Information Security Awareness Raising Strategy Using Fuzzy AHP Method with HAIS-Q and ISO/IEC 27001:2013: A Case Study of XYZ Financial Institution

Yohan Adhi Styoutomo[1]* and Yova Ruldeviyani[2]
[1−2]Master of Information Technology, Faculty of Computer Science, University of Indonesia
Jakarta 10430, Indonesia
Email: [1]yohan.adhi@ui.ac.id, [2]yova@cs.ui.ac.id

***Abstract*—XYZ financial institution is a government institution that receives and processes transaction reports from banks and remittances, so its data classification is very confidential. However, during the Work from Home (WFH) policy in the Covid-19 pandemic, XYZ financial institution has received many spam/phishing attacks. Hence, this incident shows that some employees need an awareness of information security. The research offers a different Information Security Awareness (ISA) questionnaire using the Human Aspects of the Information Security Questionnaire (HAIS-Q) and ISO/IEC 27001:2013 as focus areas. The research uses the theory of Knowledge, Attitude, and Behavior (KAB) to determine the dimensions that need improvement and priority ranking using Fuzzy Analytical Hierarchy Process (FAHP). Furthermore, the research conducts a Focus Group Discussion (FGD) to explore the root causes of employee behavior. The FGD results show that there are still employees who do not know about information security, such as password combinations and length, so limited knowledge affects employees' attitudes and behaviors. The research results from 34 respondents show that the employees' information security awareness level is in the moderate category (78.8%). They still need to increase their awareness of information security, especially in managing passwords, using email and the Internet, and reporting incidents. Recommendations have been prepared to improve the dimensions and areas that have yet to be categorized as good. In the future, the ISA questionnaire is expected to be used in other organizations.**

***Index Terms*—Information Security Awareness, Fuzzy Analytical Hierarchy Process (FAHP), Human Aspects of the Information Security Questionnaire (HAIS-Q), ISO/IEC 27001:2013**

Received: Feb. 23, 2022; received in revised form: June 06, 2022; accepted: July 13, 2022; available online: Sept. 06, 2023.
*Corresponding Author

I. Introduction

TODAY, organizations consider data or information as a strategic asset to be protected from cyber-attacks. During the Covid-19 pandemic, according to a cybersecurity business report, several cybercrimes and data leaks cost more than $6 trillion in 2021 [1]. Therefore, organizations invest heavily in implementing the latest and most advanced technologies to mitigate data leaks [2].

XYZ financial institution is a government agency that manages transaction data from reporting parties and remittances. The data received are analyzed and examined to determine whether there is a possibility of a criminal act occurring from the transaction data [3]. During the Covid-19 pandemic, this institution implements a Work from Home (WFH) policy. From January to March 2021, XYZ financial institution recorded 215 malware attacks with 162 categories of trojans, 42 potentially unwanted programs, 9 viruses, and 2 adware. In addition, XYZ financial institution received 247 spam/phishing emails during the period, and 11 people clicked on the link in the email and opened the attachment. In 2017, XYZ financial institution faced a ransomware attack that directly attacked employees. The Information Technology (IT) division recovered encrypted data for one month, and it disrupted the continuity of the organization's business processes [4]. Therefore, information security awareness needs to be evaluated appropriately. The researchers want to know the extent of Information Security Awareness (ISA) of XYZ financial institution employees.

The phishing and ransomware attacks faced by XYZ financial institution are social engineering. These attacks exploit humans to create vulnerabilities [5]. Facing social engineering attacks requires multidisciplinary handling. So, it is not enough to rely on hardware/software purchases. It requires the human aspect as its leading role [6]. IT incidents are dominated mainly by exploiting human behavior that ignores policies or procedures to resolve work or problems more quickly [7]. In other words, the cause of the error is human behavior itself, intentionally or unintentionally [6]. Employees' compliance with poor policies or procedures triggers data leakage violations [8]. This situation is reinforced by the results of the 2019 ENISA survey, which states that the exploitation of human behavior is the cause of corporate information security breaches [9].

From various perspectives, ISA from employees encourages positive influence in behavior to comply with company security policies [7]. Previous research states that the mishandling of information classification is the cause of the lack of employees' ISA. Furthermore, humans become the weakest link, so ISA becomes research and practice for organizations. The company has made all efforts to educate information security awareness, but the company feels that the vulnerability from insider threats is 90% [6]. Other studies have shown that the current ISA has many areas that have not been mapped in evaluation for further exploration. The failure of the ISA campaign is influenced by not reflecting the factors influencing its success [10].

On the other hand, humans are the most influential element in managing information security [9]. Organizations that promote ISA education do not guarantee that employees behave according to applicable policies or Standard Operating Procedures (SOPs) [2]. Measurements are needed to reflect whether ISA programs are adequate and whether each treatment will be under control [8, 10]. If the organization knows how to prepare and improve the areas of human competence, it will create the most robust chain of security [11]. Top management's commitment and motivation are needed to encourage security awareness so employees can respond well to unexpected events or noncompliance [10]. Before moving on to an improvement program, the organization must evaluate it effectively to know the essence and areas that need improvement [2]. ISA must include at least three essential elements, namely behaviors, attitudes, and knowledge, and the organization should pay attention to these three elements in the evaluation [5].

Several previous studies have measured information security awareness in different case studies. All focus on quantitatively distributing questionnaires with focus areas based on the Human Aspects of Information Security Questionnaire (HAIS-Q) [2, 11–14]. For the limitation of the questionnaire, it does not look at the background of why employees do this personally [6]. Organizations are usually reluctant to find out more about the behavior. So, Focus Group Discussions (FGDs) are carried out to find out the root causes of conduct at the level to answer the gap [10]. By measuring the questionnaire, indications of areas and essential aspects that need to be improved can be seen [10]. FGDs/interviews generate reasons for employee behavior. If organizations can be based on solid reasons they work and behave, they can encourage commitment through concrete actions to improve ISAs [2]. A practical ISA assessment is obtained by understanding personnel behavior [7].

From the previous explanation, security problems are not only a matter of technology but also about knowledge, attitude, and behavior. Therefore, awareness of information security needs to be evaluated appropriately. The researchers want to know employees' information security awareness level in XYZ financial institution. Then, the recommendations are prepared based on the results of the questionnaire and the root causes of the FGD results in each dimension area. For XYZ financial institutions, the measurement results can be used as a benchmark for monitoring indicators, and recommendations can be used to increase information security awareness among employees.

II. Literature Review

A. Human Aspects of the Information Security Questionnaire (HAIS-Q)

A survey with HAIS-Q measures information security awareness and is divided into 7 primary and 21 secondary focus areas. The employee ISA can be considered the organizational basis for performing education and training because it identifies the employees' strengths and shortcomings in each of the focus areas of the ISA [15]. The HAIS-Q focal areas and subregions are broken down into categories, as seen in Table I.

B. ISO/IEC 27001:2013

HAIS-Q has provided a focus area that must be considered in conducting an evaluation [2, 11–14]. However, the focus of this area does not cover all types of social engineering attacks. Therefore, the addition of adaptive control from ISO/IEC 27001:2013 can be done as suggested by previous research [13]. The existence of this additional control assists the organization in making improvements in areas that need improvement [5] since employees can be exposed to social engineering attacks, not just phishing emails [6].

There are several different standards for information security, and one of them is known as ISO/IEC 27001:2013. The organization can reduce the risk of

TABLE I
FOCUS AREAS AND SUB-AREAS OF HUMAN ASPECTS OF INFORMATION SECURITY QUESTIONNAIRE (HAIS-Q).

