Indonesian Journal of Computer Science
ISSN 2302-4364 (*print*) dan 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam, No. 1, Padang, Indonesia, Telp. (0751) 7056199, 7058325
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Pengukuran Tingkat Kesadaran Keamanan Informasi Pegawai Pada Instansi Pemerintah

Krisna Maria Rosita Dewi[1], Ricko Dwiki Yudistira[2], Yova Ruldeviyani[3]
krisna.maria@ui.ac.id, r.d.yudistira@student.reading.ac.uk, 3yova@cs.ui.ac.id
[1,3]Universitas Indonesia
[2]University of Reading

Informasi Artikel

Diterima : 25 Apr 2024
Direview : 29 Apr 2024
Disetujui : 30 Apr 2024

Kata Kunci

Kesadaran Keamanan Informasi Pegawai, KAB, HAIS-Q, Indeks KAMI

Abstrak

Sumber Daya Manusia (SDM) menjadi faktor yang mempengaruhi keberhasilan penerapan e-government di era perkembangan teknologi yang sangat pesat. Namun, SDM juga berperan menimbulkan resiko keamanan informasi bagi organisasi. Dalam rangka menghadapi menghadapi resiko keamanan informasi, BMKG menerapkan sistem manajemen keamanan informasi dengan melaksanakan pengimplementasian ISO/IEC 27001:2013 pada tahun 2020 dan direncanakan untuk diterapkan juga pada tiga lokasi Balai Wilayah BMKG. Oleh karena itu, penelitian ini bertujuan untuk melakukan pengukuran tingkat kesadaran keamanan informasi pegawai di ketiga lokasi tersebut dengan menggunakan konsep *Knowledge, Attitude, Behavior* (KAB) dan metode HAIS-Q yang digabungkan dengan sub area pengelolaan aset informasi dari Indeks KAMI. Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan informasi pegawai tergolong dalam kategori baik dengan nilai 81,67%. Beberapa area yang perlu ditingkatkan terkait *password management* (79,81%), *mobile computing* (75,59%), dan *incident reporting* (79,81%). Balai Wilayah A memiliki tingkat kesadaran keamanan informasi pegawai yang paling rendah dengan nilai rata-rata 79,75%.

Keywords

Employee Information Security Awareness, KAB, HAIS-Q, KAMI's Index

Abstract

Human Resources (HR) have become a factor that affects the success of e-government implementation in the era of rapid technological development. However, HR also play a role in creating information security risks for the organization. In order to deal with information security risks, BMKG implemented an information security management system by implementing ISO/IEC 27001:2013 in 2020. It also plans to implement it at three locations of the BMKG Regional Office. Therefore, this study aims to measure employees' level of information security awareness at the three locations using the Knowledge, Attitude, Behavior (KAB) concept and the HAIS-Q method combined with the information asset management sub-area of the KAMI's Index. The results showed that employees' level of information security awareness is classified in the good category with a value of 81.67%. Some areas that need to be improved are password management (79.81%), mobile computing (75.59%), and incident reporting (79.81%). Regional Center A has the lowest employee information security awareness level, with an average score of 79.75%.

A. Pendahuluan

Teknologi Informasi dan Komunikasi (TIK) berkembang sangat pesat dari masa ke masa. Kemajuan teknologi yang terjadi berperan penting bagi kehidupan manusia yang dimanfaatkan dalam berbagai bidang seperti sosial budaya, ekonomi, kesehatan, pendidikan, dan juga pemerintahan [1]. Pada sektor pemerintahan, teknologi informasi menjadi salah satu instrumen yang digunakan dalam rangka mewujudkan electronic Government (e-Government) untuk memberikan pelayanan kepada masyarakat yang lebih efisien dan efektif. Salah satu faktor yang mempengaruhi keberhasilan penerapan e-Government adalah sumber daya manusia [2]. Namun, sumber daya manusia, dalam hal ini pegawai, juga turut berperan dalam menimbulkan resiko keamanan informasi bagi organisasi [3].

Berdasarkan laporan Hasil Monitoring Keamanan Siber Periode Desember 2022 dari BSSN, terdapat anomali trafik tertinggi mencapai 1.073.635 pada 2 Desember 2022. Jumlah anomali trafik yang begitu tinggi menunjukkan adanya potensi terjadinya serangan siber. Hasil monitoring BSSN menyebutkan bahwa klasifikasi anomali tertinggi yaitu *malware* yang mencapai 15,828,804 trafik [4]. Selain itu, berdasarkan hasil monitoring firewall BMKG terdapat anomali trafik mencapai 605.190 di bulan Juli 2023 [5]. Tanpa adanya kesadaran akan keamanan informasi dari pegawai dalam menghadapi kemajuan teknologi, maka instansi terkait akan sangat rentan terhadap berbagai ancaman serangan siber yang mungkin terjadi.

Badan Meteorologi Klimatologi dan Geofisika (BMKG) merupakan salah satu instansi pemerintahan yang telah melaksanakan ISO/IEC 27001:2013 dalam rangka menerapkan sistem manajemen keamanan informasi yang terstandarisasi. Hal ini dimulai dari unit kerja Pusat Jaringan Komunikasi pada tahun 2020. Kedepannya penerapan ISO/IEC 27001 akan dilaksanakan di lima Balai Wilayah BMKG, yang telah diawali dengan penerapan di salah satu Balai Wilayah BMKG di tahun 2022. Pada tahun 2023, ISO/IEC 27001:2013 diterapkan di salah satu Balai Wilayah yang lain. Tiga Balai Wilayah BMKG lainnya direncanakan akan melakukan penerapan ISO/IEC 27001 pada tahun 2024.

