

Dalam penelitian mengenai keamanan informasi, pendekatan KAB sering digunakan untuk menganalisis perilaku pengguna terhadap praktik keamanan informasi dalam aktivitas digital sehari-hari. Parsons *et al.* menyatakan bahwa pengukuran kesadaran keamanan informasi dapat dilakukan dengan menilai hubungan antara pengetahuan, sikap, dan perilaku pengguna terhadap kebijakan dan praktik keamanan informasi yang berlaku dalam suatu sistem [8].

2.5.1 *Knowledge* (Pengetahuan)

Knowledge mengacu pada tingkat pemahaman individu terhadap ancaman keamanan informasi serta praktik yang diperlukan untuk menjaga keamanan data. Pengetahuan ini mencakup pemahaman mengenai berbagai jenis ancaman seperti *phishing*, *malware*, rekayasa sosial (*social engineering*), serta pentingnya menjaga kerahasiaan informasi seperti PIN, *password*, dan kode OTP dalam penggunaan layanan digital [8].

2.5.2 *Attitude* (Sikap)

Attitude berkaitan dengan persepsi dan tingkat kepedulian individu terhadap pentingnya keamanan informasi. Sikap yang positif terhadap keamanan informasi dapat

mendorong individu untuk lebih berhati-hati dalam menggunakan sistem teknologi informasi serta mematuhi kebijakan keamanan yang berlaku [8].

2.5.3 Behavior (Perilaku)

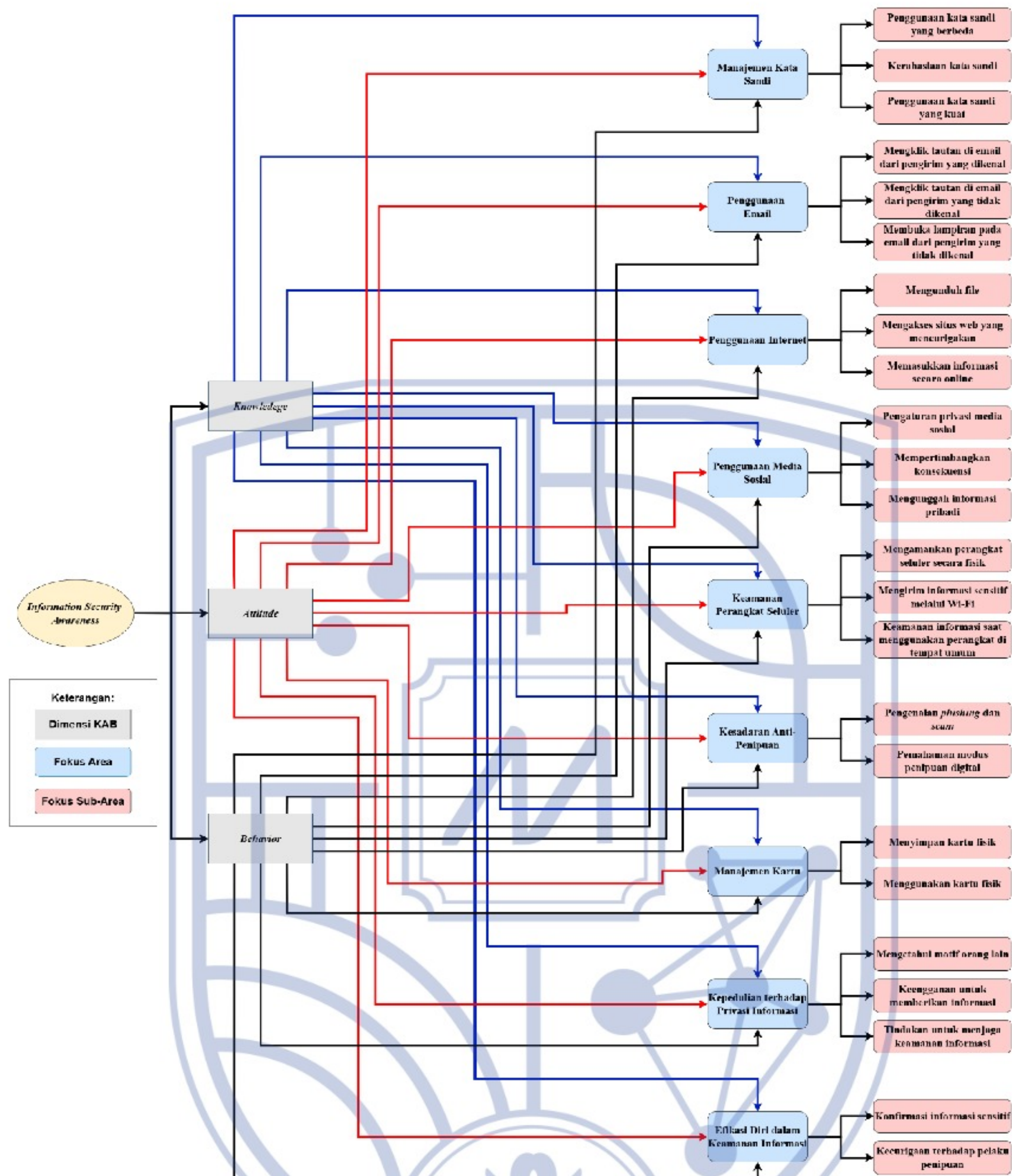
Behavior merupakan tindakan nyata individu dalam menjaga keamanan informasi, seperti tidak membagikan kode OTP kepada pihak lain, tidak mengklik tautan mencurigakan, serta menggunakan jaringan internet yang aman saat melakukan transaksi digital. Dimensi perilaku ini menjadi indikator penting dalam menilai sejauh mana pengguna menerapkan praktik keamanan informasi dalam aktivitas digital sehari-hari [8].