Focus Area (Code)	Sub-Area (Code)
Password management (A1)	Using the same password (B1) Sharing passwords (B2) Using a strong password (B3)
Email use (A2)	Clicking on links in emails from known senders (B4) Clicking on links in emails from unknown senders (B5) Opening attachments emails from unknown senders (B6)
Internet use (A3)	Downloading files (B7) Accessing dubious websites (B8) Entering information online (B9)
Social media use (A4)	Social media privacy settings (B10) Considering the consequences (B11) Posting about work (B12)
Mobile devices (A5)	Physically securing mobile devices (B13) Sending sensitive information via Wi-Fi (B14) Shoulder surfing (B15)
Information handling (A6)	Disposing of sensitive printouts (B16) Inserting removable media (B17) Leaving sensitive material (B18)
Incident reporting (A7)	Reporting suspicious behavior (B19) Ignoring poor security behavior by colleagues (B20) Reporting all incidents (B21)

TABLE II
PERSONAL RESPONSIBILITY OF ISO/IEC 27001:2013.

ISO/IEC 27001:2013 Clause	ISO/IEC 27001:2013 Category	ISO/IEC 27001:2013 Control
Organization of information security	Mobile devices and teleworking	Mobile devices policy Teleworking
Asset management	Information classification Media handling	Classification of information Management of removable media
Access control	User responsibilities System and application access control	Usage of secret authentication information Secure log-on procedures
Physical and environmental areas	Secured areas	Physical entry controls Working in secure areas
Operations security	Control of operational software	Installation of software on operational systems
Communications security	Security of network services Information transfer	Security of network services Confidentiality or non-disclosure agreement
Information security incident management	Management of information security incidents and improvements	Reporting information security weakness

information leakage through the proper selection of ISO/IEC 27001:2013 controls [16]. The selection of controls aims to reduce risk to a level acceptable to the organization [17]. Among the available controls in ISO/IEC 27001:2013, the measures are the responsibility of individual staff members. The clauses, categories, and controls are outlined in Table II, indicating that employees are required to carry out these controls.

Several clauses in ISO/IEC 27001:2013 in Table II can be eliminated because they have been represented in HAIS-Q. The organization of information security and communication security (mobile device control) clauses in ISO/IEC 27001:2013 have been shown in the HAIS-Q mobile device focus area. Both clauses describe the same scope as HAIS-Q. They focus on user security in securing devices while working in mobility. Moreover, the ISO/IEC 27001:2013 asset management clause has been covered in the information handling focus area of HAIS-Q, and the ISO/IEC 27001:2013 information security incident management clause is also in the HAIS-Q incident handling focus area. Since the scope is the same, it can be deleted because it has already been covered in the HAIS-Q focus area. The deletion results are shown in Table III which lists the clauses and controls from ISO/IEC 27001:2013 used.

TABLE III
FOCUS AREAS AND SUB-AREAS OF ISO/IEC 27001:2013.

Focus Area (Code)	Sub-Area (Code)	ISO/IEC 27001:2013
Access control (A8)	Usage of secret authentication information (B22) Secured log-on procedures (B23)	Annex A.9.3.1 Annex A.9.4.2
Physical and environmental area (A9)	Physical entry controls (B24) Working in secure areas (B25)	Annex A.11.1.2 Annex A.11.1.5
Operations security (A10)	Installation of software on operational systems (B26)	Annex A.12.5.1
Communications security (A11)	Confidentiality or non-disclosure agreement (B27)	Annex A.13.2.4

C. Social Engineering

The term “social engineering attack” refers to a set of manipulation techniques that take advantage of human error to gather sensitive information [18]. A wide range of threats must be covered by an ISA measurement system to reveal the weaknesses of personnel in all areas [19]. Table IV shows the type of social engineering attack mapped to the focus area in the research. It indicates that the attack is already included

TABLE IV
FOCUS AREAS MAPPING WITH SOCIAL ENGINEERING ATTACKS.

Focus Area	Social Engineering Attacks
Password management	Phishing, pretexting, online social engineering
Email use	Phishing, pretexting, baiting, ransomware
Internet use	Phishing, pretexting, baiting, ransomware, pop-up windows, quid pro quo, online social engineering, pharming
Social media use	Pretexting, online social engineering
Mobile devices	Impersonation on the help desk, shoulder surfing
Information handling	Baiting, dumpster diving, stealing an important document
Incident reporting	Reverse social engineering
Access control	Stealing important documents
Physical and environmental area	Tailgating/piggybacking
Operations security	Ransomware, fake software
Communications security	Reverse social engineering, phone/email scams, whaling attack

in all focus areas.

D. Fuzzy Analytical Hierarchy Process (FAHP)

In choosing priorities, several previous studies use Analytical Hierarchy Process (AHP) [2, 11–14]. The AHP was the foundation upon which FAHP was built [20]. Through the use of hierarchies, AHP can reduce complex dilemmas involving decision-making to more manageable forms [21]. However, AHP has drawbacks when selecting alternatives with more than seven points [22]. It also has to maintain the consistency of the ratio below 0.1 with many options, and it has problems with data validity [20]. In addition, subjectivity is a bias in assessing the AHP weights. Regarding alternative therapies, it can be pretty challenging to arrive at a consistent value with the ratio [23]. Therefore, the research uses FAHP to cover the shortcomings of AHP [24]. The value derived from the FAHP can deliver an accuracy level that is very close to that of the conclusion reached by the expert, which is 84.62% [25]. As a result, the FAHP is utilized in the research as a follow-up enhancement from earlier studies.

III. Research Method

The research applies the theoretical framework provided by HAIS-Q (Table I) and ISO/IEC 27001:2013 (Table III). As a result, 11 focus areas and 27 sub-areas have been derived for the research. The hierarchy of dimensions as well as the focus areas are presented in Fig. 1. ISA surveys comprise 27 sub-areas for each dimension, including behavior, attitude, and knowledge.

Figure 2 illustrates the procedures conducted. In the first step, interviews are carried out with three individuals who can validate the focus area, finish the Pairwise Comparison Survey (PCS), and calculate the FAHP. In the second step, the researchers create a questionnaire and conduct a pilot study, which includes ten participants, before sending it out to a larger pool of respondents (34 representatives from each directorate). In the end, the research performs calculations that are validated through FGDs and interviews with the Chief Information Officer (CIO). So, it can provide recommendations to improve the ISA.

A. Research Instruments

Because the company wants ISO/IEC 27001:2013 certification, the interview process is conducted with three experts with experience in phishing emails and ISO/IEC 27001:2013 implementation. These three individuals confirm the XYZ financial institution' needs. In a PCS, three experts describe each dimension's weight and emphasis area.

The researchers create the questionnaire according to the number of sub-areas for each dimension. The scale used is a Likert scale of 1–5. For each category, the dimensions are different. The scale of knowledge is "very not knowledgeable" (scale 1) to "very knowledgeable" (scale 5). In the attitude dimension, the scales are "strongly disagree" (scale 1) to "strongly agree" (scale 5). Meanwhile, the behavior scale is from "never" (scale 1) to "always" (scale 5) [15].

A pilot study is conducted on ten participants to check whether the readability, validity, and reliability tests are accurate. So, it can be disseminated to 34 respondents from each directorate. Results from the completed are subjected to a second round of testing to ensure their validity and reliability [15].

B. Data Collection Procedures

The researchers gather data online because of the Covid-19 pandemic. Additionally, online data storage and processing can be done more quickly. The PCS questionnaire is created using Google Forms. Then, the questionnaire is distributed via electronic mail (e-mail) and WhatsApp. The 34 pre-selected respondents from each directorate are given questionnaires, which are higher than the number of respondents in prior studies [14]. They completed questionnaires from November 1 to November 28, 2021.

C. Data Analyzing Method

The questionnaire results are multiplied by their weight after receiving the weighted value from FAHP processing. In addition, the processed data are classified into three levels: bad, average, and good. Classes of ISA are listed in Table V [26].

