CHAPTER 4

UNINTENTIONAL INSIDER THREATS COUNTERMEASURE MODEL (UITCM) DEVELOPMENT

4.1 Introduction

To achieve the objectives of this study, this chapter discussed the development of UITCM which was developed based on several steps. The initial version of the model was developed based on the literature review results of the existing countermeasures. The development of the model takes into consideration all important elements that have been suggested in previous countermeasure models.

In order to improve the model, the second version of UITCM was developed. A survey was conducted towards IT Executives of Malaysian SMEs, to identify factors and likelihood of UITs in Malaysian SMEs. In this chapter, survey analysis and findings were described. The survey focuses on the likelihood of UITs and contributing factors of UITs in Malaysia SMEs. The pilot study was used to validate the appropriateness of the questions for the survey. The proposed model in this study gone through a two-stage validation process, the first one is investigation through literatures and existing models analysis and the second stage is through two rounds of Delphi technique. The final version of the model that was proposed after series of validation is described in this chapter.

4.2 Development Process of UIT Countermeasure Model (UITCM)

In order to develop the UITCM, the development process was conducted in three steps as following:

- Step 1: Development of initial version of UITCM.

• Step 2: Development of second version of UITCM.

• Step 3: Development of final version UITCM.

Summary of the development activities is shown in Figure 4.1.