Beberapa penelitian terdahulu seperti Andress [6], Xu [7] dan Bulgurcu [8] melakukan penelitian yang berkaitan dengan kesadaran keamanan informasi pegawai mengguanakan tiga konsep utama yaitu *Confidentiality, Integrity, Availability* (CIA) dan telah berhasil melakukan penelitian yang terkait dengan kesadaran keamanan informasi pegawai menggunakan metode HAIS-Q serta memetakan hasil penelitian menggunakan konsep *Knowledge, Attitude, Behavior* (KAB). Selain itu, Puspitaningrum, dkk [9] melakukan penelitian lanjutan dengan memadukan sub area pada HAIS-Q dengan sub area manajemen aset informasi pada Indeks Keamanan Informasi (KAMI). Berdasarkan dari penelitian-penelitian tersebut dan diskusi dengan *expert* dari Pusat Jaringan Komunikasi, metode HAIS-Q yang dikombinasikan dengan Indeks KAMI dan konsep KAB adalah metode yang paling sesuai dengan kebutuhan organisasi pada studi kasus penelitian ini.

Oleh karena itu, penelitian ini bertujuan untuk mengukur tingkat kesadaran keamanan informasi pegawai di tiga lokasi Balai Wilayah BMKG dengan menggunakan sub area metode HAIS-Q dan sub area manajemen aset informasi Indeks KAMI. Hingga saat ini BMKG belum melakukan penelitian terkait sejauh mana kesadaran keamanan informasi pegawai di ketiga Balai Wilayah tersebut.

Hasil yang diperoleh dari penelitian ini diharapkan dapat memberikan gambaran, rekomendasi dan bahan pertimbangan bagi pemangku kebijakan untuk melakukan pengambilan keputusan dalam rangka peningkatan kesadaran keamanan informasi menyongsong rencana pengimplementasian ISO/IEC 27001 di Balai Wilayah BMKG masing-masing.

Penelitian ini tersusun dari kajian literatur menjabarkan terkait penelitian terdahulu dan teori-teori dari penelitian yang dilakukan, metode penelitian menjelaskan terkait alur serta instrumen penelitian, hasil dan pembahasan dari penelitian yang telah dilakukan dan simpulan dari penelitian yang telah dilakukan.

B. Kajian Literatur

Kesadaran Keamanan Informasi

Keamanan informasi merupakan faktor yang penting diperhatikan dalam dalam membangun suatu sistem manajemen keamanan informasi. Andress [6] memaparkan bahwa keamanan informasi memiliki tiga konsep utama yang disebut *Confidentiality, Integrity, Availability* (CIA). Xu dkk. [7] menjelaskan pengertian CIA sebagai berikut:

- *Confidentiality* berarti hanya pengguna yang memiliki wewenang untuk melakukan akses pada suatu sistem informasi atau data;
- *Integrity* berarti menjamin keakuratan suatu informasi untuk dapat dipercaya;
- *Availability* berarti memastikan ketersediaan akses bagi pengguna yang memiliki wewenang terhadap suatu sistem informasi atau data.

Peningkatan kesadaran keamanan informasi merupakan jalur yang sangat efektif dalam rangka menjaga keamanan informasi organisasi maupun perusahaan [10]. Kesadaran keamanan informasi dari pegawai berperan besar terhadap hasil pelaksanaan keamanan informasi dan secara signifikan dapat mempengaruhi tingkat kepatuhan pegawai terhadap aturan penerapan keamanan informasi [8].

Human Aspects Of Information Security Questionnaire (HAIS-Q)

HAIS-Q merupakan model kuesioner yang berfokus pada perilaku yang berkaitan dengan *human errors* [11]. Kuesioner didesain untuk mewakili area-area kebijakan keamanan informasi yang relevan bagi pegawai. Berdasarkan penelitian Parsons [11], dilakukan pengembangan kerangka model yang terdiri dari tujuh fokus area yaitu *password management, email use, internet use, Social Networking Site (SNS) use, Incident reporting, Mobile computing,* dan *Information handling*. Setiap fokus areanya terdiri dari tiga sub area, sehingga total sub area adalah 21 yang dapat merepresentasikan seluruh fokus area.

Indeks Keamanan Informasi (KAMI)

Indeks KAMI ialah instrumen yang disusun berdasarkan kriteria ISO 27001:2009 untuk membantu melakukan evaluasi dan asesmen tingkat kesiapan instansi pemerintah dalam menerapkan sistem manajemen keamanan informasi [12]. Penilaian Indeks KAMI mencakup lima area, yaitu tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, teknologi dan keamanan informasi.