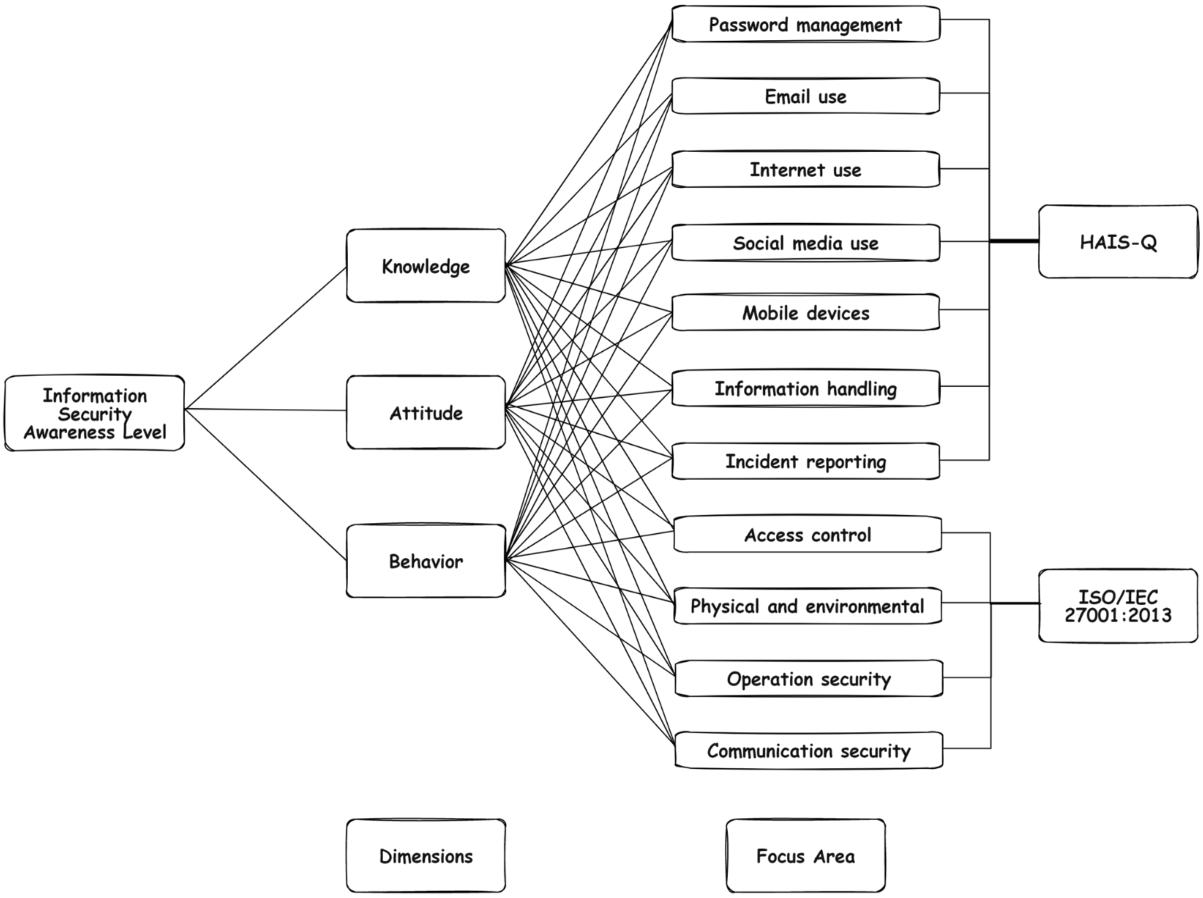

Fig. 1. Theoretical framework.

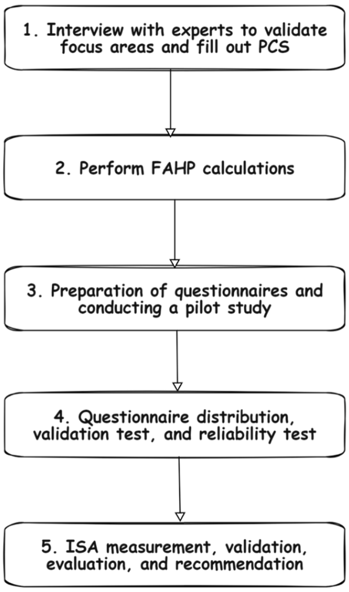
1. Interview with experts to validate focus areas and fill out PCS
2. Perform FAHP calculations
3. Preparation of questionnaires and conducting a pilot study
4. Questionnaire distribution, validation test, and reliability test
5. ISA measurement, validation, evaluation, and recommendation

Fig. 2. Research flow diagram.

TABLE V
SECURITY AWARENESS LEVEL.

Awareness	Measurement (%)	Attribute
Good	80–100	🟩
Average	60–79	🟨
Poor	$\leq$ 59	🟥

D. Validation Process

Using FGD with the five lowest scorers whom the CIO accompanies, the researchers confirm the processing results. The FGD can discover the root cause of the rise in the value of security awareness [2]. As a result, the FGD/interview questions begin with low-value topics. Then, the research can achieve a more in-depth investigation of the level of awareness in attitude and behavior dimensions through FGDs/interviews, which have a higher level of reliability than questionnaires [10].

TABLE VI
RESPONDENTS’ DEMOGRAPHICS.

Variable	Item	Amount	%
Gender	Male	25	73.50
	Female	9	26.50
Age	20–25	1	2.94
	26–30	10	29.41
	31–35	12	35.30
	36–40	10	29.41
	41–45	1	2.94
Education	Undergraduate	27	79.40
	Master	7	20.60

IV. RESULTS AND DISCUSSION

From the results of online data collection with a distribution period from November 1 to 22, 2021, there were 34 respondents from XYZ Financial Institution internal employees filled out questionnaires. Table VI shows the demographics of the respondents. The majority of respondents are dominated by male, aged between 26 and 40 years. Most of them have undergraduate education.

A. Dimension Scale and Focus Area Scale

Because the XYZ financial institution blueprint will implement ISO/IEC 27001:2013, the focus areas and subareas already represent the organization’s needs, according to the results of interviews with internal IT experts at XYZ financial institution. The ISO/IEC 27001:2013 certification of XYZ financial institution, particularly banks, has been obtained by its stakeholders. Stakeholders’ and internal organizations’ demand for data security credibility has prompted XYZ financial institution to implement ISO/IEC 27001:2013. Afterward, the IT specialist completes the PCS and enters it into FAHP for data processing. Processing for the dimensional weights and the focus area weights are shown in Tables VII and VIII, respectively. Table VII shows that three dimensions (knowledge, attitude, and behavior) have equally important values. However, based on experts from FAHP for each focus area shown in Table VIII, it can be seen that five focus areas with the highest weight are password management, email use, information handling, Internet use, and mobile devices. Figures A1– A3 in Appendix are the results of FAHP processing for comparisons between dimensions based on the focus area filled in by the expert. Figure A1 in Appendix on the knowledge dimension, according to the expert, is the most important focus areas (having scores of 8 and 9). It has password management, email use, and Internet use. Then, Fig. A2 in Appendix on the very important attitude dimension is in the focus area, namely the use of email, information handling, access control, and physical and environmental areas. Last, Fig. A3 in Appendix on the behavior dimension is also very important in password management and mobile devices.

TABLE VII
THE RESULTS OF DIMENSION WEIGHT.

Dimension	Weight
Knowledge	0.3333
Attitude	0.3333
Behavior	0.3333

TABLE VIII
FOCUS AREA WEIGHT.