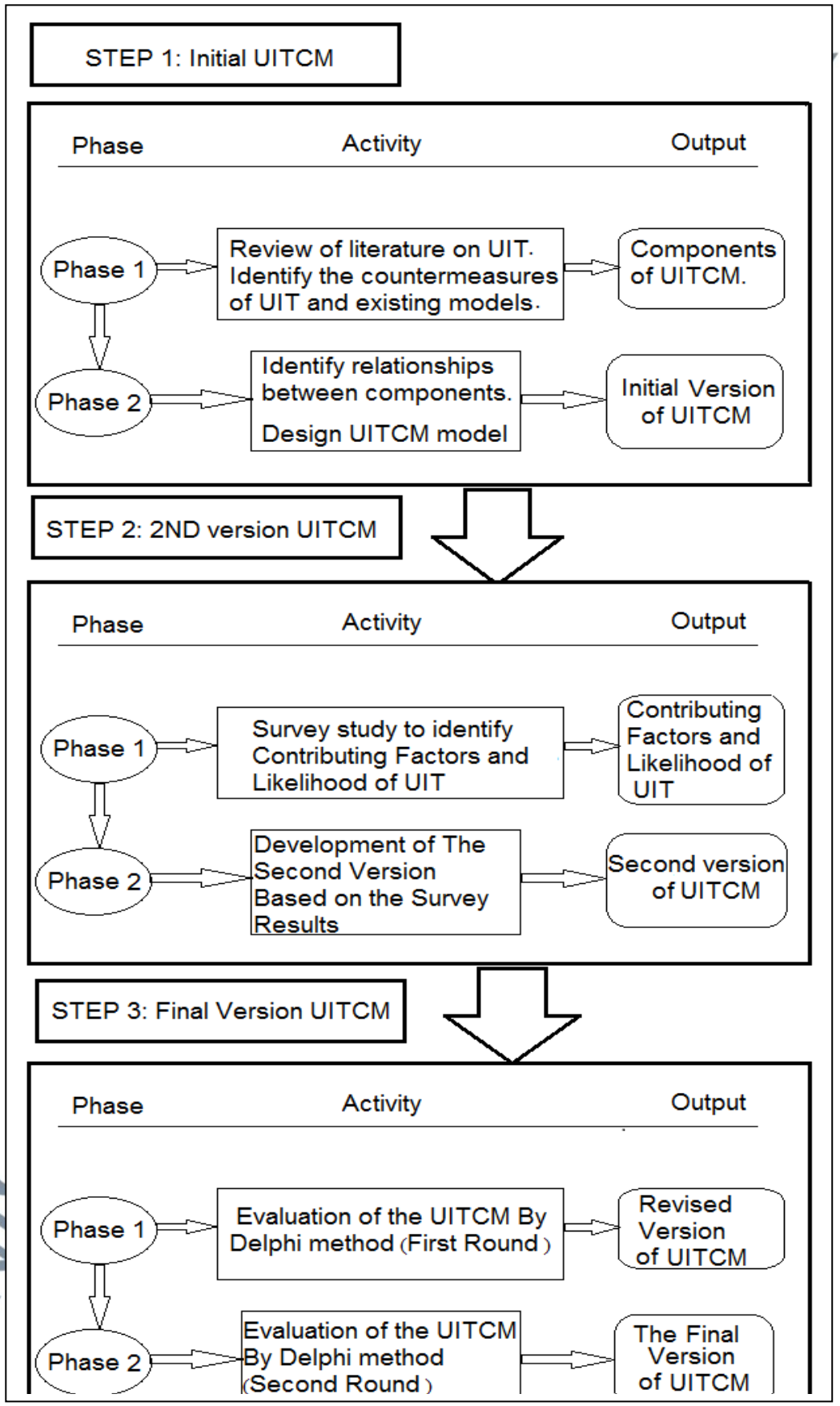

Figure 4. 1: Summary of Activity

4.3 Step 1: Development of Initial Version of UITCM

Table 4.1 shows the Table 4.1 shows the development activities of the initial version. In this table, the development of initial UITCM was carried out in two phases:

- Phase 1: Identification of the model components.
- Phase 2: Development of initial version of UITCM.

The activities conducted in the first phase include literature review on countermeasures approaches, strategies, techniques and tools and analysing existing models of UITs.

In the second phase, the development was based on the model's components that were identified in Phase 1. Prior to proposing the conceptual model of UIT countermeasures, a comparative analysis of the existing models and countermeasures was performed to ensure that there is no repetition and to ensure that all aspects and areas are covered. Then, UITCM model components were divided on the basis that UIT Countermeasures should include three main domains namely organisational aspects, human factor's aspects, in addition to automated defence tools. Subsequently, relationships that hold between components have then been identified and initial version of the model was proposed. The proposed initial version of UITCM is shown in Figure 4.2. Table 4.2 shows the references of where all the components have been derived in developing the conceptual model of UITCM.

Table 4. 1: (UITCM) / Initial Version development activities

Input	Existing countermeasures of UITs
Process	Phase 1: identification of the model components. Phase 2: model development.
Output	Initial Version of UIT Countermeasure Model (UITCM)

Table 4. 2: List of References for UITCM Components

UITCM Components	Reference
•Law &regulation, policy enforcement, Procedure,	• Generic Mitigation Strategies for

standard, best practise, baseline. •Improve data flow. • Risk analysis, Auditing. • Security education, Training, awareness • IDS, accesses control, data classification, APT prevention, IAM, EDR, UEBA, CCTV, RFID. • Data encryption. • Watermarking forensic, intelligence operation.	Information Leaks (Wan, 2019).
•Maintain employee readiness. • Effective security practices. • Maintain staff values. • Improve work planning and control • Improve work setting • Usability of software /security tools. • Remote memory wipe for lost equipment. • software to recognize bogus emails Standard systems (antivirus, anti-malware, DLP, firewalls.	• UIT Mitigation Strategies and Countermeasures (Greitzer et al., 2014).
• Improve design of user-system interfaces. • Affordable access to mental health/drug treatment services. • Appropriate time off for employees. • Team-building activities to enhance mood. • Incident-driven reviews (policies, practices, training materials). • Periodically, fully re-evaluate risk. • Password protection. • Wireless and Bluetooth safeguards. • Email safeguards (anti-phishing, anti-malware), • Security information event management (SIEM). • Anti-malware, intrusion detection and prevention system (IDS/IPS).	• Unintentional insider threats: A foundational study (CER, 2013).
• Trust model.	• (Schneier ,2004)
• Instrumental conditioning	• (Gonzalez & Sawicka ,2002)
• Improve design of work environment	• (HSE,1999;Wood & Banks, 1993;Bratus et al., 2008;Kerm et

	al,2007;Jeffrey et al.,2002; Mansor et al., 2011;Murphy et al., 1986)
• Automation.	• (Carstens et al.,2004;Edwards et al ,2007;Gonzales & Sawicka 2002;Rupere et al,2012).
• Standard Operating Procedure.	• (Rupere et al, 2012).
• Backup systems (Spatial /Temporal) Replication.	• (Brown, 2004).
• Stimulation of risk perception.	• (Trcˇek & Kandus, 2003).
• Collaborative Reinforcement Model.	• (Saha & Misra, 2009).