2.6 Human Aspects of Information Security Questionnaire (HAIS-Q)

Human Aspects of Information Security Questionnaire (HAIS-Q) merupakan instrumen yang dikembangkan oleh Parsons *et al.* untuk mengukur tingkat kesadaran keamanan informasi individu berdasarkan aspek perilaku manusia. Instrumen ini menilai sejauh mana individu memahami praktik serta menerapkan perilaku yang aman dalam penggunaan sistem teknologi informasi [8].

HAIS-Q dirancang untuk mengukur kesadaran keamanan informasi melalui tiga dimensi utama, yaitu *knowledge* (pengetahuan), *attitude* (sikap), dan *behavior* (perilaku). Ketiga dimensi tersebut sejalan dengan model *Knowledge, Attitude, and Behavior* (KAB) yang menjelaskan bahwa kesadaran keamanan informasi terbentuk dari hubungan antara pengetahuan pengguna mengenai ancaman keamanan, sikap terhadap pentingnya keamanan informasi, serta perilaku yang diterapkan dalam menjaga keamanan informasi [8,9].

Dalam penelitian ini, instrumen HAIS-Q diadaptasi untuk mengukur tingkat kesadaran keamanan informasi pada pengguna *mobile banking* BCA. Penyusunan pernyataan kuesioner didasarkan pada pengembangan sembilan fokus area. Lima fokus area utama mengacu pada instrumen HAIS-Q, yaitu manajemen kata sandi, penggunaan email, penggunaan internet, penggunaan sosial media, keamanan perangkat seluler. Selain itu, guna meningkatkan relevansi dengan konteks penggunaan *mobile banking*, penelitian ini mengintegrasikan empat fokus area tambahan hasil adaptasi dari studi literatur dan validasi pakar (*expert judgment*), yaitu: kesadaran anti penipuan, manajemen kartu, kepedulian terhadap privasi informasi, dan efikasi diri dalam keamanan informasi, yang dapat dilihat pada Gambar 2.1. Setiap fokus area ini diukur melalui tiga dimensi utama KAB. Penjabaran lebih mendetail mengenai fokus area dan sub-area penelitian disajikan pada Tabel 2.1 [11,12].



Gambar 2.1 Fokus Area dan Sub-Area

Berdasarkan Gambar 2.1, penelitian ini menggunakan beberapa fokus area dan sub-area sebagai dasar penyusunan indikator penelitian. Uraian mengenai fokus area dan sub-area tersebut dijelaskan lebih lanjut pada Tabel 2.1.

Tabel 2.1 Penjabaran Fokus Area

Fokus Area	Fokus Sub-Area	Penjelasan
Manajemen Kata Sandi	Penggunaan kata sandi yang berbeda	Jika kata sandi diketahui oleh orang lain, maka risiko penyalahgunaan dan tindakan penipuan akan sangat besar.
	Kerahasiaan kata sandi	
	Penggunaan kata sandi yang kuat	