Focus Areas (code)	Weight
Password management (A1)	0.294
Email use (A2)	0.153
Internet use (A3)	0.097
Social media use (A4)	0.025
Mobile devices (A5)	0.085
Information handling (A6)	0.101
Incident reporting (A7)	0.045
Access control (A8)	0.059
Physical and environmental (A9)	0.060
Operations security (A10)	0.043
Communication security (A11)	0.037

B. ISA Questionnaire

ISA questionnaire is put to the readability test by the IT experts in the research. A pilot study is conducted to test the validity of the Pearson method and the reliability of Cronbach’s alpha using SPSS. The results of the pilot study’s questionnaire are given to 34 participants. Table A1 in Appendix contains its results. The question is inverted when marked with an asterisk (*).

C. Validity Test and Reliability Test

Results from 34 respondents are retested using questionnaires that have been distributed online to ensure their validity and reliability. The validity test uses Pearson correlation coefficients for each dimension. The results can be seen in Table IX. Table IX shows that all Pearson values from all focus areas on each dimension are above the r-table value for 34 respondents. The value is 0.3388 (significance level 0.05 for a two-way test). It shows that the results of filling out 34 respondents are valid.

Table X is the result of Cronbach’s alpha processing using the Statistical Package for the Social Sciences (SPSS) application. The purpose of the reliability test is to see how consistent the research results are when they are repeated in the same way. Table X shows that the value of Cronbach’s alpha for 27 questions in

TABLE IX
THE RESULTS OF PEARSON CORRELATION VALUES.

Area	Sub-area	Knowledge	Attitude	Behavior
A1	B1	0.440	0.673	0.644
	B2	0.734	0.588	0.716
	B3	0.703	0.734	0.483
A2	B4	0.443	0.414	0.433
	B5	0.347	0.778	0.401
	B6	0.637	0.769	0.344
A3	B7	0.673	0.519	0.759
	B8	0.375	0.384	0.801
	B9	0.598	0.789	0.654
A4	B10	0.398	0.357	0.640
	B11	0.623	0.796	0.539
	B12	0.571	0.472	0.802
A5	B13	0.579	0.777	0.620
	B14	0.600	0.556	0.792
	B15	0.665	0.525	0.343
A6	B16	0.543	0.354	0.517
	B17	0.401	0.725	0.586
	B18	0.804	0.610	0.548
A7	B19	0.520	0.705	0.494
	B20	0.648	0.821	0.814
	B21	0.631	0.819	0.369
A8	B22	0.549	0.389	0.751
	B23	0.660	0.858	0.706
A9	B24	0.628	0.524	0.395
	B25	0.649	0.723	0.713
A10	B26	0.612	0.785	0.860
A11	B27	0.766	0.777	0.592

Note: password management (A1), email use (A2), Internet use (A3), social media use (A4), mobile devices (A5), information handling (A6), incident reporting (A7), access control (A8), physical and environmental (A9), operations security (A10), and communication security (A11).

TABLE X
THE RESULT OF CRONBACH'S ALPHA.

Dimension	Cronbach's Alpha	Number
Knowledge	0.911	27
Attitude	0.936	27
Behavior	0.929	27

each dimension is above 0.7. Hence, the questionnaire questions are reliable.

D. Results and Validation

Table XI shows the level of ISA measurement in XYZ financial institution. It is 78.8%, meaning that the result is average. The finding shows that ISA in XYZ financial institution's employees needs to be monitored and followed up to improve the current culture. In the knowledge dimension, employees' security awareness levels are already in the high category, despite getting poor results in email and social media use. Meanwhile, the results are in the average category for the dimensions of attitude and behavior. In this case, the value of knowledge (81.5%) is greater, followed by attitude (77.6%) and behavior (77.2%). The attitude and behavior dimensions generally have a lower value than the knowledge dimension. Hence, it can be concluded that good attitudes and behavior do not necessarily accompany good knowledge [27]. Other factors can influence attitudes and behavior, such as personality, organization, or culture [10]. Moreover, the results show that XYZ financial institution's ISA level is still below other institutions, such as the Ministry of Research, Technology, and Higher Education, when viewed from the HAIS-Q focus area (A1-A7) (85.59%) [12]. Similarly, according to HAIS-Q (A1 to A7), XYZ financial institution is average in comparison to the Directorate General of Post and Information Technology (Direktorat Jenderal Sumber Daya dan Perangkat Pos dan Informatika (SDPPI)) in Ministry of Communications and Informatics (78.33%) [14].

TABLE XI
THE RESULTS OF THE INFORMATION SECURITY AWARENESS (ISA) SURVEY.

Focus Area	Knowledge	Attitude	Behavior	Total
Password management	81.0%	79.0%	78.2%	79.4%
Email use	71.0%	77.1%	75.3%	74.4%
Internet use	80.4%	74.1%	70.4%	75.0%
Social media use	79.6%	83.7%	76.3%	80.0%
Mobile devices	83.5%	81.6%	77.8%	81.0%
Information handling	82.5%	77.3%	84.3%	81.4%
Incident reporting	82.7%	77.1%	77.3%	79.0%
Access control	89.1%	74.4%	77.9%	80.5%
Physical and environmental area	90.9%	71.8%	78.5%	80.4%
Operation security	89.4%	81.8%	68.8%	80.0%
Communications security	91.2%	77.6%	81.8%	83.5%
Total	81.5%	77.6%	77.2%	78.8%

The results of the ISA measurement on XYZ financial institution do not follow the organization's character. In contrast, in a government institution that receives and analyzes financial transactions, its employees are expected to have a high level of ISA. Additionally, financial transaction data from banking and remittances received and analyzed include sensitive and confidential data. Similar research in Australia in the banking sector finds that the ISA level for banking employees is 83%–93% for the HAIS-Q focus area (A1-A7) because financial/banking organizations manage confidential information from personal data and transaction data [13]. Therefore, employees in XYZ financial institution must have a level of information security awareness equal to or higher than the financial/banking industry. However, no similar study for the focus area of ISO/IEC 27001:2013 (A8-A11), so the minimum score is equated with research in the banking sector of at least 83% [13].

Then, FGD is conducted on five respondents with low values to discover the cause of the ISA's low value. In managing passwords, respondents know that creating a password must be a combination of uppercase and lowercase letters, numbers, and symbols according to the information in the password receipt for the first time at work. However, the password must be different from their social media or identity, which they do not know yet. Due to many applications at XYZ financial institution and not yet adopting a Single Sign-On (SSO) system, they think that matching passwords on all applications will be easier to remember. Moreover, if a colleague borrows their users and passwords, they do not think that it will be bad for them. Their answers are in line with the previous research in Croatia that a third of the total respondents (28 people) use a bad password combination, which is easy to guess. Moreover, their data are vulnerable in virtual space or social media and easily exploited. It happens because of the habit of equating passwords between social media and applications in organization, so if social media passwords are leaked, application password in organizations can easily be exploited [28].

In using email, when they open the email, they immediately see the contents of the email without verifying the sender or recipient. If they find the content interesting, they will respond by opening the file attached. They do not know how to check whether the sender is valid or not, both internally and externally. Based on previous studies, employees who are easily influenced by gimmicks and their lack of sensitivity become their weak points to be exposed to phishing email attacks. The employees create this behavior because the organizational culture is not well-socialized when they join the company [29].

For Internet usage, they do not know which links or websites to verify when they search through the Internet because, currently, several websites are not verified using Secure Sockets Layer (SSL). When they open a website, if the information provided is interesting, they will use it as a reference, download the related file, or fill in the required information. The human aspect of Internet usage is not just someone who knows whether this site is malicious or not, but they must have a commitment to rejecting any form of cybersecurity risk on the Internet. This commitment makes people obey, and it becomes a habit [30].