The model was formulated on the basis that UIT Countermeasures includes organisational aspects, human factor's aspects, in addition to automated defence tools. The proposed components in the Initial UIT Countermeasure Model (UITCM) are pictured in (Appendix A) tables 1, 2 and 3 with the explanation of the countermeasures items in each domain.

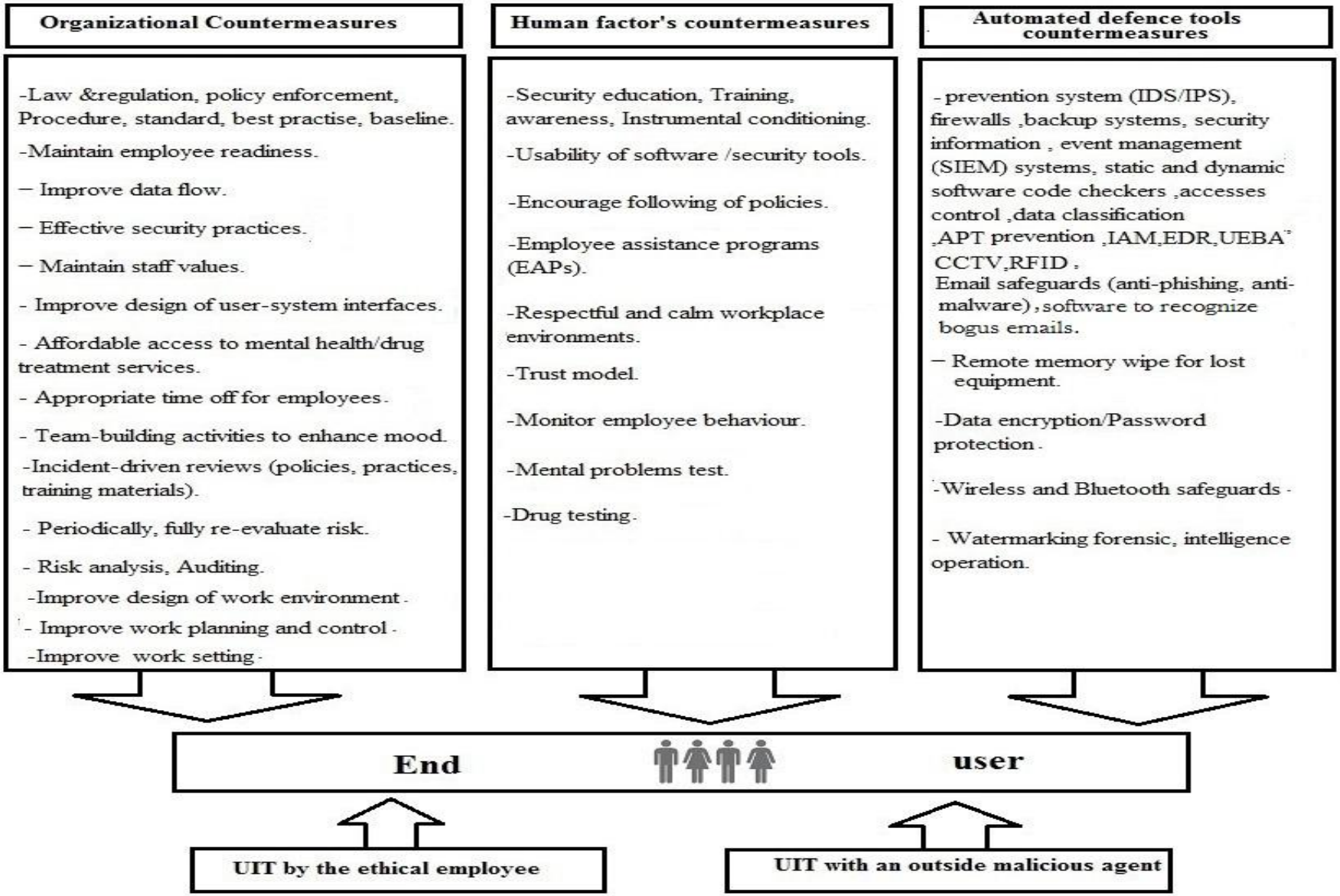

Figure 4. 2: Initial Version of UIT Countermeasure Model (UITCM)

4.4 Step 2: Development of Second Version of UITCM

Table 4.3 shows development activities of the second version of UITCM. In this table, the development of second version was carried out in two phases:

- Phase 1: Identification of contributing factors and likelihood of UIT.
- Phase 2: Development of Second Version of UITCM

The activities conducted in the first phase include, a survey which was conducted with Malaysian SMEs to determine the contributing factors of UIT. In second version, the development give additional attention to countermeasures of UIT factors identified during survey to ensure the proposed model have covering them.