Penelitian Terdahulu

Puspitaningrum, dkk.[9]melakukan penelitian yang bertujuan merancang model pengukuran tingkat kesadaran keamanan informasi pada pegawai di Direktorat Jenderal SDPPI Kementerian Komunikasi dan Informatika. Metode yang digunakan adalah *Human Aspects of Information Security Questionnaire* (HAIS-Q) dan dikombinasikan dengan aspek manajemen aset informasi dalam Indeks KAMI untuk mengukur kesadaran informasi pegawai. Penelitian dilakukan dengan menyebarkan kuesioner kepada 28 pegawai di SDPPI dan juga melakukan wawancara dengan beberapa senior manajemen. Penelitian ini didukung oleh Kritzinger, dkk[13]yang melakukan penelitian mengenai pengukuran tingkat kesadaran keamanan informasi pegawai yang dilakukan di Afrika Selatan. Penelitian dilakukan dengan mengumpulkan data melalui kuesioner elektronik dengan 356 responden dari berbagai industri. Metode pengumpulan data menggunakan HAIS-Q dengan 63 pertanyaan yang terbagi kedalam tujuh fokus area, yaitu *password management, email use, internet use, social media use, mobile devices, information handling, dan incident reporting.*

Penelitian lain dilakukan oleh Arisya, dkk.[14]dengan menggunakan konsep KAB untuk mengukur kesadaran keamanan informasi pengguna aplikasi *Mobile Banking* (M-Banking). Pada penelitian ini, tingkat kesadaran keamanan informasi dihitung dengan menggunakan metode *Analytic Hierarchy Process* (AHP). Data dikumpulkan dengan cara menyebarkan kuesioner pada 210 responden pengguna aplikasi M-Banking. Kuesioner memuat 51 pertanyaan yang berkaitan dengan KAB yang diaplikasikan kedalam tujuh variabel area pada HAIS-Q.

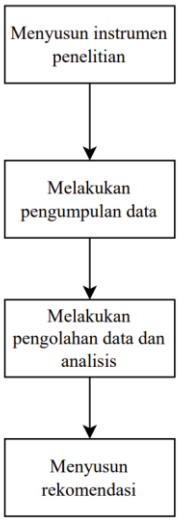
Penelitian dengan menggunakan konsep KAB juga dilakukan oleh Hermawan, dkk[15]untuk pengukuran tingkat kesadaran keamanan teknologi informasi pada pegawai Instansi XYZ. Model konsep KAB digunakan untuk menilai tingkat security awareness and priority pada penelitian ini. Kuesioner pada penelitian ini juga didasarkan pada HAIS-Q dan metode *Analytic Hierarchy Process* (AHP). Kuesioner memuat 21 parameter dan disebarkan kepada 30 karyawan di salah satu cabang instansi tersebut.

C. Metode Penelitian

Penelitian ini melalui beberapa tahapan (Gambar 1) yang dirincikan sebagai berikut:

1) Menyusun instrumen penelitian: instrumen penelitian menggunakan kuesioner yang disusun berdasarkan pernyataan metode HAIS-Q dikombinasikan dengan Indeks KAMI yang dijabarkan kedalam 24 pernyataan kuesioner.
2) Melakukan pengumpulan data: Setelah divalidasi, pengumpulan data dilakukan dengan menyebarkan kuesioner kepada pegawai di tiga Balai Wilayah BMKG.
3) Melakukan pengolahan data dan analisis: Setelah data terkumpul, maka dilakukan pengolahan data dan analisis.

Menyusun rekomendasi: Data yang telah diolah dan dianalisis kemudian dilakukan penarikan kesimpulan dan disusun rekomendasi untuk meningkatkan kesadaran keamanan informasi pegawai.



Gambar 1. Alur Tahapan Penelitian

Penyusunan Instrumen Penelitian

Metode yang digunakan dalam melakukan penelitian ini adalah *Human Aspects of Information Security Questionnaire* (HAIS-Q) yang akan berfokus pada tujuh area, yaitu manajemen password, penggunaan email, penggunaan internet, penggunaan Social Networking Site (SNS), pelaporan insiden, *mobile computing*, dan penanganan informasi. Pada penelitian ini juga akan dilakukan modifikasi pada kuesioner dengan menambahkan salah satu area dari Indeks Keamanan Informasi (KAMI) yaitu pengelolaan aset informasi. Pernyataan-pernyataan disusun sesuai dengan modifikasi fokus area HAIS-Q dan Indeks KAMI yang telah ditentukan dan disesuaikan dengan model KAB[16]. Selain itu, pernyataan-pernyataan tersebut telah dilakukan validasi oleh expert setelah melakukan proses wawancara dan diskusi untuk menentukan tingkat urgensi dari masing-masing subjek area (Tabel 1).

Tabel 1. Tingkat Urgensi Subjek Area

Urgensi	Subjek Area
1	*Password management*
2	*Incident reporting*
3	*Management information assets*
4	*Information handling*
5	*Mobile computing*
6	*Social Networking Site (SNS) use*
7	*internet use*
8	*Email use*

Pengumpulan Data

Instrumen penelitian ini menggunakan kuesioner dengan *google form* untuk melakukan pengumpulan data. Pengambilan data akan menggunakan metode *stratified random sampling,* yaitu teknik pengambilan sampel secara acak pada populasi yang tidak homogen dengan membagi populasi ke dalam sub kelompok / strata [17]. Kuesioner akan disebarkan kepada pegawai di tiga Balai Wilayah BMKG. Jumlah populasi pada penelitian ini yaitu sebanyak 213 pegawai, dengan pegawai di Wilayah A sebanyak 72 pegawai, Wilayah B sebanyak 83 pegawai, dan Wilayah C

sebanyak 58 pegawai. Penghitungan jumlah sampel keseluruhan dilakukan dengan menggunakan rumus Slovin [18], [19] yang ditunjukkan pada persamaan (1).