For the results of the discussion on social media usage, there are no written rules regarding this matter, so filling out the questionnaire becomes doubtful. For social media configurations, they never check. Usually, the default is from initiating account creation. Even if there is a limit, only friends can see. Studies related to low social media security show that employees do not understand the theoretical or practical consequences of using social media for organizations [31]. Employees' misunderstanding of the unwritten organizational culture makes them think that social media is outside the scope that will affect the company [29].

On mobile devices, they know that they should not leave their laptops carelessly. However, they do not know that working from home must be in a closed condition and room. Moreover, in using Wi-Fi, they already understand the dangers of using public Wi-Fi. Shoulder surfing attacks focus on negligent user behavior to maintain workplace safety [32]. The attitude that tends not to care about the environment makes this attack effective for exploiting user information [33].

In handling information, the discussion results reveal that the respondents already have a clear understanding of how to classify information. However, they leave a few documents on their desks in preparation for the following day's work. Regarding the USB flash drive, it is best to avoid plugging it in and format it immediately if it is still functional. In similar research, information on the desk is the employees' responsibility [34]. It requires support from the organization in the form of policies so that employees behave in line with the organizational culture [35].

In incident reporting, IT issues have been reported to the support team. The action is taken to the violation reporting system in Whistleblowing System (WBS). However, some respondents still do not know how to report to WBS and what kind of reporting is if there are indications of new suspicious actions. Usually, there is no evidence, so it makes them confused about whether to report or not. Reporting the issue provides a dilemma among employees. Therefore, it is necessary to have extra security behavior in voicing the role [36]. Despite no definite evidence, organizations must also support clear policies and procedures for providing a complaint service [37].

On access control, the discussion results show that they have used the internal cloud to exchange information. However, the existing files have not been locked. As a result, providing a link without locking is considered safe enough. For a computer, if it is only left for a short time or closed, it is rarely locked. That is why employee behavior through an authentication process encourages maintaining the confidentiality and integrity of data [38]. Authentication rules are made by the company as the first mover of information can be sent to the right people [27].

The discussion results on the physical and environmental side convey that they have no suspicions when lending ID cards to friends and never pay attention to the people behind who come in. Usually, if there are other people, the security will accompany them. When the manager sets the example by not allowing people into the organizational space, other members of the organization may be more inclined to follow the boss' example in preventing the threat of piggybacking [39]. Through the example of staying alert taught by superiors, the employees can prevent threats of abuse of access and other people who can easily enter the organization (a piggyback attack) [5].

Regarding operational security, the respondents already know which applications are allowed or not. However, it is easier and faster to install the application themselves rather than asking the service team. Some applications are downloaded from the Internet, or other people's reviews make work easier. Hence, the role of ISA cannot be entirely assigned to employees. Several roles are the responsibility of the IT department to encourage these habits [40]. Additionally, application whitelisting needs to be clear so that the IT department can take action if there are applications outside the policy [41].

For communications security, the respondents already know that their work is confidential. However, sometimes for personal data, coworkers give it directly to the person who asks. It sometimes happens from the bank or remittances, and there are obstacles in submitting reports so that the Person in Charge (PIC) contact is quickly given. Confirmation to colleagues or superiors is a guideline that encourages information security [42]. The non-disclosure agreement is a standard for employees to think and act without providing information that can harm the organization [5].

E. Recommendation

Before making recommendations, the research tries to interview the CIO of the ISA success factors with three dimensions, as shown in Table XII. It explains that the CIO is ready to support equating the same understanding of information security through outreach, training, and rules in the form of policies and procedures. Employees with good knowledge are expected to be able to distinguish between attitudes that are allowed and those that are not so that information security attitudes become everyday behavior. Furthermore, the research prepares recommendations for increasing ISAs at XYZ financial institution. Top management's wishes will encourage recommendations aligned with business needs [41].

Although the scores for all focus areas are under banking characteristics (< 90%), the discussion results with the CIO focus on the four priority focus areas according to Table XI, including password management, email usage, Internet usage, and incident reporting. First, for password management, it is recommended to make password security policies, such as using combination passwords. Using the same password with social media can improve information security knowledge and attitudes [43]. Implementing password management technology through Active Directory through group policy can force users to create more complex password combinations [44]. Additionally, two-factor authentication can prevent sharing passwords [45].

TABLE XII
INFORMATION SECURITY AWARENESS (ISA) TARGETS.

Dimensions	Success Factor in Information Security Awareness (ISA)
Knowledge	All employees have the same knowledge through the implementation of training and information security policies or procedures.
Attitude	All employees can take a stand on what must be done to maintain organizational confidentiality.
Behavior	All employees make information security behavior a culture or daily habit.

Second, for email usage, organizations can simulate phishing attacks periodically. Simulations can encourage employees to behave more consistently according to organizational culture [46]. Third, XYZ financial institution can increase Internet usage awareness by implementing application and browser controls to protect users from harmful websites and devices from malicious applications, files, and downloads [47]. For example, the organization can use SecureWeb. It is a web browser extension with a security token. It can protect users' passwords and provide protection solutions for sensitive data. It also includes encryption and decryption on local users' computers to control security on their browsers [48].

Fourth, reporting incidents to increase ISA can be done through dialogue activities or discussions between employees. Employees can explain their incidents and experiences to other employees who will work to implement positive safety behaviors. Group discussions will also become more interactive and attention-grabbing to encourage more consistent incident reporting [37]. Last, there can be a creation of review and periodic review of all policies and procedures for all focus areas, covering password management, email usage, Internet usage, social media usage, mobile devices, information handling, incident reporting, access control, physical and environmental areas, operations security, communications security [49].

V. CONCLUSION

During WFH, there are phishing email attacks on 11 employees in XYZ financial institution. These phishing email attacks include social engineering attacks that exploit human vulnerabilities. However, ISA education does not guarantee that employees behave by applicable policies or SOPs. Measurements are needed to reflect whether the ISA program is adequate and the treatment will be controlled.

Measurement of ISA at XYZ financial institutions uses three dimensions (knowledge, attitude, and behavior) with HAIS-Q and ISO/IEC 27001:2013 as controls. The data are processed using FAHP. The results show that the ISA is 78.8% (average) with knowledge (81.5% - good), attitude (77.6% - average), and behavior (77.2% - average). Attitude and behavior dimensions below 80% are employee dimensions that need improvement. Meanwhile, the focus areas that need improvement are password management, email usage, Internet usage, and incident reporting at XYZ financial institution.

Moreover, based on the research results, several things are recommended. Information awareness in the password management area can be increased through password policies, password management, and two-factor authentication. Meanwhile, periodic phishing email simulations can be carried out in email usage. At the same time, in Internet use, XYZ financial institution can implement application and browser controls to prevent access to dangerous websites, applications, files, and downloads and use token based SecureWeb. Last, incident reporting is carried out through discussions between employees to share experiences related to information security so that the discussion will encourage employees' awareness in reporting incidents or other improvements.

The research focuses on the measurement of ISA and has a limitation in terms of the number of interviewees as it only includes the lowest scorers and not all respondents. Additionally, other methods, such as role-playing games or simulations based on the guidelines provided by the National Institute of Standards and Technology (NIST) can be explored to enhance the effectiveness of information security training and awareness programs. These alternative approaches may provide valuable insights into improving employees' knowledge, attitudes, and behaviors regarding information security within the organization.

References

[1] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Computers & Security*, vol. 106, pp. 1–22, 2021.

[2] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and information security awareness," *Computers & Security*, vol. 88, pp. 1–8, 2020.

[3] Australian Government, *Anti-money laundering and counter-terrorism financing act 2006*. Attorney-General's Department, 2021.

[4] M. Alawida, A. E. Omolara, O. I. Abiodun, and M. Al-Rajab, "A deeper look into cybersecurity issues in the wake of Covid-19: A survey," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 8176–8206, 2022.