In phase two, based on the results from questionnaire and an additional information that were extracted from the deep focused search in the previous studies, more components, elements, and design principles of UITCM were gathered. The relations between the model's components were determined, and the three main domains were divided into subgroups.

Table 4. 3: (UITCM) / Second Version development activities

Input	Initial version of UIT Countermeasure Model (UITCM)
Process	Phase 1: identification of contributing factors and likelihood of UIT. Phase 2: model development.
Output	second version of UIT Countermeasure Model (UITCM)

4.4.1 Phase 1: Identification of Contributing Factors and Likelihood of UIT

This study identified the likelihood of UITs to justify the need for the proposed model and examined whether the study problem still existed by identifying the likelihood of UITs. The most contributing factors of UITs have been identified in order to give them more focus and concern during the model development process and to ensure that they covered from all its aspects. The questionnaire of this study serves as a roadmap for developing the proposed model by determining of how much the

need for the model, as well as identifying the most contributing factors of UITs to be fully covered.

4.4.1.1 Pilot Study

A pilot study was carried out prior to final data collection to reveal deficiencies that can affect the consistency of the survey instrument and to validate the appropriateness of the questions for the present study. A total of fifty (50) surveys questionnaires were used to validate the survey instrument among IT Executives working in Malaysian SMEs. The reliability and validity tests were conducted based on the pilot study data and actual study data as well.

A. Reliability of Survey Questions

The reliability of the questionnaire answers was measured by Cronbach's coefficient alpha values. The term "reliability" in this study refers to the extent to which the measurement produces the same results with repeated measurement (Malhotra & Brik, 2003). The measurement of reliability provides internal consistency in the measurement of variables (Kim & Cha, 2002). The instrument's reliability is revealed to be more than 0.60 which is acceptable (Hair et al., 2006; Sekaran, 2003).

To ensure that the data collected is true and consistent to the extent possible, the reliability of the data was measured by utilizing Cronbach's coefficient alpha values (excellent reliability ranges 0.90 and above, high reliability 0.70 - 0.90, moderate reliability 0.50 -0.70 and low reliability 0.50 and below) which measured the internal consistency of the characters (Hinton et al., 2004; Field, 2005). The pilot study showed an excellent reliability of the UITs likelihood with (0.950) and a high

reliability of the UITs contributing factors questions with (0.892) as shown in Table1 (Appendix D).

The actual study showed a very high reliability of the questions of both likelihood and contributing factors of UITs. Table 4.4 shows the reliability tests results of the questions for the UITs likelihood and UITs contributing factors, with very high values of (0.993 and 0.933 respectively). The results of the reliability test proved that the questionnaire was reliable.

Table 4. 4: Cronbach Alpha Reliability Test (Actual Study)

Variables	Number of items	Cronbach Alpha	Type
Likelihood of UIT	6	0.993	Excellent reliability
UIT Contributing factors	20	0.933	Excellent reliability

B. Validity of Survey Questions

Questionnaire validity is the extent to which the results really measure what they are supposed to measure. These measures the degree of agreement of the results or conclusions obtained from the research questionnaire with the real world. The validity of the instrument is essential in data collection. Therefore, the correct data will determine validity of the results and research quality (Taherdoost, 2016).

The validity test of the questionnaire was conducted using Pearson correlations. Pearson's correlation coefficient is the statistical test that measures the association, or relationship, between variables. It gives information about the magnitude of the correlation, as well as the direction of the relationship, if one variable increases, the other variable tends to also increase if positive correlation or decrease if negative correlation. Correlation coefficient values range from –1 to +1, where 0 indicates that

there is no association, and the relationship gets stronger when the coefficient approaches an absolute value of 1 (Schober & Boer, 2018).

Degree of correlation refers to the coefficient of correlation. Degree of correlation considers as a very high correlation if the coefficient value lies between ± 0.90 and ± 1.00. If the value lies between ± 0.70 and ± 0.90, then it is considers as a high correlation. When the value lies between ± 0.50 and ± 0.70, then it is considers as a moderate correlation. If the value lies between ± 0.30 and ± 0.50, then it is considers as a low correlation, and there is no correlation when the value lies between 0.00 and ± 0.30 (Mukaka, 2012).