$$n = \frac{N}{1+Ne^2} \qquad (1)$$

Pada persamaan (1), n merupakan jumlah sampel keseluruhan. N merupakan jumlah populasi, sedangkan e merupakan *error rate* sebesar 5%. Berdasarkan persamaan (1) tersebut, maka dilakukan penghitungan sampel yang diperlukan sebagai berikut:

$$n = \frac{213}{1 + 213(0{,}05)^2}$$

$$n = \frac{213}{1{,}5325}$$

$$n = 138{,}989 \approx 139 \; sampel$$

Berdasarkan dari perhitungan tersebut, maka total sampel yang diperlukan adalah 139 responden. Selanjutnya, penentuan jumlah sampel pada masing-masing lokasi penelitian dapat menggunakan metode *stratified random sampling* sesuai dengan persamaan (2).

$$ni = \frac{Ni}{N} \; x \; n \qquad (2)$$

Pada persamaan (2), ni merupakan jumlah sampel menurut strata. Ni merupakan jumlah populasi menurut strata. N merupakan jumlah populasi, sedangkan n merupakan jumlah sampel keseluruhan.

Berdasarkan persamaan (2) tersebut, maka dilakukan penghitungan sampel yang diperlukan pada masing-masing wilayah yang dijabarkan pada Tabel 2.

Tabel 2. Jumlah responden masing-masing wilayah

Nama Wilayah	Penghitungan Sampel
Wilayah A	$n_i = \frac{72}{213}$ x 139 = 46,9859 ≈ **47 sample**
Wilayah B	$n_i = \frac{83}{213}$ x 139 = 54,1643 ≈ **54 sample**
Wilayah C	$n_i = \frac{58}{213}$ x 139 = 37,8498 ≈ **38 sample**

Berdasarkan Tabel 2, wilayah A membutuhkan 47 responden, wilayah B membutuhkan 54 responden, dan wilayah C membutuhkan 38 responden. Setiap pernyataan pada kuesioner dilakukan uji validitas dan reliabilitas dengan menggunakan SPSS *Version* 26. Pengujian validitas dilakukan untuk mengevaluasi keandalan dan keakuratan instrumen penelitian yang digunakan. Sedangkan, pengujian reliabilitas dilakukan untuk mengevaluasi konsistensi jawaban seseorang pada pernyataan dalam kuesioner.

Pengolahan Data

Hasil data yang diperoleh dari kuesioner akan dipetakan pada tingkat kesadaran keamanan informasi berdasarkan teori dari Kruger dkk. [16], ditunjukkan pada Tabel 3.

Tabel 3. Tingkat Kesadaran Keamanan Informasi

Tingkat Kesadaran	Hasil Pengukuran (%)
Baik	80-100
Rata-rata	60-79
Buruk	kurang dari sama dengan 59

Respon kuesioner dirancang dengan menggunakan skala Likert. Skala Likert merupakan skala psikometrik yang umum digunakan dalam kuesioner, biasanya digunakan untuk mengukur pendapat, dan persepsi seseorang atau kelompok [20]. Tabel 4 menunjukan skala yang digunakan pada kuesioner penelitian ini dengan rentang skor 1 hingga 5.

Tabel 4. Skala Likert

Skor	Pilihan Jawaban	Singkatan
5	Sangat Setuju	SS
4	Setuju	S
3	Ragu-ragu	RG
2	Tidak Setuju	TS
1	Sangat Tidak Setuju	STS

Penyusunan Rekomendasi

Penyusunan rekomendasi untuk meningkatkan kesadaran keamanan informasi pegawai didasarkan dari hasil pengolahan data dan analisis yang telah dilakukan dan divalidasi oleh *expert*.

D. Hasil dan Pembahasan

Demografi Responden

Kuesioner yang disebarkan secara random kepada 139 pegawai, maka didapatkan data demografi responden sesuai yang ditunjukkan pada Tabel 5.

Tabel 5. Data Demografi Responden

No	Variabel	Item	Persentase
1	Jenis Kelamin	Laki-Laki	44%
		Perempuan	56%
2	Umur	17-25 tahun	19%
		26-40 tahun	53%
		41-60 tahun	28%
3	Pendidikan terakhir	SMA/SMK	2%
		D1	3%
		D3	3%
		D4/S1/setara	75%
		S2/setara	17%
4	Lama bekerja	0-5 tahun	29%
		6-10 tahun	11%
		11-20 tahun	51%
		>20 tahun	9%

Berdasarkan Tabel 5, jumlah responden Perempuan lebih banyak dibandingkan jumlah responden Laki-Laki untuk total ketiga wilayah. Selain itu, responden dengan rentang umur 26-40 tahun mendominasi dengan persentase 53% dibandingkan dengan kategori lainnya. Ditinjau dari variabel Pendidikan terakhir, responden dengan lulusan D4/ S1 memiliki nilai persentase 75%.

Sedangkan untuk variabel Lama bekerja, nilai persentase responden didominasi oleh responden dengan pengalaman kerja selama 11-20 tahun sebesar 51%.

Pengujian Validitas dan Reliabilitas

Pengujian validitas pada penelitian ini dilakukan menggunakan SPSS Version 26 untuk mendapatkan nilai korelasi pearson. Pengujian dilakukan perhitungan R Tabel dengan probabilitas 0,05 dan dF=N-2, dimana N merupakan jumlah sampel. Sehingga R Tabel diperoleh nilai sebesar 0,1678 (dF=137). Setiap responden memberikan jawaban pada 3 pernyataan di masing-masing fokus area, dimana simbol "a" pada pernyataan merupakan dimensi *knowledge*, simbol "b" merupakan dimensi *attitude*, dan simbol "c" merupakan dimensi *behavior* yang ditunjukkan pada Tabel 4. Berdasarkan hasil pengolahan data, setiap pernyataan data dinyatakan valid karena nilai Korelasi Pearson > R Tabel [21], [22].