[5] T. Grassegger and D. Nedbal, "The role of employees' information security awareness on the intention to resist social engineering," *Procedia Computer Science*, vol. 181, pp. 59–66, 2021.

[6] H. Aldawood, T. Alashoor, and G. Skinner, "Does awareness of social engineering make employees more secure?" *International Journal of Computer Applications*, vol. 177, no. 38, pp. 45–49, 2020.

[7] M. Thangavelu, V. Krishnaswamy, and M. Sharma, "Impact of comprehensive information security awareness and cognitive characteristics on security incident management–An empirical study," *Computers & Security*, vol. 109, 2021.

[8] R. Torten, C. Reaiche, and S. Boyle, "The impact of security awareness on information technology professionals' behavior," *Computers & Security*, vol. 79, pp. 68–79, 2018.

[9] L. Hadlington, J. Binder, and N. Stanulewicz, "Exploring role of moral disengagement and counterproductive work behaviours in information security awareness," *Computers in Human Behavior*, vol. 114, 2021.

[10] G. Assenza, A. Chittaro, M. C. De Maggio, M. Mastrapasqua, and R. Setola, "A review of methods for evaluating security awareness initiatives," *European Journal for Security Research*, vol. 5, pp. 259–287, 2020.

[11] A. Solomon, M. Michaelshvili, R. Bitton, B. Shapira, L. Rokach, R. Puzis, and A. Shabtai, "Contextual security awareness: A context-based approach for assessing the security awareness of users," *Knowledge-Based Systems*, vol. 246, 2022.

[12] D. D. H. Wahyudiwan, Y. G. Sucahyo, and A. Gandhi, "Information security awareness level measurement for employee: Case study at Ministry of Research, Technology, and Higher Education," in *2017 3rd International Conference on Science in Information Technology (ICSITech)*. Bandung, Indonesia: IEEE, Oct. 25–26, 2017, pp.

654–658.

[13] M. Pattinson, M. Butavicius, K. Parsons, A. McCormac, and D. Calic, “Managing information security awareness at an australian bank: A comparative study,” *Information & Computer Security*, vol. 25, no. 2, pp. 181–189, 2017.

[14] 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)*. Palembang, Indonesia: IEEE, Oct. 17–18, 2018, pp. 1–6.

[15] 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,” *Computers & Security*, vol. 66, pp. 40–51, 2017.

[16] R. Tatiara, A. N. Fajar, B. Siregar, and W. Gunawan, “Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001,” *Journal of Physics: Conference Series*, vol. 978, pp. 1–6, 2018.

[17] A. Firdani, S. Suprapto, and A. R. Perdanakusuma, “Perencanaan pengelolaan keamanan informasi berbasis ISO 27001 menggunakan Indeks KAMI studi kasus: Dinas Komunikasi dan Informatika Kabupaten Rembang,” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no. 6, pp. 6009–6015, 2019.

[18] H. Aldawood and G. Skinner, “Educating and raising awareness on cyber security social engineering: A literature review,” in *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*. Wollongong, NSW, Australia: IEEE, Dec. 4–7, 2018, pp. 62–68.

[19] F. Salahdine and N. Kaabouch, “Social engineering attacks: A survey,” *Future Internet*, vol. 11, no. 4, pp. 1–17, 2019.

[20] A. Gnanavelbabu and P. Arunagiri, “Ranking of MUDA using AHP and Fuzzy AHP algorithm,” *Materials Today: Proceedings*, vol. 5, no. 5, pp. 13 406–13 412, 2018.

[21] R. Octavianus and P. Mursanto, “The analysis of critical success factor ranking for software development and implementation project using AHP,” in *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*. Yogyakarta, Indonesia: IEEE, Oct. 27–28, 2018, pp. 313–318.

[22] W. Yusnaeni, M. Marlina, R. Y. Hayuningtyas, and R. Sari, “Comparison AHP-MABAC And WASPAS methods for supplier recommendations,” *Jurnal Teknik Komputer AMIK BSI*, vol. 7, no. 2, pp. 145–150, 2021.

[23] T. K. Biswas and M. C. Das, “Selection of commercially available electric vehicle using fuzzy AHP-MABAC,” *Journal of The Institution of Engineers (India): Series C*, vol. 100, pp. 531–537, 2019.

[24] D. Bozanic, D. Tešić, and J. Milićević, “A hybrid fuzzy AHP-MABAC model: Application in the Serbian Army–The selection of the location for deep wading as a technique of crossing the river by tanks,” *Decision Making: Applications in Management and Engineering*, vol. 1, no. 1, pp. 143–164, 2018.

[25] Q. Setyani, R. Andreswari, and M. A. Hasibuan, “Target analysis of students based on academic data record using method Fuzzy Analytical Hierarchy Process (FAHP) case study: Study program Information Systems Telkom University,” in *2018 6th International Conference on Cyber and IT Service Management (CITSM)*. Parapat, Indonesia: IEEE, Aug. 7–9, 2018, pp. 1–6.

[26] Y. Normandia, L. Kumaralalita, A. N. Hidayanto, W. S. Nugroho, and M. R. Shihab, “Measurement of employee information security awareness using Analytic Hierarchy Process (AHP): A case study of Foreign Affairs Ministry,” in *2018 International Conference on Computing, Engineering, and Design (ICCED)*. Bangkok, Thailand: IEEE, Sept. 6–8, 2018, pp. 52–56.

[27] M. Sas, G. Reniers, K. Ponnet, and W. Hardyns, “The impact of training sessions on physical security awareness: Measuring employees’ knowledge, attitude and self-reported behaviour,” *Safety Science*, vol. 144, 2021.

[28] L. Luic, D. Svelec-Juricic, and P. Misevic, “The impact of knowledge of the issue of identification and authentication on the information security of adolescents in the virtual space,” *WSEAS Transactions on Systems and Control*, vol. 16, pp. 527–533, 2021.

[29] R. AlMindeel and J. T. Martins, “Information security awareness in a developing country context: Insights from the government sector in Saudi Arabia,” *Information Technology & People*, vol. 34, no. 2, pp. 770–788, 2021.

[30] H. Stewart and J. Jürjens, “Information security management and the human aspect in organizations,” *Information & Computer Security*, vol. 25, no. 5, pp. 494–534, 2017.

[31] M. Alsulami, “Social media security awareness in Saudi Arabia,” *Tehnički glasnik*, vol. 16, no. 2, pp. 213–218, 2022.

[32] L. Zhou, K. Wang, J. Lai, and D. Zhang, “Behaviors of unwarranted password identification via shoulder-surfing during mobile authentication,” in *2021 IEEE International Conference on Intelligence and Security Informatics (ISI)*. San Antonio, TX, USA: IEEE, Nov. 2–3, 2021, pp. 1–3.

[33] L. Bošnjak and B. Brumen, “Shoulder surfing experiments: A systematic literature review,” *Computers & Security*, vol. 99, pp. 1–34, 2020.

[34] M. Al Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, “Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency,” *Procedia Computer Science*, vol. 161, pp. 1206–1215, 2019.

[35] H. Aldawood and G. Skinner, “Contemporary cyber security social engineering solutions, measures, policies, tools and applications: A critical appraisal,” *International Journal of Security (IJS)*, vol. 10, no. 1, pp. 1–15, 2019.

[36] L. Jaeger and A. Eckhardt, “When colleagues fail: Examining the role of information security awareness on extra-role security behaviors,” 2018. [Online]. Available: https://aisel.aisnet.org/ecis2018_rp/124

[37] F. G. Alotaibi, N. Clarke, and S. M. Furnell, “A novel approach for improving information security management and awareness for home environments,” *Information & Computer Security*, vol. 29, no. 1, pp. 25–48, 2020.