The results of the pilot study showed a very high correlation between all items of the UITs likelihood. The pilot study findings showed a significant correlation between the most selected factors by the participants and no correlation between the most selected factors and the least selected factors. See Tables 2 and Tables 3 (Appendixes D). As regards to the actual study results, all items of the likelihood were valid as shown in Table 4.5. Based on significant values obtained from the sig. (2_tailed) correlation, all probability values were = (0.000) with very high correlations ranged from 0.98** to 1.00**.

For example, Table 4.5 shows significant relationship between (Likelihood 1 and Likelihood 2). Based on the very high correlation (r=.988**) and the p value quoted under Sig. (2-tailed) which is 0.000 (reported as p < .001) which is less than 0.05. At the bottom of Table 4.5 is displayed "**Correlation is significant at the 0.01 level (2-tailed)". This means that the Pearson's correlation coefficient r = 0.988 with N of 311 is statistically significant at 0.01 level (p = 0.000), which of course is also significant at 0.05 level. Thus, there is a significant relationship between Likelihood 1 and Likelihood 2.

The correlation between (Likelihood 1 and Likelihood 2) means that the participants' answers for Likelihood 1 and Likelihood 2 were consonant meaning that the same participant has chosen the same answer for Likelihood 1 and Likelihood 2.

Where:

r = Pearson Correlation which represents the degree of correlation.

P value = probability value which should be less than 0.05 to prove that there is a significant relationship.

N = Number of participants.

Likelihood 1: represents (How likely would the organization face unintentional insider threats?)

Likelihood 2: represents (How likely would employees accidentally jeopardizing security of organization through data leaks or similar errors?)

Likelihood 3: represents (How likely would similar organizations face unintentional insider threats?)

Likelihood 4: represents (How likely would the organization not to face unintended insider threats?)

Likelihood 5: represents (How likely would finding employees are not aware of unintended insider threats in the organization?)

Likelihood 6: represents (How likely would employees unintentionally make mistakes affecting the information security of the organization?).

Table 4. 5: Correlations of the likelihood items (Actual Study)

Likelihood items	Likelihood 2	Likelihood 3	Likelihood 4	Likelihood 5	Likelihood 6
Likelihood 1	.988** .000	.977** .000	.993** .000	.989** .000	.991** .000

	311	311	311	311	311
Likelihood 2		.986** .000 311	.991** .000 311	.995** .000 311	.997** .000 311
Likelihood 3			.982** .000 311	.985** .000 311	.986** .000 311
Likelihood 4				.990** .000 311	.994** .000 311
Likelihood 5					.994** .000 311

** Correlation is significant at the 0.01 level (2-tailed).

The validity test of the questionnaire items of UITs contributing factors showed significant positive correlations (0.54** - 0.91**) among the most selected factors by the respondents (ignorance and negligence, situation awareness and human error respectively). However there were no correlations among the most selected factors and the least selected factors. The P values were < 0.05 (P=0.000) as shown in Table 4.6. The significant positive correlation of the most selected factors among each other and absence of correlations among the most selected factors and the least selected factors proved that the majority of the respondents had selected these three factors (ignorance and negligence, situation awareness and human error) respectively. Thus the answers of contributing factors of UITs were valid.

Where:

Factor1: implies (Human error)

Factor2: implies (Fatigue and sleepiness)

Factor3: Implies Perceived psychological exertion and tension

Factor4: Implies Consciousness of the Condition

Factor5: Implies Staff qualifications and experience

Factor6: Implies Thought's stray

Factor7: Implies Complacency

Factor8: Implies Ignorance and carelessness

Factor9: Implies Intentions, as well as legislative incentives and disincentives

Factor10: Implies Probability of threat as a personality trait

Factor11: represents (Gender)

Factor12: Implies Emotion

Factor13: Implies Consequences of Age

Factor14: Implies Medications and hormones have an impact.

