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

# Measurement of Employee Information Security Awareness: A Case Study of National Civil Service Agency

**Ahmad Fadhil[1], Setiadi Yazid[2]**
ahmad.fadhil23@ui.ac.id, setiadi@cs.ui.ac.id
University of Indonesia

**Article Information**

Submitted : 27 Dec 2023
Reviewed: 29 Dec 2023
Accepted : 30 Dec 2023

**Keywords**

BKN, ASN, HAIS-Q, KAB, Information security Awareness

**Abstract**

National Civil Service Agency is a State institution tasked with the role and function of overseeing and implementing national civil servant management using information technology. There are 4.2 million civil servant data distributed throughout Indonesia that must be safeguarded by BKN. As the utilization of information systems grows, it also leads to an increase in information security risks. Based on the reports from Id-SIRTII/CC and BKN's internal report, there has been an increase in cyber attacks targeting BKN. In addition, there are other types of attacks that occur, such as online defacement, phishing, DDOS, and employee data theft, as well as the presence of employees who are still indifferent to information security. Based on this, the objective of this research is to measure the level of information security awareness among BKN employees and identify the factors that influence it. The Human Aspects of Information Security Questionnaire (HAIS-Q) using the Knowledge, Attitude, and Behavior (KAB) model was selected for measurement, with an additional focus on the Management of Information Systems/Technology Assets, consisting of a total of 75 statements. The quantitative measurements conducted yielded a result of 88.80% for the level of information security awareness among BKN employees, categorized as good. Furthermore, there is a significant influence on information security awareness from the dimensions of knowledge towards attitude, attitude towards behavior, and knowledge towards behavior.

## A. Introduction

The National Civil Service Agency (BKN) is a non-ministerial institution that is held accountable to the President via the minister of state apparatus empowerment and bureaucratic reform, as stipulated in Presidential Regulation (Perpres) Number 58 of 2013. The provisions of Presidential Regulation 58/2013 regarding the role, responsibilities, and operations of BKN were expanded with the enactment of Law No. 5 of 2014 pertaining to State Civil Apparatus (ASN) [1]. As stipulated in Law 5/2014, Article 1, Paragraph (21) designates BKN with the responsibility of coordinating and instructing ASN Management in Indonesia.

Additionally, BKN is tasked with safeguarding the data of ASN, which is in charge of data and information management in the ASN domain. According to a statistical book published by BKN, the total number of civil servants in Indonesia is 4.28 million. Among this workforce, central agencies employ the remaining 25% and regional agencies employ 75% of the civil servants.

BKN has supported its duties and functions with information technology and provided services to the community and civil servants. BKN manages a total of 166 web-based information systems, which include the BKN portal site (www.bkn.go.id), the ASN Information System (siasn.bkn.go.id) [2], the CASN selection system (www.ssacsn.bkn.go.id) [3], the ASN performance system (kinerja.bkn.go.id), the National Civil Service Information System (simpegnas.bkn.go.id), and nineteen additional information system services are managed by BKN.

As the government sector increasingly implements information systems, it becomes more susceptible to information security disruptions. Security Incident Response Team on Internet Infrastructure/Coordination Center (Id-SIRTII/CC) annual report for 2022 Indonesia ranks among the ten countries most targeted by cyber attacks, accounting for 976,429,996 incidents. Among these, the MyIoBot Botnet, capable of assuming complete control over user systems, stands as the most severe, with a total of 254,260,339 attacks. Indonesia experienced 2,348 instances of web defacement in the same year, with the government sector being the most severely impacted with 885 cases [4].

According to the report, a total of 236 complaints were lodged in 2022, with the government administration sector receiving the highest number of complaints. There are 21,302 government-related files exposed on the darknet. In order to create the possibility that negligent individuals may exploit it for their own benefit. Among the 427 agencies in Indonesia that have experienced data exposure in the darknet, the government sector accounts for the largest proportion (76.20%). Furthermore, 98 incidents of data breaches were reported to have occurred in the government sector, making it the sector most likely to be the target of data theft [4].

Furthermore, information from the Directorate of Information Technology Infrastructure BKN indicates that between 2022 and 2023, a total of 27 security and data center incidents transpire. The aforementioned incidents have underscored the importance of information security cognizance among BKN employees. While monitoring tools and security technologies like firewalls are crucial components of security, the human element must also be taken into account.

A multitude of prior studies have examined the technique of measuring information security awareness. In South Africa, Kritzinger et al. (2023) conducted research to validate the HAIS-Q instrument. According to the findings of this research, gender, age, language proficiency, and organizational size are all significant considerations in the development, creation, or revision of information security awareness programs [5]. An additional research investigation, conducted by Vina Ardelia Effendy et al. (2022), assessed the degree of information security cognizance at XYZ polytechnic through the utilization of HAIS-Q modeling. The study's results indicated that the research site possessed a moderate level of awareness [6], suggesting that additional monitoring efforts are necessary to raise awareness. Fadlika et al. (2023) assessed PT ABC's awareness of information security through the implementation of the HAIS-Q method in conjunction with the IS/IT Asset Management Focus Area. On the basis of the user survey, the authors identified the areas in need of development but refrained from offering recommendations [7].

The Human Aspects of Information Security-Questionnaire (HAIS-Q) is an internationally acknowledged instrument utilized to assess cognizance of information security on a global scale. The HAIS-Q has been employed in a multitude of instances, encompassing academic institutions, government agencies, and commercial enterprises [5], [7]–[10]. Despite its extensive adoption, previous research has yet to integrate the HAIS-Q with the ISO/IEC 27001:2013 standard, and no research has specifically investigated the extent of awareness of information security among employees of BKN. Furthermore, there is no research that explicitly examines the degree of information security awareness among BKN employees [11].