[38] L. Hadlington and S. Chivers, “Segmentation analysis of susceptibility to cybercrime: Exploring individual differences in information security awareness and personality factors,” *Policing: A Journal of Policy and Practice*, vol. 14, no. 2, pp. 479–492, 2020.

[39] M. Sas, K. Ponnet, G. Reniers, and W. Hardyns, “Assigning roles for campus security awareness,” 2021. [Online]. Available: https://biblio.ugent.be/publication/8741653/file/8741654

[40] M. M. Al-Daeef, N. Basir, and M. M. Saudi, “Security awareness training: A review,” in *Proceedings of the World Congress on Engineering 2017*, London, U.K., July 5–7, 2017.

[41] I. Hwang, R. Wakefield, S. Kim, and T. Kim, “Security awareness: The first step in information security compliance behavior,” *Journal of Computer Information Systems*, vol. 61, no. 4, pp. 345–356, 2021.

[42] D. Popescul, “Information security awareness in contemporary organizations–Challenges and solutions,” *Security & Future*, vol. 2, no. 3, pp. 134–137, 2018.

[43] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, “Information security governance challenges and critical success factors: Systematic review,” *Computers & Security*, vol. 99, 2020.

[44] M. Yıldırım and I. Mackie, “Encouraging users to improve password security and memorability,” *International Journal of Information Security*, vol. 18, pp. 741–759, 2019.

[45] Q. Xie and L. Hwang, “Security enhancement of an anonymous roaming authentication scheme with two-factor security in smart city,” *Neurocomputing*, vol. 347, pp. 131–138, 2019.

[46] H. Aldawood and G. Skinner, “Reviewing cyber security social engineering training and awareness programs–Pitfalls and ongoing issues,” *Future Internet*, vol. 11, no. 3, pp. 1–16, 2019.

[47] Microsoft, “App & browser control in Windows Security.” [Online]. Available: https://shorturl.at/gmowY

[48] S. Liang, Y. Zhang, B. Li, X. Guo, C. Jia, and Z. Liu, “Secureweb: Protecting sensitive information through the web browser extension with a security token,” *Tsinghua Science and Technology*, vol. 23, no. 5, pp. 526–538, 2018.

[49] D. Snyman and H. Kruger, “The application of behavioural thresholds to analyse collective behaviour in information security,” *Information and Computer Security*, vol. 25, no. 2, pp. 152–164, 2017.

Appendix

The Appendice can be seen in the next page.

TABLE A1
ISA QUESTIONNAIRE.

	Knowledge	Attitude	Behavior
Focus area: Password management			
B1	Passwords on social media account with work account passwords are allowed to be the same. *	It is safe to use the same password for social media and work accounts. *	I use different passwords for social media and work accounts.
B2	I can share work account passwords with coworkers. *	I do not share work account passwords with coworkers or family.	I share work account passwords with trusted people, such as coworkers or family. *
B3	A good password has a minimum length of eight letters and a combination of letters, numbers, and symbols.	In creating a working password, it is enough only to use letters. *	I combine letters, numbers, and symbols on personal computers or office applications.
Focus area: Email use			
B4	Employees can click on unknown/dangerous links in emails from people they know. *	It is always safe to click links in emails from people I know. *	I always do not click links in emails, even if it is sent from people I know.
B5	Employees are not allowed to click links in emails from unknown senders.	It is okay to click on an email link from an unknown sender. *	If an email from an unknown sender looks appealing, I click the link in it. *
B6	Employees are allowed to open malicious emails from unknown senders. *	There is a risk of opening malicious email attachments from unknown senders.	I do not open emails if I do not know the sender.
Focus area: Internet use			
B7	Employees allow to download malicious files into computers if it helps in work. *	It can be risky to download malicious files on a work computer from unknown sites.	I download files to my work computer because it helps to get work done. *
B8	While employees are at work, employees must not access malicious websites.	I can access any website at work, but it does not mean the website accessed is safe.	When accessing the Internet at work, I visit the website I want. *
B9	Employees enter information on many websites if it helps the job. *	If it helps with work, entering information on a specific site is fine. *	I ensure the security of the website before I enter personal information data.
Focus area: Social media use			
B10	Periodically, employees evaluate the privacy settings on social media accounts to avoid accounts being hacked.	It is a good idea to review social media privacy settings regularly.	I do not review social media privacy settings regularly. *
B11	The employee is not to blame for something he/she posts on social media. *	It does not matter if I post on social media, which I usually do not say in public. *	I do not post anything on social media before considering the negative consequences.
B12	I can post what I want about work on social media. *	There is a considerable risk of posting information about work on social media.	I post whatever I want about work on social media, even if it is confidential. *
Focus area: Mobile devices			
B13	Employees must take care of the office laptop when working in public places.	When working in a public place with an office laptop, I feel safe leaving my laptop behind. *	When working in public, I always leave my laptop unattended. *
B14	Employees can send sensitive (restricted/confidential) work files over public WIFI networks.	In my opinion, it is risky to send sensitive work files using a WIFI network.	I send sensitive work files using a public WIFI network that everyone can access. *
B15	When working on sensitive documents, I make sure others cannot see the laptop screen. *	It is risky to access sensitive work files on the laptop if others can see my work.	I make sure other people cannot see the laptop screen if I work on confidential documents.
Focus area: Information handling			
B16	Documents that are confidential/restricted can be disposed of in the same way as those that are open/non-confidential. *	Confidential/restricted documents can be directly thrown in the trash. *	When sensitive documents need to be disposed of, I ensure that they are destroyed.
B17	If I find a USB flash drive in a public place, I should not plug it into my work computer.	If I find a USB flash drive in a public place, it is okay to plug it into a work computer. *	I would not plug a USB flash drive found in a public place into my work computer.
B18	Employees can leave documents containing sensitive information on their desks/cubicles. *	There is a risk of leaving documents containing sensitive information on the desk.	I leave a document containing sensitive information on my desk to work on the next day. *

	Knowledge	Attitude	Behavior
Focus area: Incident reporting			
B19	If I see someone acting suspiciously at my workplace, I must report it.	It is okay to ignore someone suspicious at my workplace. *	If I see someone acting suspiciously at work, I will report it to security.
B20	I must not ignore the data leaking behavior of my coworkers.	There is nothing wrong with ignoring the behavior of a coworker who leaks data. *	If I see a colleague ignoring information security rules, I do not report it. *
B21	I do not need to report an information security leak incident. *	I will ignore it if it does not significantly impact data leakage. *	There is a high risk of addressing information security leaks, although the impact is negligible.
Focus area: Access control			
B22	The secret file is passworded before being sent using email or other official media.	I send sensitive files via the cloud with no password on secret files. *	I send confidential work files using Google Drive outside of office facilities. *
B23	The work computer is not locked. If it is not used or left, there is a need.	I do not lock my computer if I stay a little longer. *	I lock my computer when I stay, even if it is the other way around.
Focus area: Physical and environmental			
B24	Employees enter the office using ID cards and ensure no one else is behind.	If someone forgets to bring it, I lend my ID card to my friends/others. *	I report to security that I forget to bring my ID card.
B25	Employees are not allowed to receive guests at the desk.	I have guests at my desk. *	I often receive guests at my desk. *
Focus area: Operations security			
B26	Office computers can only install licensed applications for office use.	I can install any application on my work computer. *	I install applications that I download from the Internet in addition to office applications. *
Focus area: Communications security			
B27	Employees are not allowed to provide work-related information without the supervisor’s approval or other employees’ personal information.	If someone else asks for work-related information, I will immediately provide that information. *	I will seek approval from my supervisor to provide work-related information.