Penggunaan Email	Mengklik tautan di email dari pengirim yang dikenal	Email dapat digunakan oleh penipu untuk mengambil data sensitif dari pengguna yang kurang berhati-hati dalam penggunaannya.
	Mengklik tautan di email dari pengirim yang tidak dikenal	
	Membuka lampiran pada email dari pengirim yang tidak dikenal	
Penggunaan Internet	Mengunduh file	Pelaku penipuan dapat membuat tautan web palsu yang dapat menjebak pengguna yang tidak bertanggung jawab untuk memberikan data sensitif tentang akun mereka dan menyalahgunakannya.
	Mengakses situs web yang mencurigakan	
	Memasukkan informasi secara online	
Penggunaan Media Sosial	Pengaturan privasi media sosial	Pengguna yang kurang berhati-hati dapat menyebarkan data sensitif di media sosial mereka dan berisiko disalahgunakan oleh orang-orang yang tidak bertanggung jawab.
	Mempertimbangkan konsekuensi	
	Mengunggah informasi pribadi	
Keamanan Perangkat Seluler	Mengamankan perangkat seluler secara fisik	Penggunaan perangkat seluler dan jaringan yang ceroboh dapat menyebabkan informasi sensitif akun pengguna diakses oleh orang lain selain pengguna itu sendiri dan rentan terhadap penyalahgunaan.
	Mengirim informasi sensitif melalui Wi-Fi	
	Keamanan informasi saat menggunakan perangkat di tempat umum	
Kesadaran Anti Penipuan	Pengenalan <i>phishing</i> dan <i>scam</i>	Penjelasan bank terkait pencegahan kasus penipuan sangat penting untuk diketahui dan diterima guna meningkatkan kesadaran keamanan informasi para penggunanya.
	Pemahaman modus penipuan digital	
Manajemen Kartu	Menyimpan kartu fisik	Pada kartu fisik, terdapat beberapa informasi sensitif yang perlu dirahasiakan oleh pengguna, dan penyimpanan serta penggunaannya harus diperhatikan.
	Menggunakan kartu fisik	
Kepedulian terhadap Privasi Informasi	Mengetahui motif orang lain	Kesadaran pengguna tentang penggunaan informasi akun sensitif oleh pihak lain penting untuk kesadaran keamanan informasi pengguna.
	Keengganan untuk memberikan informasi	
	Tindakan untuk menjaga keamanan informasi	
Efikasi Diri dalam Keamanan Informasi	Konfirmasi informasi sensitif	Informasi sensitif pada akun pengguna akan aman jika pengguna memiliki keterampilan pribadi yang baik dalam melindungi informasi tersebut.
	Kecurigaan terhadap pelaku penipuan	

2.7 Metode *Analytical Hierarchy Process* (AHP)

Analytical Hierarchy Process (AHP) merupakan metode pengambilan keputusan multikriteria yang dikembangkan oleh Thomas L. Saaty. Metode ini digunakan untuk menentukan bobot prioritas atau tingkat kepentingan dari sejumlah kriteria melalui proses perbandingan berpasangan (*pairwise comparison*). AHP efektif dalam penelitian ilmiah karena mampu mengonversi penilaian subjektif pakar menjadi nilai kuantitatif yang dapat dianalisis secara sistematis. Dalam metode AHP, suatu permasalahan disusun dalam bentuk struktur hierarki yang terdiri dari tujuan, kriteria, dan alternatif keputusan. Struktur hierarki ini membantu peneliti dalam memahami hubungan fungsional antar elemen yang terlibat dalam proses pengambilan keputusan [10]. Pada penelitian ini, kriteria yang dibandingkan adalah sembilan fokus area keamanan informasi yang strukturnya dapat dilihat pada Gambar 2.1.

Penilaian perbandingan berpasangan pada penelitian ini dilakukan melalui *expert judgment* yang melibatkan empat *experts* yaitu dua dosen spesialisasi di bidang keamanan informasi dan keamanan siber, serta dua staf BTI Universitas Mikroskil yang memiliki pengalaman operasional dalam mengelola infrastruktur TI, untuk detailnya dapat dilihat pada Tabel 3.2. Pemilihan *experts* tersebut dilakukan untuk memperoleh penilaian dari perspektif akademis dan praktis dalam menentukan tingkat kepentingan setiap kriteria keamanan informasi. Namun, pengalaman operasional staf BTI tidak secara khusus merepresentasikan pengelolaan infrastruktur TI pada sektor perbankan. Oleh karena itu, penilaian mereka didasarkan pada kompetensi di bidang teknologi dan keamanan informasi, bukan sebagai representasi praktisi perbankan. Setiap *experts* diminta memberikan penilaian terhadap tingkat kepentingan antar kriteria menggunakan skala Saaty 1–9. Hasil penilaian tersebut kemudian disusun ke dalam matriks perbandingan berpasangan sebagai dasar perhitungan bobot kepentingan dan pengujian konsistensi data [10]. Nilai skala perbandingan yang umum digunakan dapat dilihat pada tabel berikut:

Tabel 2.2 Skala Perbandingan Berpasangan

Nilai	Keterangan
1	Kedua elemen sama penting
3	Elemen yang satu sedikit lebih penting
5	Elemen yang satu lebih penting
7	Elemen yang satu sangat lebih penting
9	Elemen yang satu mutlak lebih penting
2,4,6,8	Nilai antara dua penilaian yang berdekatan