The aforementioned description suggests that in order to safeguard the accessibility, privacy, and integrity of the data held, numerous organizations have established information security as a critical concern within their information management [12]. To enhance information security, it is imperative to augment the security consciousness and understanding of all personnel regarding the fundamental principles of information security [13]. This study will determine the extent to which BKN employees are cognizant of information security and the determinants of that awareness. The findings of this inquiry will provide suggestions for improving the security protocols of the organization. It is anticipated that these insights will positively impact the level of awareness regarding information security at BKN.

## B. Research Method

This research employed a mixed methods approach, integrating both qualitative and quantitative preliminary data. Qualitative data were gathered through interviews, while quantitative data were collected through surveys. Qualitative research possesses intricate attributes due to its emphasis on comprehensive comprehension and depiction of an individual's experience within a specific context [14], [15]. Qualitative data collected by researchers must therefore be processed using suitable techniques or analytic methods in order to obtain answers consistent with the formulation of the research problem and to comprehend the social and cultural context associated with the phenomenon

under investigation. A case study methodology appropriate for information security awareness measurement research was implemented. In the interim, secondary data collection was conducted to supplement the requirements of this research through a review of the methods literature and literature studies from multiple prior studies.

The questionnaire was employed as the research instrument in this study, which incorporated results from prior scholarly publications and included citations [5]–[7], [10], [16]–[19]. The security question components of the questionnaire are derived from eight areas of the ISO/IEC 27001:2013 standard [7], [11] and seven main areas of the HAIS-Q [7], [18]. Password management, email usage, internet usage, social media usage, mobile device usage, information control, and incident reporting are among the seven domains that exhibit substantial overlap. However, in the realm of IT/IS asset management, there is no overlap. Password management, email usage, internet usage, social media usage, mobile device usage, information control, incident reporting, and IT/IS asset management are thus the primary areas of interest for this study. Furthermore, as shown in Table 1, each of these areas of concentration is subdivided into three distinct dimensions: knowledge, attitude, and behavior (K, A, B).

**Table 1.** Research Design Summary

| no | Focus Area | Focus Area Code | Sub Focus Area | Indicator Code |
|---|---|---|---|---|
| 1 | Password Management | A | Using the same Password<br>Sharing Passwords<br>Using a Strong Password | KA, AA, BA |
| 2 | Email Use | B | Known sender email link clicking<br>Unknown sender email link clicking<br>Opening attachments in emails from unknown sender | KB, AB, BB |
| 3 | Internet Use | C | Downloading Files<br>Accessing Dubious Websites<br>Entering Information Online | KC, AC, BC |
| 4 | Social Media Use | D | SM privacy Setting<br>Considering consequences<br>Posting about work | KD, AD, BD |
| 5 | Mobile Devices | E | Physically Securing Mobile devices<br>Sending Sensitive Information via Wi-Fi<br>Shoulder Surfing | KE, AE, BE |
| 6 | Information Handling | F | Disposting of sensitive print-outs<br>Inserting Removable media<br>Leaving Sensitive Material | KF, AF, BF |
| 7 | Incident Reporting | G | Reporting suspicious behavior<br>Ignoring poor security behavior by colleagues | KG, AG, BG |
| 8 | IS/IT Asset Management | H | Security insident reporting<br>Regulations for installing software on agency-owned IT assets. | KH, AH, BH |

Using the sample determination formula created by Slovin, the number of samples used in this investigation was ascertained as follows:

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

Notes:
n = Number of samples to be analyzed
N = Total population of BKN
e = margin of error

Based on the given equation, the research sample size was 342 out of a total of 2394 personnel in BKN. The margin of error was 5% and the accuracy rate was 95%.

The data gathering approach employs a questionnaire that was disseminated to respondents between December 1st and December 6th, 2023. The questionnaires are disseminated in the format of statements through the utilization of the Google Form specifically designated for the ASN at BKN. The questionnaire employs a Likert scale ranging from 1 to 5, with "1" indicating strong disagreement, "2" indicating disagreement, "3" indicating neutrality, "4" indicating agreement, and "5" indicating strong agreement. The stages of this investigation are illustrated in Figure 1 below:

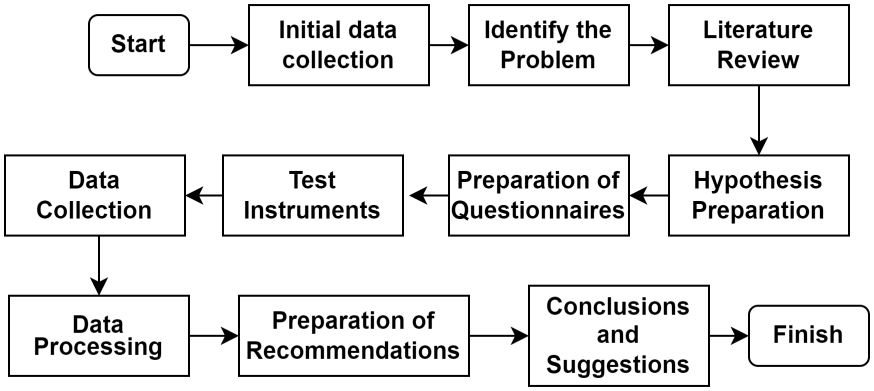


**Figure1.** Stages of Research

To measure the level of information security awareness, this study refers to the KAB model introduced by Kruger & Kearney (2006) using descriptive statistical data analysis. As for the stages of analysis used as follows [13]:

a. Create a query answer distribution table according to the focus area.
b. Calculation of the values received from respondents based on each area focus according to the assessment already established.
c. To summarize the scores of the respondents' answers.
d. Calculation of average values.
e. Calculate the percentage of each focus area using the formula:

$$DP = \frac{n}{N} \times 100\%$$

Explanation of the formula:
DP = Descriptive Percentage (%)
n = Scores obtained.
N = Maximum score for the question item

f. Assess percentage results using predetermined assessment categories [13] where percentage measures can be applied to each focus area.