Tabel 6. Pengujian Validitas

Fokus Area	Pernyataan	Nilai Korelasi Pearson	Keterangan
Password Management	Q1a	0.282	Valid
	Q1b	0.307	Valid
	Q1c	0.319	Valid
Mobile Computing	Q2a	0.475	Valid
	Q2b	0.589	Valid
	Q2c	0.491	Valid
Social Networking Site (SNS) Use	Q3a	0.541	Valid
	Q3b	0.496	Valid
	Q3c	0.575	Valid
Internet Use	Q4a	0.519	Valid
	Q4b	0.473	Valid
	Q4c	0.569	Valid
Incident Reporting	Q5a	0.317	Valid
	Q5b	0.358	Valid
	Q5c	0.417	Valid
Management Information Assets	Q6a	0.560	Valid
	Q6b	.0458	Valid
	Q6c	0.489	Valid
Information Handling	Q7a	0.430	Valid
	Q7b	0.444	Valid
	Q7c	0.497	Valid
Email Use	Q8a	0.495	Valid
	Q8b	0.386	Valid
	Q8c	0.520	Valid

Pengujian reliabilitas dilakukan menggunakan SPSS *Version* 26 untuk mendapatkan nilai Cronbach Alpha. Suatu variabel dapat dikatakan reliabel jika memberikan nilai Cronbach Alpha > 0,60 [21], [22]. Berdasarkan hasil pengujian reliabilitas, nilai Cronbach Alpha bernilai sebesar 0,827 (Tabel 7) yang mengindikasikan pernyataan dalam kuesioner tergolong reliabel. Semakin tinggi nilai Cronbach Alpha maka semakin reliabel instrumen yang digunakan [23].

Tabel 7. Pengujian Reliabilitas

Nilai Cronbach Alpha	Keterangan
0.827	Reliabel

Hasil Pengukuran Tingkat Kesadaran Keamanan Informasi Pegawai

Hasil pengukuran untuk setiap subjek area diklasifikasikan dengan menggunakan metode HAIS-Q dan Indeks KAMI. Pada tabel hasil pengukuran tingkat kesadaran keamanan informasi dibedakan dalam warna hijau, kuning, merah sesuai dengan Tabel 3. Hasil pengukuran tiap wilayah dijabarkan sebagai berikut:

Tabel 8. Hasil Pengukuran Tingkat Kesadaran di Balai Wilayah A

Fokus Area	*Knowledge*	*Attitude*	*Behaviour*	Total
Password Management	79,57	76,60	74,89	77,02
Mobile Computing	73,62	79,57	70,21	74,47
Social Networking Site (SNS) Use	76,17	77,87	76,17	76,74
Internet Use	82,98	84,68	81,28	82,98
Incident Reporting	87,23	57,02	82,98	75,74
Management Information Assets	73,62	87,66	74,89	78,72
Information Handling	86,81	91,06	87,66	88,51
Email Use	84,26	84,26	82,98	83,83
Total	80,53	79,84	78,88	**79,75**

Berdasarkan Tabel 8, wilayah A mendapatkan nilai total kesadaran keamanan informasi sebesar 79,75 yang termasuk dalam kategori masih rata-rata. Jika ditinjau dari Model KAB, dimensi *Knowledge* tergolong Baik (80,53%), sedangkan dimensi *Attitude* memperoleh nilai 79,84% dan *Behaviour* memperoleh nilai 79,88% dimana nilai tersebut tergolong kategori Rata-Rata. Terdapat 3 fokus area yang termasuk dalam kategori Baik, yaitu *Internet Use* (82,98%), *Information Handling* (88,51%), dan *Email Use* (83,83%). Sedangkan terdapat 5 fokus area lainnya berada pada kategori Rata-Rata dengan nilai total terendah sebesar 74,47% (*Mobile Computing area*). Namun, terdapat area dengan kategori Buruk, yaitu di area *Incident Reporting* dimensi *Attitude* yang memiliki nilai sebesar 57,02%. Nilai tertinggi terdapat pada fokus area *Information Handling* pada dimensi *Attitude* yaitu 91,06%.

Pada Wilayah A, fokus area *incident reporting* pada dimensi Attitude yang masih pada kategori buruk perlu menjadi fokus utama yang perlu ditingkatkan, agar para pegawai dapat menginterpretasikan pengetahuan yang dimiliki terhadap sikap mereka dalam pengambilan keputusan terkait dengan pelaporan insiden keamanan informasi. Oleh karena itu perlu dilakukan sosialisasi kepada pegawai terkait pelaporan insiden bahwa setiap insiden yang terjadi perlu untuk dilaporkan kepada atasan yang bertanggungjawab. Selain itu, secara keseluruhan pada Balai Wilayah A juga masih berada pada kategori rata-rata sehingga perlu untuk dilakukan

pembuatan dan sosialisasi kebijakan maupun standar operasional prosedur secara menyeluruh pada fokus area *password management*, *mobile computing*, SNS *use*, dan *manajemen information asset* untuk peningkatan kesadaran keamanan informasi pegawai.