Factor15: Organizational expenditure

Factor16: represents (Culture)

Factor17: represents (Communication)

Factor18: Implies Implementation of privacy policies

Factor19: Implies Assistance from management

Factor20: Implies workplace atmosphere layout

Table 4. 6: Correlations of contributing factors of UITs (Actual Study)

	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6	Factor 7	Factor 8	Factor 9	Factor 10	Factor 11	Factor 12	Factor 13	Factor 14	Factor 15	Factor 16	Factor 17	Factor 18	Factor 19	Factor 20
Factor 1	.079 .164 311	.094 .099 311	.594** .000 311	.202 .120 311	.179 .202 311	.061 .283 311	.538** .000 311	.107 .060 311	.087 .127 311	.124 .129 311	.175 .512 311	.107 .060 311	.071 .215 311	.149 .419 311	.162 .104 311	.209 .110 311	.179 .112 311	.129 .123 311	.144 .211 311
Factor 2		.842** .000 311	.047 .409 311	.391 .130 311	.442 .510 311	.772** .000 311	.043 .455 311	.740** .000 311	.911** .000 311	.638** .000 311	.452 .470 311	.740** .000 311	.893** .000 311	.532** .000 311	.488 .110 311	.377 .120 311	.442 .310 311	.612** .000 311	.549** .000 311
Factor 3			.056 .327 311	.464 .110 311	.525** .000 311	.650** .000 311	.050 .375 311	.879** .000 311	.924** .000 311	.757** .000 311	.537** .000 311	.879** .000 311	.752** .000 311	.631** .000 311	.579** .000 311	.448 .120 311	.525** .000 311	.727** .000 311	.652** .000 311
Factor 4				.120 .134 311	.106 .061 311	.036 .524 311	.905** .000 311	.063 .265 311	.052 .365 311	.074 .195 311	.104 .067 311	.063 .265 311	.042 .461 311	.088 .120 311	.096 .090 311	.124 .028 311	.106 .061 311	.077 .177 311	.086 .132 311
Factor 5					.885** .000 311	.302 .110 311	.109 .055 311	.528** .000 311	.429 .410 311	.613** .000 311	.865** .000 311	.528** .000 311	.349 .110 311	.736** .000 311	.802** .000 311	.965** .000 311	.885** .000 311	.639** .000 311	.713** .000 311
Factor 6						.341 .230 311	.096 .090 311	.597** .000 311	.485 .120 311	.693** .000 311	.977** .000 311	.597** .000 311	.395 .120 311	.832** .000 311	.907** .000 311	.854** .000 311	1.000** .000 311	.722** .000 311	.805** .000 311
Factor 7							.033 .564 311	.572** .000 311	.704** .000 311	.493 .130 311	.349 .130 311	.572** .000 311	.865** .000 311	.410 .340 311	.376 .110 311	.291 .130 311	.341 .160 311	.473 .310 311	.424 .110 311
Factor 8								.057 .313 311	.047 .412 311	.067 .241 311	.094 .098 311	.057 .313 311	.038 .505 311	.080 .159 311	.087 .125 311	.113 .047 311	.096 .090 311	.069 .222 311	.077 .173 311
Factor 9									.812** .000 311	.862** .000 311	.611** .000 311	1.000** .000 311	.661** .000 311	.718** .000 311	.658** .000 311	.510** .000 311	.597** .000 311	.827** .000 311	.741** .000 311
Factor 10										.700** .000 311	.496 .410 311	.812** .000 311	.814** .000 311	.583** .000 311	.535** .000 311	.414 .230 311	.485 .540 311	.672** .000 311	.602** .000 311
Factor 11											.709** .000	.862** .000	.570** .000	.833** .000	.764** .000	.592** .000	.693** .000	.959** .000	.860** .000

											311	311	311	311	311	311	311	311	311
Factor 12												.611** .000 311	.404 .110 311	.851** .000 311	.928** .000 311	.834** .000 311	.977** .000 311	.739** .000 311	.824** .000 311
Factor 13													.661** .000 311	.718** .000 311	.658** .000 311	.510** .000 311	.597** .000 311	.827** .000 311	.741** .000 311
Factor 14														.475 .410 311	.435 .700 311	.337 .210 311	.395 .410 311	.547** .000 311	.490 .120 311
Factor 15															.917** .000 311	.710** .000 311	.832** .000 311	.869** .000 311	.968** .000 311
Factor 16																.774** .000 311	.907** .000 311	.797** .000 311	.888** .000 311
Factor 17																	.854** .000 311	.617** .000 311	.688** .000 311
Factor 18																		.722** .000 311	.805** .000 311
Factor 19																			.897** .000 311

The results of the validity test proved that the questionnaire was valid.

In conclusion, based on the pilot study, it proves the validity and reliability of the questionnaire provided.