The information security awareness level is measured using the scale in Table 2 [13].Three categories are used to categorize information security awareness levels: good (measured between 80 and 100%), right (measured between 60 and 79%), and low (values ≤ 59).

**Table 2**. Information security awareness assessment scale

| Awareness | Measurement (%) |
|---|---|
| **Good** | 80-100 |
| **Average** | 60-79 |
| **Poor** | ≤ 59 |

The study will assess both the staff's level of awareness regarding information security and the factors that impact this awareness. The hypothesis of this investigation is depicted in Figure 2.

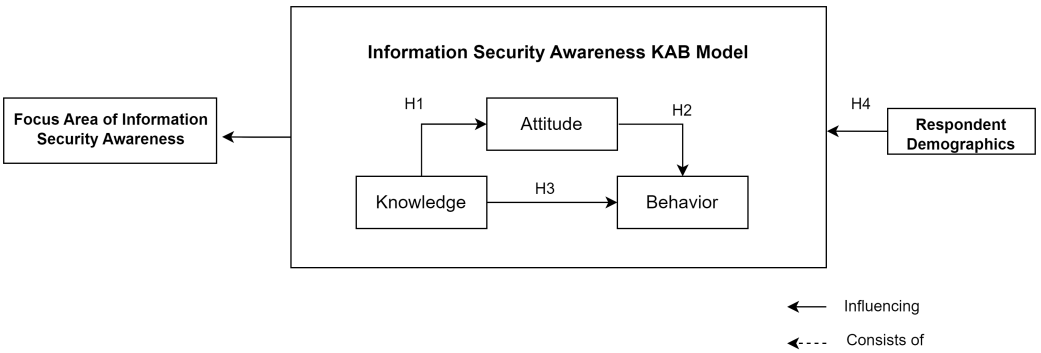


**Figure2.** The Research Hypothesis

The Research hypothesis consists of:

- HI: The knowledge dimension has a significant effect on the attitude dimension,
- H2: The knowledge dimension has a significant effect on the behavior dimension
- H3: The attitude dimension has a noteworthy impact on the behavior dimension
- H4: The Demographics Respondent has a significant effect on the Knowledge, Attitude, and Behavior Model

## C. Result and Discussion

### 1. Demographic of Respondents

A total of 356 respondents completed the questionnaire. The demographic characteristics of the participants in this study encompassed gender, age, job tenure, educational level, position, and work unit at BKN. Table 3 displays the demographic characteristics of the participants.

**Table 3**. Respondent Demographics

| Categories | | Total | Percentage |
|---|---|---|---|
| **Gender** | Male | 185 | 52% |
| | Female | 171 | 48% |
| **Age** | <= 26 years | 44 | 12% |
| | 27-42 years | 290 | 82% |
| | 43-58 years | 21 | 6% |
| | > 58 years | 1 | 0,3% |
| **Job tenure** | SMA (High school) | 5 | 5% |
| | D1/D2/D3 (Diploma) | 23 | 6% |
| | D4/S1 (Bachelor) | 247 | 69% |
| | S2 (Master) | 79 | 22% |
| | S3 (Doctor) | 2 | 1% |
| **Job Title** | Managerial | 16 | 4% |
| | Non-Managerial | 340 | 96% |
| **Working Unit** | BKN headquarters | 196 | 55% |
| | Regional Office | 160 | 45% |

The questionnaire was predominantly completed by male employees, including 52% of the total respondents. Out of the participants who completed the questionnaire, 82% fell between the age range of 27 to 42 years, while only one responder was older than 58 years. 69% of respondents had a D4/S1 degree, whereas only 1% had a doctoral-level education. The majority of employees, specifically 96%, have non-managerial roles, while the remaining 4% are in managerial positions. Finally, the central BKN employs 55% of the workforce, while the BKN regional office employs the remaining 45%.

### 2. Results of the Information Security Awareness Level Measurement

According to the examination of descriptive statistical data, the overall level of information awareness among BKN staff regarding information security is rated as "good" with a score of 89%. This value is derived from the mean of the values across all indicators of statements within the knowledge dimension, attitude dimension, and behavioral dimension. In terms of information security, the knowledge dimension has a score of 88% on the "well" scale, the attitudinal dimension has a value of 89% on the "good" scale, and the behavioral dimension also has a value of 89% on the "good" scale.