Tabel 9. Hasil Pengukuran Tingkat Kesadaran di Balai Wilayah B

Fokus Area	*Knowledge*	*Attitude*	*Behaviour*	Total
Password Management	78,52	76,67	79,26	78,15
Mobile Computing	71,11	76,30	70,74	72,72
Social Networking Site (SNS) Use	77,04	78,15	82,22	79,14
Internet Use	72,22	81,11	77,78	77,04
Incident Reporting	91,11	65,19	84,81	80,37
Management Information Assets	72,96	88,15	77,41	79,51
Information Handling	88,52	90,37	88,89	89,26
Email Use	84,44	88,15	86,67	86,42
Total	79,49	80,51	80,97	**80,32**

Berdasarkan Tabel 9, wilayah B mendapatkan nilai total kesadaran keamanan informasi sebesar 80,32 yang termasuk dalam kategori Baik. Jika ditinjau dari Model KAB, dimensi *Knowledge* tergolong Rata-Rata dengan nilai 79,49%, sedangkan dimensi *Attitude* memperoleh nilai 80,51% dan *Behaviour* memperoleh nilai 80,97% dimana kedua nilai tersebut tergolong kategori Baik. Terdapat 3 fokus area yang termasuk kedalam kategori Baik, yaitu *Incident Reporting* (80,37%), *Information Handling* (89,26%), dan *Email Use* (86,42%). Sedangkan terdapat 5 fokus area lainnya berada pada kategori Rata-Rata dimana nilai total terendah terdapat pada area *Mobile Computing* sebesar 72,72%. Nilai total tertinggi terdapat pada fokus area *Information Handling* sebesar 89,26%. Sedangkan nilai total terendah terdapat pada *Mobile Computing* sebesar 72,72%. Selain itu, nilai terendah terdapat pada area *Incident Reporting* dimensi *Attitude* sebesar 65,19%, sedangkan nilai tertinggi terdapat pada area *Information Handling* dimensi *Attitude* sebesar 90,37%.

Pada Wilayah B, rata-rata pegawai telah memiliki tingkat kesadaran keamanan informasi yang baik, namun berdasarkan masing-masing fokus area, masih ada yang terkategori rata-rata di beberapa dimensi. Dilihat dari hasil Wilayah B yang tidak terdapat kategori buruk di masing-masing fokus area, maka dimensi pada fokus area yang masih rata-rata dapat difokuskan ditingkatkan dengan pemberian penyuluhan berkala meningkatkan pengetahuan para pegawai terkait dengan kesadaran keamanan informasi.

Tabel 10. Hasil Pengukuran Tingkat Kesadaran di Balai Wilayah C

Fokus Area	*Knowledge*	*Attitude*	*Behaviour*	Total
Password Management	85,79	86,32	84,74	85,61
Mobile Computing	76,84	84,21	82,11	81,05
Social Networking Site (SNS) Use	86,32	86,32	88,42	87,02
Internet Use	80,00	86,84	84,21	83,68
Incident Reporting	90,00	74,21	87,89	84,04
Management Information Assets	78,95	91,05	84,74	84,91
Information Handling	90,53	92,11	92,11	91,58
Email Use	89,47	89,47	90,53	89,82
Total	84,74	86,32	86,84	**85,96**

Berdasarkan Tabel 10, wilayah C mendapatkan nilai total kesadaran keamanan informasi sebesar 85,96% yang termasuk dalam kategori Baik. Jika ditinjau dari Model KAB, setiap dimensi berada pada kategori Baik, yaitu *Knowledge* memperoleh nilai 84,74%, *Attitude* memperoleh nilai 86,32%, dan *Behaviour* memperoleh nilai 86,84%. Selain itu, semua fokus area tergolong kategori Baik dengan nilai total tertinggi pada area *Information Handling* (91,58%) dan nilai total terendah terdapat pada area *Mobile Computing* (81,05%). Nilai terendah terdapat pada area *Incident Reporting* dimensi *Attitude* dengan nilai sebesar 74,21% dan nilai tertinggi terdapat pada area *Information Handling* dimensi *Attitude* dengan nilai sebesar 92,11%.

Pada Wilayah C, para pegawai telah memiliki tingkat kesadaran informasi yang baik, dilihat dari rata-rata keseluruhan dimensi KAB dan fokus area yang tergolong dalam kategori baik. Berdasarkan hasil tersebut, Wilayah C hanya perlu lebih berfokus untuk mempertahankan tingkat kesadaran keamanan informasi pegawai dengan menyebarkan informasi terkait dengan keamanan informasi secara konsisten. Sedangkan untuk fokus area yang masih berada pada kategori rata-rata perlu ditingkatkan kesadaran keamanan informasi pegawai pada fokus area *password management*, *mobile computing*, SNS *use*, *intertnet use*, dan *manajemen information asset*. Perlunya dilakukan pembuatan dan sosialisasi kebijakan maupun standar operasional prosedur yang jelas terkait fokus area tersebut untuk dapat meningkatkan kesadaran keamanan informasi pegawai di Balai Wilayah C.