4.4.1.2 SMEs Survey

In the survey, the respondents were the IT Executives of Malaysian SMEs.

4.4.1.2.1 Response Rate and Data Adequacy

The total number of distributed questionnaires was 500. To avoid low response rate, the total number of questionnaires were distributed to 500 participants. As recommended by (Ramayah, et.al. 2005), a response rate should fall between 10-30 percent. In addition,(Babbie & Mouton, 2001) suggested that response rate of 50 percent or more is adequate for analysis and reporting Here, in this research, out of the 500 surveys, 311 questionnaires were returned which represented approximately 62.2% response rate. Table 4.7 shows the summary of data collection and response rate.

Table 4. 7: Summary of Data Collection and Response Rate

Responses	Total
Distributed questionnaires	500
Returned questionnaires	311
Response rate	62.2%

This research follows Tabachnick & Fidell (2007) recommendation in identifying the adequacy of the sample size (n). Using generalized formula, the adequacy of sample size was calculated: n > 50 + 8 m as shown in Table 4.8.Here, m is 2, as the variables of the study are the contributing factors of UIT and likelihood level of UIT.

Table 4. 8: Calculation Result of Sample Adequacy

Details	Result
Sample Size (n)	311
No. of Variables (m)	2
Adequacy	50+(8*2)= 66

Table 4.8 summarizes the calculation of the adequacy of the sample size used for the analysis reported in this study. Adequacy calculation showed that 66 samples were adequate. This indicated that a total of 66 out of the number of data were appropriate for the research. Therefore using 311 samples increases the accuracy of the result and sufficient data is achieved because the amount of data exceeds the sufficiency of 66 (n = 311 > 66) for this study.

4.4.1.2.2 Instrument of Study

The questionnaire consists of three sections (refer Appendix B).

• Section 1: Respondents' background information and experience, such as gender, age and working experience.

A. Gender of Respondents

The participants of this study were asked about their gender (male or female) through close-ended question. The current study which conducted in the selected SME's showed that out of the total respondents 63% of them were males while the total number of female respondents constitutes 37% (refer Table 4.9 and Figure 4.3).

Table 4. 9: Gender of Respondents

Type	Frequency	Percentage (%)
Male	196	63.0
Female	115	37.0
Total	311	100.0

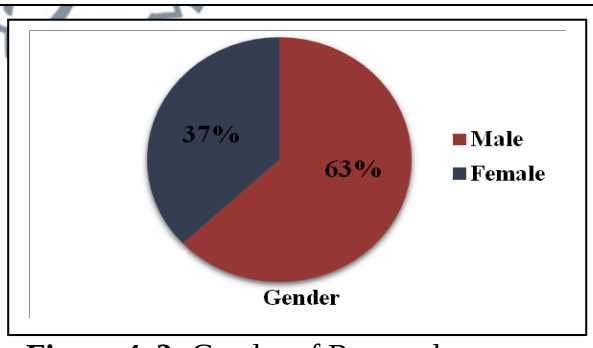

Figure 4. 3: Gender of Respondent

B. Age of Respondents

The participants of this study were asked about their age through close-ended question, by choosing an age domain from the five domains available which started from 20 and ended at above 60. When considering the age of the SME's respondents, 23.2 % aged between 20-30 years, 30.2 % between 31-40 years, 28.6 % between 41-50 years, 14.1 % between 51-60 years, and 3.9 % of the respondents aged 60 or above. Table 4.10 and Figure 4.4 present the distribution of the respondents by age.

Table 4. 10: Age of Respondents

Range	Frequency	Parentage (%)
20-30	72	23.2
31-40	94	30.2
41-50	89	28.6
51-60	44	14.1
Above 60 years	12	3.9
Total	311	100.0

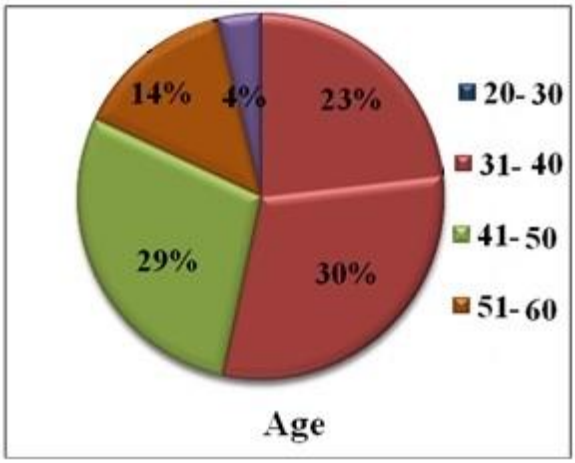

Figure 4. 4: Age of Respondents

C. Respondents' Working Experience in IT Industry

The participants of this study were asked about their working experience in IT industry, through close-ended question, by choosing number of years from the five domains available which started from one year and ended at above 20.