**Table 4**. Results of The Information Security Awareness Level Measurement

| no | Code | Focus Area | Knowledge | Attitude | Behavior | Awareness level |
|---|---|---|---|---|---|---|
| **1** | A | Password Management | 88 | 88 | 88 | 88 |
| **2** | B | Email Use | 88 | 88 | 86 | 87 |
| **3** | C | Internet Use | 91 | 87 | 84 | 87 |
| **4** | D | Social Media Use | 91 | 90 | 91 | 90 |
| **5** | E | Mobile Devices | 90 | 88 | 90 | 89 |
| **6** | F | Information Handling | 91 | 91 | 91 | 91 |
| **7** | G | Incident Reporting | 88 | 90 | 88 | 88 |
| **8** | H | IS/IT Asset Management | 88 | 90 | 89 | 89 |
| | | **Average** | 89 | 89 | 88 | 89 |

Based on the provided table, it is evident that the behavioral dimension exhibits the lowest average value of 88% in comparison to the attitude and behavior dimensions. Concurrently, the mean result for both the knowledge and attitude aspects is 89%. The emphasis area with the lowest score is the domain of electronic mail usage and internet usage. While the value of this scale, as derived from Kruger & Kearney (2006), is considered favorable, it does not guarantee the absence of information security incidents in the specific area of interest. This was demonstrated through the outcomes of interviews, which revealed that certain employees continued to access links from dubious senders due to their perceived curiosity, leading to occurrences of information security issues.

Moreover, the areas that received the greatest marks were information management, with an average of 91%, and social media utilization, with an average of 90%. The significant importance of information handling lies in the presence of document shredding equipment in every work group, facilitating the disposal of papers for employees. Furthermore, BKN has transitioned its primary business operations to digital platforms, resulting in a significant reduction in the printing of sensitive documents. Social media usage was highly rated due to the limits imposed on employees of BKN, a government agency, to prevent the dissemination of potentially disruptive content in society. Consequently, BKN employees exercise greater caution when utilizing social media platforms, particularly those pertaining to their professional responsibilities.

## 3. Hypothesis Testing

The data processing was carried out to obtain the results of the hypothesis test. The study used the application SmartPLS 4.0 with the method of partial least squares structural equation modeling (PLS-SEM) because it has good performance in dealing with complex models, does not limit sample size, as well as data distribution [20]–[22]. At the initial stage, the dissemination of the questionnaire was carried out on a small scale as a pre-test, with 35 respondents from the ASN Officer in. Then, after the pre-tests using validity and reliability tests were subsequently conducted, main disseminations of the quizzer were obtained, and 356 respondents were obtained that could be resumed for further examination.

### a. Validity Test

The validity test is employed to assess the load factor value utilizing the smartPLS application. Based on the Hair et al. study (2021), any factor value below 0.70 should be excluded in order to ensure that the research model yields a validity value that meets the specified criteria.

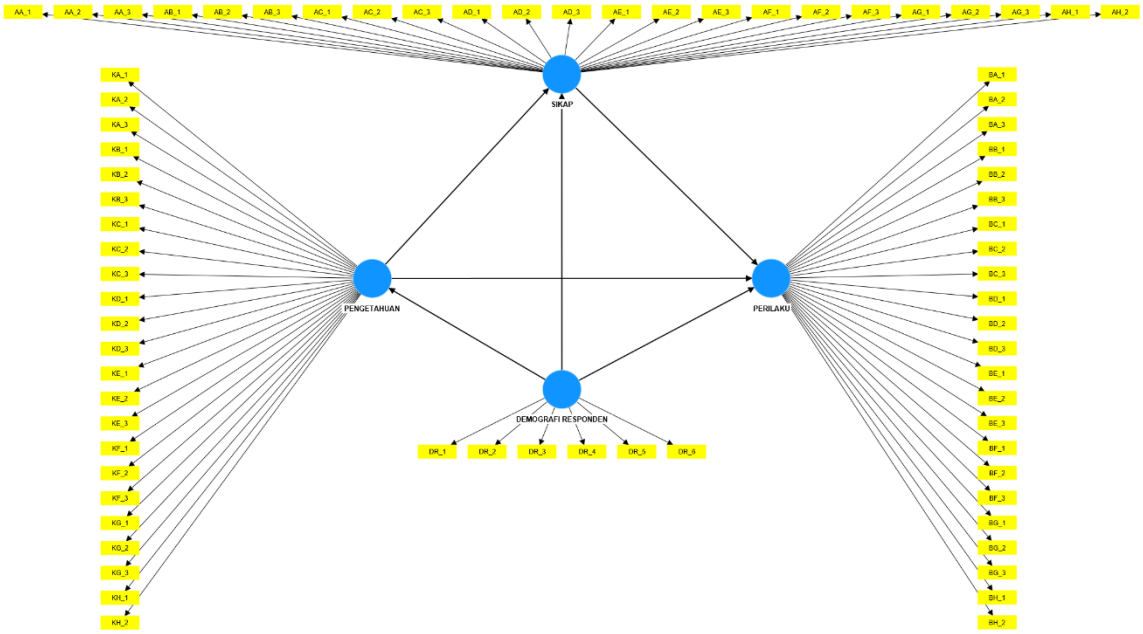


**Figure3.** Research Model

According to the validity test results, there is a questionnaire indication with a value less than 0.70, indicating that the indicator should be eliminated [21]. The indicators that have been eliminated based on the variables can be observed in the subsequent information:

- Knowledge Variable : KD_1, KD_2, KD_3, KE_1, KE_2, KE_3, KF_1, KF_2, KH_1, KA_1, KA_2, KA_3, KB_1, KB_2, KB_3, KC_1, KC_2, KC_3, dan KH_2
- Attitude Variable : AB_1, AB_2, AB_3, AD_2, AD_3, AE_1, AH_1, AA_1, AA_2, dan AA_3
- Behavior Variable : BA_1, BA_2, BA_3, BB_1, BB_2, BB_3, dan BD_1
- Demographic Variable : DR_2, DR_3, DR_4, DR_5, dan DR_6