Tabel 11. Hasil Pengukuran Tingkat Kesadaran Rata-Rata

Fokus Area	*Knowledge*	*Attitude*	*Behaviour*	Total
Password Management	80,86	79,28	79,28	79,81
Mobile Computing	73,53	79,57	73,67	75,59
Social Networking Site (SNS) Use	79,28	80,29	81,87	80,48
Internet Use	77,99	83,88	80,72	80,86
Incident Reporting	89,50	64,89	85,04	79,81
Management Information Assets	74,82	88,78	78,56	80,72
Information Handling	88,49	91,08	89,35	89,64
Email Use	85,76	87,19	86,47	86,47
Total	81,28	81,87	81,87	**81,67**

Berdasarkan Tabel 11, rata-rata ketiga wilayah mendapatkan nilai total kesadaran keamanan informasi sebesar 81,67% yang termasuk dalam kategori Baik. Jika ditinjau dari Model KAB, setiap dimensi berada pada kategori Baik, yaitu *Knowledge* memperoleh nilai 81,28%, *Attitude* dan *Behaviour* memperoleh nilai 81,87%. Terdapat 5 fokus area yang termasuk kedalam kategori Baik, yaitu *Social Networking Site Use* (80,48%), *Internet Use* (80,86%), *Management Information Assets* (80,72%), *Information Handling* (89,64%), dan *Email Use* (86,47%). Sedangkan, 3 fokus area lainnya berada pada kategori Rata-Rata dimana nilai total terendah terdapat pada area *Mobile Computing* sebesar 75,59%. Nilai tertinggi terdapat pada fokus area *Information Handling* dengan nilai total 86,47%. Rata-rata tingkat kesadaran keamanan informasi secara keseluruhan pada 3 Wilayah Balai BMKG telah tergolong baik, meskipun ada 3 fokus area yang masih tergolong rata-rata. Sehingga, perlu dilakukan tindakan untuk mempertahankan dan meningkatkan tingkat kesadaran keamanan informasi pegawai.

Berdasarkan nilai rata-rata ketiga lokasi Balai Wilayah BMKG yang telah dilakukan pengukuran tingkat kesadaran keamanan informasi pegawai diperoleh bahwa Balai Wilayah A mendapatkan persentase sebesar 79,95% (Rata-Rata), Balai Wilayah B mendapatkan persentase sebesar 80,32% (Baik), dan Balai Wilayah C mendapatkan persentase sebesar 85,96% (Baik). Sehingga, nilai rata-rata untuk ketiga balai wilayah BMKG tergolong Baik dengan nilai 81,67%.

Meskipun nilai rata-rata dari ketiga balai wilayah tersebut tergolong Baik, terdapat Balai wilayah A yang masih berada pada kategori Rata-Rata. Hal ini disebabkan terdapat fokus area yang berada pada kategori Buruk (57,02%) yaitu pada area *Incident Reporting* dimensi *Attitude* pada wilayah A. Hal ini mengindikasikan bahwa responden pada wilayah tersebut masih kurang dalam menginterpretasikan pengetahuan pegawai terhadap sikap yang harus dilakukan apabila terjadi insiden keamanan.

Berdasarkan analisis di ketiga wilayah Balai, terdapat satu fokus area yang berada pada kategori Buruk yaitu terdapat pada wilayah A di fokus area *Incident Reporting* dimensi *Attitude*. Sehingga, sangat direkomendasikan untuk melakukan kegiatan sosialisasi dan pelatihan terhadap para pegawai di wilayah A agar dapat meningkatkan tingkat kesadaran keamana informasi pegawai. Selain itu perlu disusun *standard operational procedur* (SOP) untuk menyamakan persepsi seluruh pegawai terkait tatacara pelaporan insiden keamanan informasi. Sedangkan hasil pengukuran tingkat kesadaran rata-rata dari ketiga wilayah balai yang terdapat fokus area kategori Rata-Rata, diharapkan untuk ditingkatkan ke tingkat kategori baik. Pada fokus area password management, perlu dilakukan penerapan kebijakan terhadap manajemen password pegawai dengan lebih baik, seperti melakukan sosialiasi kebijakan manajemen password secara berkala baik secara offline melalui rapat, online grup disscussion maupun *email blast* kepada seluruh pegawai secara berkala. Perlu adanya tim yang mengawasi ataupun melakukan monitoring secara berkala terkait penerapan manajemen password yang sesuai. Selain itu, untuk fokus area *mobile computing* perlu disosialisasikan lebih lagi terkait resiko penggunaan internet umum/Wifi dalam melakukan pengiriman dokumen-dokumen penting, sehingga para pegawai lebih waspada dalam menggunakan perangkat *mobile* jika terkait dengan data-data penting. Pemberian rekomendasi ini telah divalidasi oleh *expert* dari Pusat Jaringan Komunikasi untuk mendukung peningkatan kesadaran keamanan informasi pegawai dalam rangka menyongsong pengimplementasian ISO 27001 di tahun 2024.

E. Simpulan

Pengukuran tingkat kesadaran keamanan informasi dilakukan dengan menggunakan kombinasi metode HAIS-Q dan indeks KAMI. Pernyataan kuesioner disusun berdasarkan tingkat urgensi fokus area yang dimana setiap fokus area mencakup 3 dimensi, yaitu Knowledge, Attitude, dan Behaviour. Berdasarkan uji validitas dan reliabilitas, pernyataan dinyatakan valid dan reliabel untuk digunakan dalam penelitian.