2.8 Integrasi Skor ISA dan Bobot Prioritas dengan *Weighted Sum Model* (WSM)

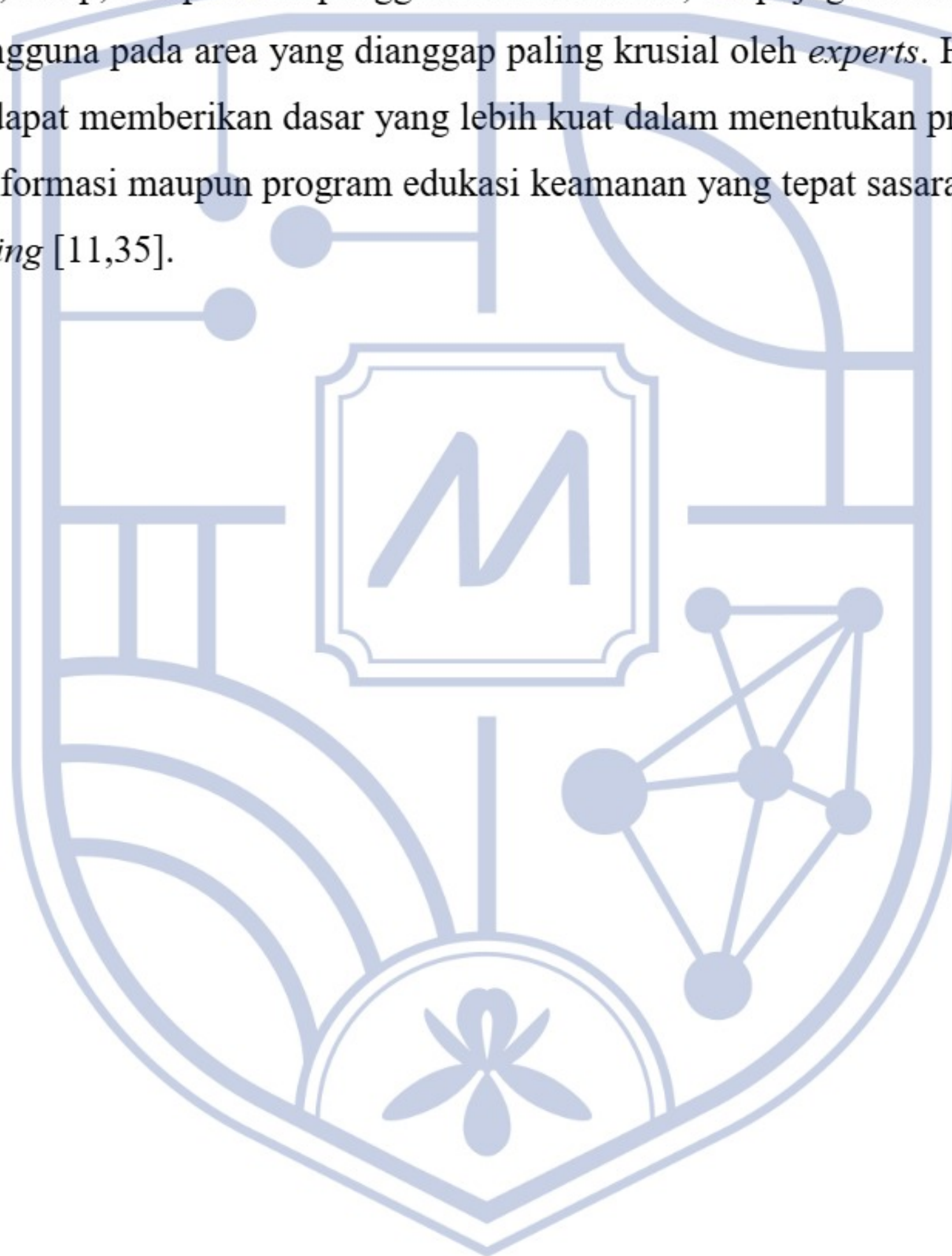
Weighted Sum Model (WSM) merupakan salah satu metode pengambilan keputusan multikriteria (*Multi-Criteria Decision Making*) yang paling mendasar dan banyak digunakan untuk mengevaluasi sejumlah kriteria dengan bobot berbeda ke dalam satu nilai akhir. Dalam penelitian ini, WSM digunakan sebagai metode integrasi untuk menggabungkan skor *Information Security Awareness* (ISA) yang diperoleh dari responden dengan bobot prioritas kriteria yang dihasilkan melalui metode *Analytical Hierarchy Process* (AHP) oleh para *experts* [20].