Then the outer model will change to the figure 4 after removing some indicators:

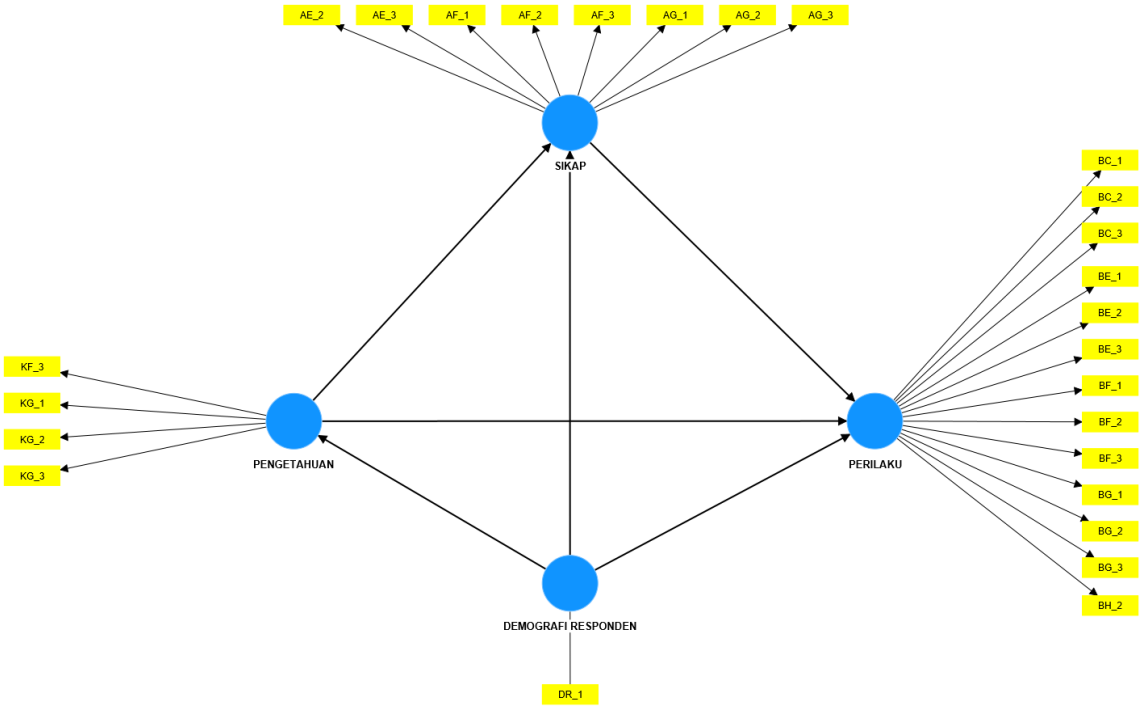


**Figure4.** Research Model After Deletion

As can be seen in the table 5, after restarting the PLS algorithm, every indication has a value greater than 0.70.

**Table 5**. Loading Factors

| | Knowledge | Attitude | Behavior | Respondent Demographics |
|---|---|---|---|---|
| **KF_3** | 0.789 | | | |
| **KG_1** | 0.863 | | | |
| **KG_2** | 0.871 | | | |
| **KG_3** | 0.857 | | | |
| **AC_1** | | 0.716 | | |
| **AD_1** | | 0.721 | | |
| **AE_2** | | 0.753 | | |
| **AE_3** | | 0.828 | | |
| **AF_1** | | 0.833 | | |
| **AF_2** | | 0.815 | | |
| **AF_3** | | 0.825 | | |
| **AG_1** | | 0.839 | | |
| **AG_2** | | 0.853 | | |
| **AG_3** | | 0.836 | | |
| **AH_2** | | 0.719 | | |
| **BC_1** | | | 0.789 | |
| **BC_2** | | | 0.783 | |
| **BC_3** | | | 0.782 | |
| **BD_2** | | | 0.751 | |
| **BD_3** | | | 0.703 | |
| **BE_1** | | | 0.763 | |

| | | |
|---|---|---|
| **BE_2** | 0.776 | |
| **BE_3** | 0.824 | |
| **BF_1** | 0.824 | |
| **BF_2** | 0.812 | |
| **BF_3** | 0.842 | |
| **BG_1** | 0.811 | |
| **BG_2** | 0.786 | |
| **BG_3** | 0.830 | |
| **BH_1** | 0.704 | |
| **BH_2** | 0.741 | |
| **DR_1** | | 1.000 |

Hair et al. (2021) state that when the average variance extracted (AVE) value is greater than 0.50 and satisfies the Fornell-Larcker criterion, both the validity and reliability of the data are evaluated.

**Table 5**. AVE Score

| Variable | AVE Score | Description |
|---|---|---|
| **Knowledge** | 0.689 | Valid |
| **Behavior** | 0.598 | Valid |
| **Attitude** | 0.650 | Valid |
| **Respondent Demographics** | 1 | Valid |

**Table 6**. Fornell Larcker Criterion

| Variabel | Respondent Demographics | Knowledge | Behavior | Attitude |
|---|---|---|---|---|
| **Knowledge** | 1.000 | | | |
| **Behavior** | 0.039 | 0.830 | | |
| **Attitude** | 0.090 | 0.716 | 0.773 | |
| **Respondent Demographics** | 0.103 | 0.692 | 0.768 | 0.806 |

In validity assessment, AVE must have a minimum value of 0.50, while the Fornell-Larcker criterion requires that the square root of AVE should be greater than its correlation with other variable constructs [21]. Both criteria have been met, showing whether the test instrument has passed the validity test.