Hasil penelitian menunjukkan bahwa secara keseluruhan tingkat kesadaran keamanan informasi sudah tergolong Baik, sehingga hanya perlu dilakukan monitoring untuk tindak lanjut dalam mempertahankan tingkat kesadaran keamanan informasi pegawai. Nilai total tingkat kesadaran keamanan informasi pegawai di Balai Wilayah A berada kategori Rata-Rata. Selain itu, tingkat kesadaran keamanan informasi pegawai pada fokus area Incident Reporting dimensi Attitude berada pada kategori Buruk. Oleh karena itu, perlu dilakukan tindak lanjut terlebih dahulu terhadap rekomendasi-rekomendasi yang telah diberikan untuk dapat meningkatkan kesadaran keamanan informasi pegawai di balai wilayah tersebut. Tingkat kesadaran keamanan informasi pegawai pada Balai Wilayah B dan C sudah tergolong baik dan tidak ada fokus area yang berada pada kategori Buruk.

F. Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Badan Meteorologi, Klimatologi, dan Geofisika (BMKG) Republik Indonesia yang telah memberikan dukungan melalui program Beasiswa S2 Dalam Negeri sehingga penelitian ini dapat terlaksana.

G. Referensi

[1] C. A. Cholik, "Perkembangan Teknologi Informasi Komunikasi/ICT dalam Berbagai Bidang," *Jurnal Fakultas Teknik Kuningan*, vol. 2, no. 2, pp. 39–46, 2021.

[2] A. A. Fauzi *et al.*, *Pemanfaatan Teknologi Informasi Di Berbagai Sektor Pada Masa Society 5.0*. PT. Sonpedia Publishing Indonesia, 2023.

[3] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," *Comput Secur*, vol. 88, p. 101640, 2020, doi: https://doi.org/10.1016/j.cose.2019.101640.

[4] Badan Siber dan Sandi Negara RI, *Hasil Monitoring Keamanan Siber*. Jakarta, 2022.

[5] Badan Meteorologi Klimatologi dan Geofisika, "Laporan Monitoring Firewall," Jakarta, 2023.

[6] J. Andress, *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress, 2014.

[7] P. Xu, J. Lee, J. R. Barth, and R. G. Richey, "Blockchain as supply chain technology: Considering transparency and security," *International Journal of Physical Distribution & Logistics Management*, vol. 51, no. 3, pp. 305–324, 2021.

[8] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS quarterly*, vol. 34, no. 3, pp. 523–548, 2010, doi: 10.2307/25750690.

[9] E. A. Puspitaningrum, F. T. Devani, V. Q. Putri, A. N. Hidayanto, Solikin, and I. C. Hapsari, "Measurement of Employee Information Security Awareness: Case Study at A Government Institution," in *2018 Third International Conference on Informatics and Computing (ICIC)*, 2018, pp. 1–6. doi: 10.1109/IAC.2018.8780571.

[10] A. McIlwraith, *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*. Routledge, 2021.

[11] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput Secur*, vol. 42, pp. 165–176, 2014, doi: https://doi.org/10.1016/j.cose.2013.12.003.

[12] Kominfo, *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik*. Jakarta: Kementerian Komunikasi dan Informatika RI, 2011.

[13] E. Kritzinger, A. Da Veiga, and W. van Staden, "Measuring organizational information security awareness in South Africa," *Information Security Journal: A Global Perspective*, vol. 32, no. 2, pp. 120–133, Mar. 2023, doi: 10.1080/19393555.2022.2077265.

[14] K. F. Arisya, Y. Ruldeviyani, R. Prakoso, and A. L. Fadhilah, "Measurement of information security awareness level: A case study of mobile banking (m-banking) users," in *2020 Fifth International Conference On Informatics And Computing (Icic)*, IEEE, 2020, pp. 1–5.

[15] D. S. Hermawan, F. Setiadi, and D. Oktaria, "Measurement Level of Information Security Awareness for Employees Using KAB Model with Study Case at XYZ Agency," in *2022 1st International Conference on Software Engineering and Information Technology (ICoSEIT)*, IEEE, 2022, pp. 174–179.
[16] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput Secur*, vol. 25, no. 4, pp. 289–296, 2006, doi: https://doi.org/10.1016/j.cose.2006.02.008.
[17] C. R. Kothari, *Research methodology: Methods and techniques*. New Age International, 2004.
[18] M. Azwar, I. Surandari, and H. I. Djohar, "Evaluating the library website of the Indonesian Ministry of Education and Culture through the End-User Computing Satisfaction (EUCS) model," *Library Philosophy and Practice (e-journal)*, 2020.
[19] G. P. Adhikari, "Calculating the Sample Size in Quantitative Studies," *Scholars' Journal*, pp. 14–29, 2021.
[20] H. Taherdoost, "What is the best response scale for survey and questionnaire design; review of different lengths of rating scale/attitude scale/Likert scale," *Hamed Taherdoost*, pp. 1–10, 2019.
[21] R. Alfian and A. M. P. Putra, "Uji validitas dan reliabilitas kuesioner medication adherence report scale (Mars) terhadap pasien diabetes mellitus," *Jurnal Ilmiah Ibnu Sina*, vol. 2, no. 2, pp. 176–183, 2017.
[22] S. S. Harahap, "Hubungan usia, tingkat pendidikan, kemampuan bekerja dan masa bekerja terhadap kinerja pegawai dengan menggunakan metode Pearson Correlation," *Jurnal Teknovasi*, vol. 6, no. 2, pp. 12–26, 2019.
[23] M. Amirrudin, K. Nasution, and S. Supahar, "Effect of variability on Cronbach alpha reliability in research practice," *Jurnal Matematika, Statistika dan Komputasi*, vol. 17, no. 2, pp. 223–230, 2021.