Pada penelitian ini, metode ISA digunakan untuk mengukur tingkat kesadaran keamanan informasi pengguna *mobile banking* BCA berdasarkan dimensi *Knowledge*, *Attitude*, dan *Behavior* (KAB). Hasil pengukuran ISA menghasilkan skor tingkat kesadaran pada masing-masing fokus area keamanan informasi berdasarkan jawaban responden. Sementara itu, metode AHP digunakan untuk menentukan tingkat kepentingan relatif dari setiap fokus area keamanan informasi berdasarkan penilaian *experts* melalui perbandingan berpasangan (*pairwise comparison*). Hasil dari metode AHP berupa bobot prioritas yang menunjukkan fokus area mana yang dianggap lebih penting dalam konteks penggunaan *mobile banking*.

Integrasi Skor ISA dan bobot prioritas dilakukan karena hasil pengukuran ISA hanya menunjukkan tingkat kesadaran pengguna pada setiap fokus area tanpa mempertimbangkan tingkat kepentingan masing-masing fokus area. Oleh karena itu, metode WSM digunakan untuk menggabungkan skor kesadaran pengguna dengan bobot prioritas hasil AHP sehingga diperoleh nilai kesadaran keamanan informasi yang lebih representatif.

Proses integrasi dilakukan dengan mengalikan skor ISA pada setiap fokus area dengan bobot prioritas AHP pada fokus area yang sama, kemudian seluruh hasil perkalian dijumlahkan untuk memperoleh nilai akhir tingkat kesadaran keamanan informasi pengguna *mobile banking*. Dengan pendekatan ini, fokus area yang memiliki tingkat kepentingan lebih tinggi akan memberikan kontribusi yang lebih besar terhadap nilai akhir dibandingkan fokus area yang memiliki bobot lebih rendah [11].

Melalui penerapan WSM, hasil akhir penelitian tidak hanya menunjukkan tingkat pengetahuan, sikap, dan perilaku pengguna secara umum, tetapi juga mencerminkan tingkat kesiapan pengguna pada area yang dianggap paling krusial oleh *experts*. Hasil integrasi ini diharapkan dapat memberikan dasar yang lebih kuat dalam menentukan prioritas kebijakan keamanan informasi maupun program edukasi keamanan yang tepat sasaran bagi pengguna *mobile banking* [11,35].



2.9 Penelitian Terdahulu

Tabel 2.3 Penelitian Terdahulu

No	Peneliti	Tahun	Metode, Model, dan Instrumen	Objek Penelitian	Hasil Penelitian	Research Gap	Relevansi terhadap Penelitian ini
1	Kruger & Kearney [7]	2006	Kuantitatif; KAB; Kuesioner	Pengguna teknologi informasi	Mengembangkan model pengukuran kesadaran keamanan informasi berbasis <i>Knowledge, Attitude, and Behavior</i> (KAB) untuk menilai tingkat kesadaran keamanan pengguna.	Penelitian hanya mengembangkan model KAB untuk pengukuran kesadaran keamanan informasi dan belum menggunakan instrumen HAIS-Q maupun metode pembobotan prioritas keamanan informasi.	Menjadi dasar teori penggunaan model KAB dalam pengukuran kesadaran keamanan informasi pengguna <i>mobile banking</i> .
2	Parsons <i>et al.</i> [8,9]	2017	Kuantitatif; KAB; HAIS-Q	Pengguna sistem informasi dalam organisasi	Mengembangkan instrumen HAIS-Q untuk mengukur ISA berdasarkan dimensi <i>knowledge, attitude, dan behavior</i> .	Penelitian berfokus pada pengembangan instrumen HAIS-Q dalam lingkungan organisasi dan belum mengintegrasikan metode AHP untuk menentukan prioritas fokus area keamanan informasi.	Menjadi acuan penggunaan instrumen HAIS-Q dalam mengukur tingkat kesadaran keamanan informasi berdasarkan dimensi KAB.

No	Peneliti	Tahun	Metode, Model, dan Instrumen	Objek Penelitian	Hasil Penelitian	Research Gap	Relevansi terhadap Penelitian ini
3	McCormac <i>et al.</i> [34]	2017	Kuantitatif; KAB; HAIS-Q	Karyawan organisasi	Tingkat kesadaran keamanan informasi dipengaruhi oleh pengetahuan dan perilaku pengguna terhadap praktik keamanan informasi.	Penelitian ini berfokus pada pengaruh karakteristik individu terhadap <i>Information Security Awareness (ISA)</i> , namun belum membahas pengukuran tingkat kesadaran keamanan informasi pada pengguna <i>mobile banking</i> serta belum menerapkan metode AHP dalam pembobotan dimensi keamanan informasi.	Mendukung pentingnya aspek <i>knowledge, attitude, dan behavior</i> dalam meningkatkan kesadaran keamanan informasi pengguna.
4	Alhogail [36]	2018	Kuantitatif; ISCF; Kuesioner	Pengguna teknologi informasi	Mengembangkan model kesadaran keamanan informasi yang menekankan pentingnya perilaku pengguna dalam menjaga keamanan informasi.	Penelitian ini berfokus pada perancangan dan validasi kerangka budaya keamanan informasi dalam organisasi, namun belum membahas pengukuran tingkat	Menjadi landasan teori terkait pentingnya perilaku pengguna dalam menjaga keamanan informasi.