ISA	A1			A2			A3			A4			A5			A6			A7			A8			A9			A10			A11		
A1	1	1	1	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8
A2	0.13	0.14	0.17	1	1	1	6	7	8	8	9	9	6	7	8	8	9	9	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8
A3	0.13	0.14	0.17	0.13	0.14	0.17	1	1	1	6	7	8	6	7	8	6	7	8	4	5	6	4	5	6	6	7	8	6	7	8	4	5	6
A4	0.13	0.14	0.17	0.11	0.11	0.13	0.13	0.14	0.17	1	1	1	6	7	8	4	5	6	6	7	8	4	5	6	0.25	0.33	0.5	0.25	0.33	0.5	1	1	1
A5	0.13	0.14	0.17	0.13	0.14	0.17	0.13	0.14	0.17	0.13	0.14	0.17	1	1	1	2	3	4	0.25	0.33	0.5	2	3	4	1	1	1	2	3	4	4	5	6
A6	0.13	0.14	0.17	0.11	0.11	0.13	0.13	0.14	0.17	0.17	0.2	0.25	0.25	0.33	0.5	1	1	1	4	5	6	2	3	4	4	5	6	2	3	4	4	5	6
A7	0.13	0.14	0.17	0.13	0.14	0.17	0.17	0.2	0.25	0.13	0.14	0.17	2	3	4	0.17	0.2	0.25	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
A8	0.13	0.14	0.17	0.13	0.14	0.17	0.17	0.2	0.25	0.17	0.2	0.25	0.25	0.33	0.5	0.25	0.33	0.5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
A9	0.13	0.14	0.17	0.13	0.14	0.17	0.13	0.14	0.17	2	3	4	1	1	1	0.17	0.2	0.25	1	1	1	1	1	1	1	1	1	4	5	6	2	3	4
A10	0.13	0.14	0.17	0.13	0.14	0.17	0.13	0.14	0.17	2	3	4	0.25	0.33	0.5	0.25	0.33	0.5	1	1	1	1	1	1	0.17	0.2	0.25	1	1	1	4	5	6
A11	0.13	0.14	0.17	0.13	0.14	0.17	0.17	0.2	0.25	1	1	1	0.17	0.2	0.25	0.17	0.2	0.25	1	1	1	1	1	1	0.25	0.33	0.5	0.17	0.2	0.25	1	1	1

Fig. A1. Knowledge dimension of Fuzzy Analytical Hierarchy Process (FAHP) Data.

ISA	A1			A2			A3			A4			A5			A6			A7			A8			A9			A10			A11		
A1	1	1	1	4	5	6	2	3	4	4	5	6	4	5	6	2	3	4	4	5	6	6	7	8	4	5	6	2	3	4	4	5	6
A2	0.17	0.2	0.25	1	1	1	6	7	8	4	5	6	6	7	8	4	5	6	4	5	6	2	3	4	2	3	4	4	5	6	6	7	8
A3	0.25	0.33	0.5	0.13	0.14	0.17	1	1	1	4	5	6	2	3	4	2	3	4	4	5	6	2	3	4	0.25	0.33	0.5	1	1	1	2	3	4
A4	0.17	0.2	0.25	0.17	0.2	0.25	0.17	0.2	0.25	1	1	1	0.13	0.14	0.17	0.11	0.11	0.13	0.13	0.14	0.17	0.11	0.11	0.13	0.13	0.14	0.17	0.17	0.2	0.25	0.13	0.14	0.17
A5	0.17	0.2	0.25	0.13	0.14	0.17	0.25	0.33	0.5	6	7	8	1	1	1	0.13	0.14	0.17	0.11	0.11	0.13	0.13	0.14	0.17	0.17	0.2	0.25	0.13	0.14	0.17	0.11	0.11	0.13
A6	0.25	0.33	0.5	0.17	0.2	0.25	0.25	0.33	0.5	8	9	9	6	7	8	1	1	1	6	7	8	4	5	6	6	7	8	4	5	6	2	3	4
A7	0.17	0.2	0.25	0.17	0.2	0.25	0.17	0.2	0.25	6	7	8	8	9	9	0.13	0.14	0.17	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
A8	0.13	0.14	0.17	0.25	0.33	0.5	0.25	0.33	0.5	8	9	9	6	7	8	0.17	0.2	0.25	1	1	1	1	1	1	8	9	9	6	7	8	4	5	6
A9	0.17	0.2	0.25	0.25	0.33	0.5	2	3	4	6	7	8	4	5	6	0.13	0.14	0.17	1	1	1	0.11	0.11	0.13	1	1	1	6	7	8	6	7	8
A10	0.25	0.33	0.5	0.17	0.2	0.25	1	1	1	4	5	6	6	7	8	0.17	0.2	0.25	1	1	1	0.13	0.14	0.17	0.13	0.14	0.17	1	1	1	6	7	8
A11	0.17	0.2	0.25	0.13	0.14	0.17	0.25	0.33	0.5	6	7	8	8	9	9	0.25	0.33	0.5	1	1	1	0.17	0.2	0.25	0.13	0.14	0.17	0.13	0.14	0.17	1	1	1

Fig. A2. Attitude dimension of Fuzzy Analytical Hierarchy Process (FAHP) data.

ISA	**A1**			**A2**			**A3**			**A4**			**A5**			**A6**			**A7**			**A8**			**A9**			**A10**			**A11**		
A1	1	1	1	6	7	8	4	5	6	6	7	8	6	7	8	4	5	6	6	7	8	4	5	6	4	5	6	6	7	8	4	5	6
A2	0.13	0.14	0.17	1	1	1	0.17	0.2	0.25	4	5	6	0.13	0.14	0.17	0.17	0.2	0.25	0.25	0.33	0.5	0.13	0.14	0.17	0.13	0.14	0.17	0.17	0.2	0.25	0.13	0.14	0.17
A3	0.17	0.2	0.25	4	5	6	1	1	1	8	9	9	1	1	1	0.17	0.2	0.25	0.17	0.2	0.25	1	1	1	1	1	1	2	3	4	0.25	0.33	0.5
A4	0.13	0.14	0.17	0.17	0.2	0.25	0.11	0.11	0.13	1	1	1	0.17	0.2	0.25	0.13	0.14	0.17	0.17	0.2	0.25	0.13	0.14	0.17	0.17	0.2	0.25	0.13	0.14	0.17	0.13	0.14	0.17
A5	0.13	0.14	0.17	6	7	8	1	1	1	4	5	6	1	1	1	6	7	8	4	5	6	6	7	8	4	5	6	6	7	8	8	9	9
A6	0.17	0.2	0.25	4	5	6	4	5	6	6	7	8	0.13	0.14	0.17	1	1	1	4	5	6	4	5	6	2	3	4	2	3	4	1	1	1
A7	0.13	0.14	0.17	2	3	4	4	5	6	4	5	6	0.17	0.2	0.25	0.17	0.2	0.25	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
A8	0.17	0.2	0.25	6	7	8	1	1	1	6	7	8	0.13	0.14	0.17	0.17	0.2	0.25	1	1	1	1	1	1	1	1	1	1	1	1	2	3	4
A9	0.17	0.2	0.25	6	7	8	1	1	1	4	5	6	0.17	0.2	0.25	0.25	0.33	0.5	1	1	1	1	1	1	1	1	1	1	1	1	2	3	4
A10	0.13	0.14	0.17	4	5	6	0.25	0.33	0.5	6	7	8	0.13	0.14	0.17	0.25	0.33	0.5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
A11	0.17	0.2	0.25	6	7	8	2	3	4	6	7	8	0.11	0.11	0.13	1	1	1	1	1	1	0.25	0.33	0.5	0.25	0.33	0.5	1	1	1	1	1	1

Fig. A3. Behavior dimension of Fuzzy Analytical Hierarchy Process (FAHP) data.