The measurement of cross loading values is carried out in order to validate against previous measurements by checking the magnitude of correlation between the construction variable and its indicator against other construction variables. Table 6 has met validation criteria based on cross-load values.

**Table 7**. Cross Loading Score

| | Respondent Demographics | Knowledge | Behavior | Attitude |
|---|---|---|---|---|
| **AE_2** | 0.094 | 0.479 | 0.557 | 0.747 |
| **AE_3** | 0.125 | 0.618 | 0.646 | 0.808 |
| **AF_1** | 0.109 | 0.508 | 0.594 | 0.809 |
| **AF_2** | 0.095 | 0.487 | 0.609 | 0.787 |
| **AF_3** | 0.053 | 0.532 | 0.621 | 0.816 |
| **AG_1** | 0.008 | 0.588 | 0.652 | 0.823 |

| | | | | |
|---|---|---|---|---|
| **AG_2** | 0.099 | 0.650 | 0.618 | 0.836 |
| **AG_3** | 0.083 | 0.577 | 0.648 | 0.818 |
| **BC_1** | 0.107 | 0.511 | 0.754 | 0.550 |
| **BC_2** | 0.113 | 0.533 | 0.748 | 0.555 |
| **BC_3** | -0.001 | 0.512 | 0.736 | 0.531 |
| **BE_1** | 0.033 | 0.472 | 0.732 | 0.564 |
| **BE_2** | 0.074 | 0.471 | 0.759 | 0.576 |
| **BE_3** | 0.077 | 0.558 | 0.803 | 0.593 |
| **BF_1** | 0.142 | 0.557 | 0.798 | 0.620 |
| **BF_2** | 0.107 | 0.541 | 0.807 | 0.632 |
| **BF_3** | 0.054 | 0.629 | 0.818 | 0.669 |
| **BG_1** | 0.035 | 0.608 | 0.799 | 0.600 |
| **BG_2** | 0.060 | 0.619 | 0.783 | 0.590 |
| **BG_3** | 0.051 | 0.682 | 0.821 | 0.666 |
| **BH_2** | 0.046 | 0.459 | 0.685 | 0.556 |
| **KF_3** | 0.064 | 0.762 | 0.550 | 0.546 |
| **KG_1** | 0.041 | 0.849 | 0.567 | 0.540 |
| **KG_2** | 0.057 | 0.864 | 0.635 | 0.617 |
| **KG_3** | -0.029 | 0.842 | 0.620 | 0.590 |
| **DR_1** | 1.000 | 0.039 | 0.090 | 0.103 |

### b. Reliability Test

Reliability testing was conducted as part of the outer model testing to determine its composite realibility and Cronbach Alpha values. Any constructive variable's value is considered dependable if its Cronbach Alpha and composite realisibility value are both greater than or equal to 0.70. Table 8 displays the values that were found in this investigation.

**Table 8**. Reliability Score

| Variable | *Cronbach's alpha (≥ 0,70)* | *Composite reliability (≥ 0,70)* |
|---|---|---|
| **Knowledge** | 0,849 | 0,875 |
| **Behavior** | 0,944 | 0,9485 |
| **Attitude** | 0,923 | 0,931 |
| **Responden Demographics** | 1 | 1 |

The total value of each constructive variable exceeds 0.70. The largest value is obtained from the respondent's demographic variable, with a value of one for Cronbach's alpha and composite reliability, respectively, while the smallest value is found on the knowledge variable, with a Cranbach alpha value of 0.875 and composite reliability of 0.849.

### c. Structural Model Test

In structural model testing, the calculations are carried out using the bootstrapping algorithm in SmartPLS. Through the bootstrapping procedure, using 5000 samples, path coefficient values (path coefficient), determination coefficient

(R square), effect measurements (F square), and variance analysis (Q square) will be analyzed.

**Table 9**. R-Square Score

| Variable | R-square | Category |
|---|---|---|
| **Knowledge** | 0.002 | Poor |
| **Behavior** | 0.656 | Moderate |
| **Attitude** | 0.485 | Moderate |

The knowledge variable yields an R2 value of 0.02, which means that only 2% of the knowledge variables are affected by other variables and as much as 98% are influenced by other factors.

On the attitude variable, the R2 value is 0.656, which means as much as 65% of the attitudinal variable is influenced by knowledge, behavior, and demographic variables, while the other 45% is affected by other factors.

The behavioral variable R2 is 0.485, which means that 48.5% of the behavior variables are influenced by knowledge, attitudes, and demographic variables, while the other 51.5% are affected by other factors.

**Table 10**. F-Square Score

| H | Variable correlation | F-Square | Description |
|---|---|---|---|
| **H1** | Knowledge -> Attitude | 0,921 | Strong |
| **H2** | Attitude -> Behavior | 0,405 | Strong |
| **H3** | Knowledge -> Behavior | 0,191 | Moderate |
| | Respondent Demographics -> Knowledge | 0,002 | Poor |
| **H4** | Respondent Demographics -> Attitude | 0,001 | Poor |
| | Respondent Demographics -> Behavior | 0,011 | Poor |

The relationship value of the variables Knowledge->Attitude and Attitude-> Behavior has values of 0.921 and 0.405, so it can be categorized strongly. The correlation of knowledge with behavior had a value of 0.191, which is categorized as moderate. Last The demographic correlations of respondents with the variables of knowledge, attitude, and behavior have values <= 0.02, so they are categorized as poor.