No	Peneliti	Tahun	Metode, Model, dan Instrumen	Objek Penelitian	Hasil Penelitian	Research Gap	Relevansi terhadap Penelitian ini
						Information Security Awareness (ISA) pada pengguna <i>mobile banking</i> menggunakan instrumen HAIS-Q berbasis dimensi KAB, serta belum menerapkan metode AHP dalam pembobotan tingkat kesadaran keamanan informasi.	
5	Indrakusuma & Hidayanto [11]	2022	Kuantitatif; KAB; HAIS-Q + AHP	Pengguna <i>digital banking</i>	Dimensi perilaku (<i>behavior</i>) memiliki pengaruh yang signifikan terhadap tingkat kesadaran keamanan informasi pengguna layanan <i>digital banking</i> .	Penelitian dilakukan pada pengguna <i>digital banking</i> secara umum dan belum mengintegrasikan hasil <i>awareness</i> dengan bobot prioritas fokus area keamanan informasi pada konteks <i>mobile banking</i> .	Menjadi referensi penggunaan instrumen HAIS-Q berbasis dimensi KAB dan metode AHP untuk mengukur prioritas kesadaran keamanan informasi dan integrasi HAIS-Q dan AHP dalam menentukan nilai akhir ISA

No	Peneliti	Tahun	Metode, Model, dan Instrumen	Objek Penelitian	Hasil Penelitian	Research Gap	Relevansi terhadap Penelitian ini
							pada pengguna <i>digital banking</i> .
6	Chaq & Imran [12]	2025	Kuantitatif; KAB; HAIS-Q + AHP	Calon tenaga kerja industri tekstil	Tingkat kesadaran keamanan informasi responden berada pada kategori sedang.	Penelitian dilakukan pada calon tenaga kerja industri tekstil sehingga konteks penelitian berbeda dengan pengguna <i>mobile banking</i> .	Menjadi referensi penggunaan metode AHP untuk menentukan bobot prioritas fokus area keamanan informasi.
7	Arisya <i>et al.</i> [15]	2020	Kuantitatif; KAB; HAIS-Q	Pengguna <i>mobile banking</i> di Indonesia	Tingkat kesadaran keamanan informasi pengguna <i>mobile banking</i> berada pada kategori baik. Masih terdapat beberapa perilaku pengguna yang berpotensi menimbulkan risiko keamanan informasi.	Penelitian hanya mengukur tingkat kesadaran keamanan informasi pengguna <i>mobile banking</i> menggunakan HAIS-Q.	Menjadi referensi pengukuran ISA berbasis dimensi KAB serta menerapkan metode AHP dalam menentukan tingkat kesadaran keamanan informasi pengguna dan menggunakan metode dalam menghitung nilai akhir ISA pada pengguna <i>mobile banking</i> .

No	Peneliti	Tahun	Metode, Model, dan Instrumen	Objek Penelitian	Hasil Penelitian	Research Gap	Relevansi terhadap Penelitian ini
8	Fadhil & Yazid [37]	2024	Kuantitatif; KAB; HAIS-Q	Pegawai Badan Kepegawaia n Negara	Tingkat <i>Information Security Awareness</i> pegawai BKN berada pada kategori baik dengan nilai sebesar 88,80%. Selain itu, terdapat pengaruh signifikan antara <i>knowledge</i> terhadap <i>attitude</i> , <i>attitude</i> terhadap <i>behavior</i> , dan <i>knowledge</i> terhadap <i>behavior</i> .	Penelitian dilakukan pada pegawai instansi pemerintah dan tidak membahas pengguna <i>mobile banking</i> maupun pembobotan prioritas keamanan informasi menggunakan AHP.	Mendukung analisis hubungan antara <i>knowledge</i> , <i>attitude</i> , dan <i>behavior</i> terhadap <i>information security awareness</i> .
9	Gofur <i>et al.</i> [35]	2024	Kuantitatif; KAB; HAIS-Q + AHP	Pegawai PT Meshindo Jayatama	Tingkat kesadaran keamanan informasi pegawai berada pada kategori baik dengan nilai 83,40%, namun masih terdapat fokus area yang perlu ditingkatkan, yaitu penggunaan perangkat <i>mobile</i> dan pengelolaan <i>password</i> .	Penelitian dilakukan pada pegawai perusahaan dan belum diterapkan pada konteks pengguna <i>mobile banking</i> .	Menjadi referensi penerapan integrasi HAIS-Q dan AHP dalam menentukan prioritas fokus area keamanan informasi.

No	Peneliti	Tahun	Metode, Model, dan Instrumen	Objek Penelitian	Hasil Penelitian	Research Gap	Relevansi terhadap Penelitian ini
10	Hari <i>et al.</i> [13]	2025	Kuantitatif; KAB; HAIS-Q + AHP	Mahasiswa Universitas Islam Negeri Raden Fatah	Tingkat kesadaran keamanan informasi berada pada kategori cukup baik, namun masih terdapat beberapa aspek keamanan yang perlu ditingkatkan. Selain itu, penggunaan metode AHP mampu mengidentifikasi prioritas aspek keamanan yang harus diperhatikan.	Penelitian dilakukan pada mahasiswa dan bukan pada pengguna <i>mobile banking</i> .	Menjadi referensi penerapan HAIS-Q dan AHP untuk menentukan prioritas aspek keamanan informasi dan menggunakan metode <i>Weighted Sum Model</i> (WSM) untuk menggabungkan skor tiap dimensi dengan bobot hasil AHP dalam memperoleh nilai akhir ISA.
11	Perkasa <i>et al.</i> [38]	2024	Kuantitatif; KAB; HAIS-Q + AHP	Siswa sekolah menengah atas di Surabaya	Tingkat kesadaran keamanan informasi siswa berada pada kategori <i>Good</i> dengan nilai total sebesar 86,38%. Fokus area yang paling rentan berdasarkan pembobotan AHP adalah <i>password management</i> , sehingga	Penelitian dilakukan pada siswa sekolah menengah atas sehingga objek penelitian berbeda dengan pengguna <i>mobile banking</i> .	Menjadi referensi penggunaan pembobotan AHP dalam menentukan fokus area keamanan informasi yang paling rentan.

No	Peneliti	Tahun	Metode, Model, dan Instrumen	Objek Penelitian	Hasil Penelitian	Research Gap	Relevansi terhadap Penelitian ini
					direkomendasikan peningkatan edukasi keamanan informasi dan kebijakan sekolah terkait keamanan informasi.		
12	Hermawan <i>et al.</i> [14]	2022	Kuantitatif; KAB; HAIS-Q + AHP	Pegawai pada instansi XYZ Agency	Tingkat kesadaran keamanan informasi pegawai pada XYZ Agency berada pada kategori baik. Namun, masih ditemukan beberapa aspek perilaku keamanan informasi pegawai yang perlu diperbaiki agar penerapan keamanan informasi dalam organisasi dapat berjalan lebih optimal.	Penelitian belum mengintegrasikan hasil pengukuran <i>awareness</i> dan bobot prioritas fokus area keamanan informasi menjadi nilai evaluasi akhir pada konteks <i>mobile banking</i> .	Menjadi referensi penggunaan HAIS-Q dan AHP dalam menentukan bobot prioritas fokus area keamanan informasi.
13	Sembiring &	2022	Kuantitatif; KAB; HAIS-Q	Pengguna <i>mobile banking</i>	Tingkat kesadaran keamanan informasi pengguna <i>mobile banking</i> berada pada kategori	Penelitian hanya mengukur tingkat kesadaran keamanan informasi pengguna <i>mobile</i>	Menjadi referensi pengukuran kesadaran keamanan informasi pengguna <i>mobile</i>

No	Peneliti	Tahun	Metode, Model, dan Instrumen	Objek Penelitian	Hasil Penelitian	Research Gap	Relevansi terhadap Penelitian ini
	Pandia [16]				cukup baik. Masih terdapat beberapa perilaku pengguna yang berpotensi menimbulkan risiko keamanan informasi.	<i>banking</i> menggunakan HAIS-Q tanpa mengintegrasikan metode AHP untuk menentukan prioritas fokus area keamanan informasi.	<i>banking</i> menggunakan instrumen HAIS-Q berbasis KAB.
14	Hutagaol <i>et al.</i> [17]	2024	Kuantitatif; Kuesioner <i>Awareness</i>	Pengguna <i>mobile banking</i> di Indonesia	Sebagian besar pengguna telah memiliki kesadaran terhadap ancaman <i>cybercrime</i> , namun masih ditemukan pengguna yang pernah mengalami percobaan maupun menjadi korban <i>cybercrime</i> sehingga diperlukan peningkatan edukasi dan kesadaran keamanan informasi pada pengguna <i>mobile banking</i> .	Penelitian hanya mengukur tingkat kesadaran pengguna <i>mobile banking</i> terhadap ancaman <i>cybercrime</i> menggunakan kuesioner umum tanpa menggunakan instrumen HAIS-Q maupun metode AHP untuk menentukan prioritas fokus area keamanan informasi.	Menjadi referensi terkait <i>cybercrime awareness</i> pengguna <i>mobile banking</i> serta pendukung fokus area keamanan informasi terkait ancaman keamanan transaksi digital.