**Table 11**. Q-Square Score

| Variabel | SSO | SSE | $Q^2$ (=1-SSE/SSO) | Relevansi |
|---|---|---|---|---|
| **Respondent Demographic** | 354.000 | 354.000 | 0.000 | |
| **Knowledge** | 1.416.000 | 743.485 | -0.000 | |
| **Behavior** | 4.602.000 | 2.160.177 | 0.387 | *Large* |
| **Attitude** | 2.832.000 | 1.279.741 | 0.310 | *Medium* |

The Q-Square value of the endogenous variable of knowledge is 0 = 0, so it can be concluded that other variables have no predictive relevance to the knowledge variable.

The Q-Square value of the behavioral endogenous variable is 0.387 > 0, so it can be concluded that other variables have predictive relevance to the attitude variable.

The Q-Square value on the endogenous variable of attitude is 0.310 > 0, but still less than 0, so it can be concluded that other variables have predictive relevance to the attitude variable.

### d. Hypothesis testing results

The hypothesis test is the final stage after outer model and inner model testing. The hypothesis test phase in the SmartPLS application involves the evaluation of path coefficients on previously tested variables as well as comparing the statistical t-values to determine whether the hypotheses are accepted or rejected. Table 9 is the output of the value of each correlation between variables in direct effect.

**Tabel 12.** Path Coefficient

| H | Variable Correlation | Path Coefficient | T statistics (≥ 1.96) | P values (< 0,05) | Conclution | |
|---|---|---|---|---|---|---|
| | | | | | Value | Significance |
| **H1** | K -> A | 0.689 | 15.808 | 0.000 | Positive | Significant |
| **H2** | A -> B | 0.520 | 5.398 | 0.000 | Positive | Significant |
| **H3** | K -> B | 0.355 | 4.075 | 0.000 | Positive | Significant |
| **H4** | DR -> K | 0.039 | 0.747 | 0.455 | Negative | Not Significant |
| | DR -> A | 0.076 | 2.019 | 0.044 | Negative | Significant |
| | DR -> B | 0.022 | 0.685 | 0.493 | Negative | Not Significant |

**Description:**
**K: Knowledge** **DR: Respondent Demographics**
**A: Attitude**
**B: Behavior**

Table 9 indicates that the direct effect estimates for H1, H2, and H3 are all positive and statistically significant, indicating that all three hypotheses are accepted. The association between knowledge and attitude yields the highest t-statistics value (15,808), whereas the relationship between a respondent's demography and behavior yields the lowest value (0,022). There is a significant t-statistics value of 2,019 in the respondent's demographic association to attitude, but the p-values are < 0.05 or negative, meaning the hypothesis that results is not acceptable.

### e. Recomendations

Research recommendations related to IT in the government can come from aspects of technology, organization, and work environment [23]. As to the description of the recommendations for the three aspects, it is as follows:.

- Technology aspects. Some things can be done in terms of raising the awareness of employees about information security from the technology side, among others: The workshop is related to technology that is often used in performing day-to-day work.

• Environmental Aspects: Create consistent information security awareness campaigns through posters, brochures, emails, or newsletters explaining security risks and safeguards.

• Organizational aspects: BKN can create a security awareness policy so that every employee can clearly understand the agency's information security policy and provide channels for questions about understanding the policy.

In addition, a survey was conducted to see the information security improvement program requested by employees, which can be seen in the table below.

**Table 13.** Recomendations

| no | Code | Information Security Awareness Program | Total | Percentage | Priority |
|---|---|---|---|---|---|
| **1** | P-1 | Message Delivery using social media | 278 | 23% | 1 |
| **2** | P-2 | Conducting an Online Workshop | 196 | 16% | 2 |
| **3** | P-3 | Conducting an Offline Workshop | 169 | 14% | 4 |
| **4** | P-4 | Conducting Seminar | 151 | 12% | 5 |
| **5** | P-5 | Guidelines book inclusion | 130 | 11% | 6 |
| **6** | P-6 | Making Flyer/Poster | 169 | 14% | 3 |
| **7** | P-7 | Making Brochure | 100 | 8% | 7 |
| **8** | P-8 | Other Answer | 21 | 2% | 8 |
| | | **Total** | 1214 | 100% | |

## D. Conclusion

The study aims to validate the KAB model that adds the respondent demographic variable using a seven-focus HAIS-Q area questionnaire and a SI/TI asset management area focus to become a model that can measure the level of information security awareness of officials in the National Civil Service Agency by carrying out measurements on officials using questionnaires.

Furthermore, this study will provide recommendations related to programs that can raise awareness of information security among BKN staff. As regards the recommendations based on data collection from questionnaires that have been completed by respondents in this study, from the results of this study, it can be concluded that:

1. The overall measurement of the level of information security awareness in the National Civil Service Agency is on the "good" scale, with a presentation value of 89%.
2. Based on the test results, we have obtained the hypothesis that the dimension of knowledge has a positive and significant influence on the dimension of attitude, the dimension of attitude has a positive and significant influence on the dimension of behavior, and the dimension of

knowledge has a positive and significant influence on the dimension of behavior. The results of this study align with previous research conducted by other scholars.

3. To maintain and raise awareness of future information security, it is necessary to carry out periodic evaluations of the well-dispatched measurements obtained from this study. To achieve this goal, we can make five priority recommendations, including: (1) the delivery of information through social media channels; (2) holding workshops; (3) making posters or flyers; and (4) including a book of information security guidelines in the management of SI and IT in BKN. (5) Making an Information Security Policy.