No	Peneliti	Tahun	Metode, Model, dan Instrumen	Objek Penelitian	Hasil Penelitian	Research Gap	Relevansi terhadap Penelitian ini
15	Ramadha n & Purwand ari [18]	2023	Kuantitatif; KAB; HAIS-Q	Pengguna aplikasi perbankan digital di Indonesia	Tingkat kesadaran keamanan informasi pengguna aplikasi perbankan digital berada pada kategori baik. Namun, aspek perilaku (<i>behavior</i>) pengguna masih lebih rendah dibandingkan aspek pengetahuan (<i>knowledge</i>) dan sikap (<i>attitude</i>) sehingga diperlukan peningkatan edukasi keamanan informasi untuk mencegah ancaman <i>social engineering</i> .	Penelitian hanya mengukur tingkat kesadaran keamanan informasi pengguna aplikasi perbankan digital menggunakan HAIS-Q tanpa mengintegrasikan metode AHP untuk menentukan prioritas fokus area keamanan informasi.	Menjadi referensi pengukuran kesadaran keamanan informasi pengguna aplikasi perbankan digital menggunakan HAIS-Q berbasis KAB serta pendukung fokus area keamanan informasi terkait ancaman <i>social engineering</i> .
16	Ananda <i>et al.</i> [19]	2025	Kuantitatif; KAB; HAIS-Q	Pengguna layanan <i>mobile banking</i>	Tingkat kesadaran keamanan informasi pengguna layanan <i>mobile banking</i> berada pada kategori baik, namun masih ditemukan beberapa perilaku	Penelitian hanya berfokus pada pengukuran tingkat kesadaran keamanan informasi pengguna layanan <i>mobile banking</i> menggunakan	Menjadi referensi pengukuran kesadaran keamanan informasi pengguna layanan <i>mobile banking</i> menggunakan HAIS-Q berbasis KAB serta

No	Peneliti	Tahun	Metode, Model, dan Instrumen	Objek Penelitian	Hasil Penelitian	Research Gap	Relevansi terhadap Penelitian ini
					pengguna yang berpotensi menimbulkan risiko keamanan informasi sehingga diperlukan peningkatan edukasi dan kesadaran keamanan bagi pengguna layanan <i>mobile banking</i> .	HAIS-Q tanpa melakukan pembobotan prioritas fokus area keamanan informasi menggunakan metode AHP.	serta pendukung fokus area keamanan informasi pada layanan <i>mobile banking</i> .

Berdasarkan tinjauan penelitian terdahulu yang telah dijelaskan pada Tabel 2.3, dapat disimpulkan bahwa pengukuran kesadaran keamanan informasi secara konsisten menggunakan model *Knowledge, Attitude, and Behavior* (KAB) dengan instrumen *Human Aspects of Information Security Questionnaire* (HAIS-Q). Tren penelitian terbaru dalam kurun waktu 2022–2025 menunjukkan adanya pengembangan metodologi melalui integrasi metode *Analytic Hierarchy Process* (AHP) untuk memberikan bobot prioritas pada setiap dimensi kesadaran secara lebih presisi. Meskipun demikian, mayoritas penelitian terdahulu berfokus pada sektor korporasi, instansi pemerintah, instansi pendidikan, atau pengguna teknologi secara umum. Namun, penelitian yang secara spesifik menganalisis tingkat kesadaran keamanan informasi pada pengguna *mobile banking*, khususnya pada pengguna *mobile banking* BCA di Kota Medan, masih terbatas.

Oleh karena itu, penelitian ini dilakukan untuk mengisi celah tersebut dengan menganalisis tingkat kesadaran keamanan informasi pengguna *mobile banking* melalui pendekatan *Information Security Awareness (ISA)* berbasis model KAB yang dipetakan ke dalam sembilan fokus area. Analisis ini kemudian diintegrasikan dengan metode *Analytical Hierarchy Process (AHP)* melalui pendekatan *Weighted Sum Model (WSM)*. Melalui metode tersebut, penelitian ini menghasilkan nilai akhir berupa tingkat kesadaran keamanan informasi pengguna *mobile banking* yang lebih representatif karena telah mempertimbangkan tingkat kepentingan relatif dari setiap fokus area keamanan informasi.