## E. Acknowledgment

The author would like to express gratitude to the Ministry of Communication and Information of the Republic of Indonesia (Kemenkominfo RI) for the Domestic Masters Scholarship program that was received.

## F. References

[1] Perpres, "Presiden Republik Indonesia Peraturan Presiden Republik Indonesia tentang Badan Kepegawaian Negara," *Demogr. Res.*, pp. 4–7, 2013.

[2] BKN, "Sistem Informasi Aparatur Sipil Negara (SIASN)," *Online*, 2021. https://www.bkn.go.id/layanan/siasn/ (accessed Dec. 20, 2023).

[3] BKN, "Sistem Seleksi Calon Aparatur Sipil Negara (SSCASN)," *Online*, 2021. https://www.bkn.go.id/layanan/sscasn/ (accessed Dec. 20, 2023).

[4] Id-SIRTII/CC, "Keamanan siber indonesia 2022," 2022.

[5] E. Kritzinger, A. Da Veiga, and W. van Staden, "Measuring organizational information security awareness in South Africa," *Inf. Secur. J.*, vol. 32, no. 2, pp. 120–133, 2023, doi: 10.1080/19393555.2022.2077265.

[6] V. A. Effendy, Y. Ruldeviyani, M. M. Rifa'i, V. A. Rahmatika, W. Nur'aini, and Y. P. Sagala, "Measurement of Employee Information Security Awareness on Data Security: A Case Study at XYZ Polytechnic," *2022 1st Int. Conf. Inf. Syst. Inf. Technol. ICISIT 2022*, pp. 272–276, 2022, doi: 10.1109/ICISIT54091.2022.9873077.

[7] R. Fadlika, Y. Ruldeviyani, Z. T. Butarbutar, R. A. Istiqomah, and A. A. Fariz, "Employee Information Security Awareness in the Power Generation Sector of PT ABC," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 4, pp. 594–603, 2023, doi: 10.14569/IJACSA.2023.0140465.

[8] Rosihan and A. N. Hidayanto, "Measurement of Employee Information Security Awareness: A Case Study at an Indonesian Correctional Institution," *2022 1st Int. Conf. Inf. Syst. Inf. Technol. ICISIT 2022*, pp. 318–323, 2022, doi: 10.1109/ICISIT54091.2022.9872988.

[9] I. G. A. Sukariana Yasa, I. M. E. Listartha, and I. M. A. Pradnyana, "Measurement of Information Security and Privacy Awareness Using the Multiple Criteria Decision Analysis (Mcda) Method," *J. Tek. Inform.*, vol. 4, no. 4, pp. 759–768, 2023, doi: 10.52436/1.jutif.2023.4.4.692.

[10] X. S. Xu, W. C. H. Hong, K. Kolletar-Zhu, Y. F. Zhang, and C. Y. Chi, "Validation and application of the human aspects of information security questionnaire

for undergraduates: effects of gender, discipline and grade level," *Behav. Inf. Technol.*, pp. 1–22, 2023, doi: 10.1080/0144929X.2023.2260876.

[11] BSN, "SNI ISO/IEC 27001:2013 Standar Nasional Indonesia Badan Standardisasi Nasional," *Online*, 2016. www.bsn.go.id (accessed Dec. 20, 2023).

[12] J. Zhen, K. Dong, Z. Xie, and L. Chen, "Factors Influencing Employees ' Information Security Awareness in the Telework Environment," pp. 1–15, 2022.

[13] 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: 10.1016/j.cose.2006.02.008.

[14] H. Heriyanto, "Thematic Analysis sebagai Metode Menganalisa Data untuk Penelitian Kualitatif," *Anuva*, vol. 2, no. 3, p. 317, 2018, doi: 10.14710/anuva.2.3.317-324.

[15] N. Badie and A. H. Lashkari, "A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP," *J. Basic Appl. Sci. Res.*, vol. 2, no. 9, pp. 9331–9347, 2012.

[16] 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: 10.1016/j.cose.2013.12.003.

[17] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "A study of information security awareness in Australian government organisations," *Inf. Manag. Comput. Secur.*, vol. 22, no. 4, pp. 334–345, 2013, doi: 10.1108/IMCS-10-2013-0078.

[18] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, 2017, doi: 10.1016/j.cose.2017.01.004.

[19] 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," *2022 1st Int. Conf. Softw. Eng. Inf. Technol. ICoSEIT 2022*, pp. 174–179, 2022, doi: 10.1109/ICoSEIT55604.2022.10029989.

[20] J. F. Hair, G. T. Hult, C. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. 2017.

[21] J. F. Hair, G. T. M. Hult, C. M. Ringle, M. Sarstedt, N. P. Danks, and S. Ray, *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R*. Cham: Springer International Publishing, 2021. doi: 10.1007/978-3-030-80519-7.

[22] M. Sarstedt, J. F. Hair, and C. M. Ringle, "'PLS-SEM: indeed a silver bullet'–retrospective observations and recent advances," *J. Mark. Theory Pract.*, vol. 31, no. 3, pp. 261–275, 2023, doi: 10.1080/10696679.2022.2056488.

[23] W. S. Wibowo, D. I. Sensuse, S. Lusa, P. A. Wibowo Putro, and A. Yulfitri, "a Systematic Literature Review on Open Government Data: Challenges and Mapped Solutions," *J. Theor. Appl. Inf. Technol.*, vol. 101, no. 5, pp. 1806–1818, 2023.