The result of this study regarding to the experience working years in IT shows that nearly 53.7% of the respondents have been working in IT industry for a period of 1-5 years. 26.4% of respondents have been working in IT industry for 6 to 10 years and 10% from 11-15 years. Out of 311 respondents, 20 (6.4%) had 16 to 20 experience years. 21 to 25 years of experience represented 3.5% of the participants (refer Table 4.11 and Figure 4.5).

Table 4. 11: Respondents' Working Experience in IT Industry

Range	Frequency	Percentage (%)
1-5	167	53.7
6-10	82	26.4
11-15	31	10.0
16-20	20	6.4
21-25	11	3.5
Total	311	100.0

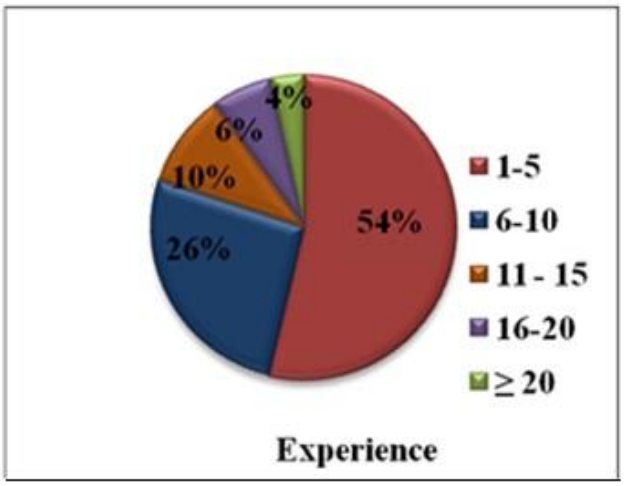

Figure 4. 5: Respondents' Working Experience in IT Industry

D. Awareness of Unintentional Insider Threats

The participants of this study were asked whether they know UITs or not, through close-ended question, by choosing yes or no from the choices available. The result of the survey shows that most executives in SMEs in Malaysia know UITs by 99 % percent or 308 respondents. Only 1 % or 3 respondents don't know about UITs. Table 4.12 and Figure 4.6 present the results on awareness of UITs by the respondents.

Table 4. 12: Respondent s' Awareness of Unintentional Insider Threats

Status	Frequency	Percentage (%)
Yes	308	99.0
No	3	1.0
Total	311	100.0

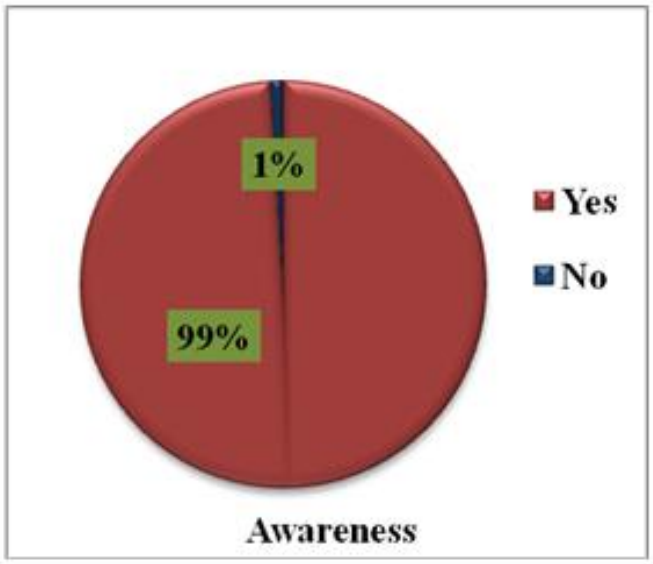

Figure 4. 6: Respondent s' Awareness of Unintentional Insider Threats

E. Organization Policy in Addressing Unintentional Insider Threats

The participants of this study were asked whether their organizations policy addressing the UITs or not, through close-ended question by choosing yes or no from the choices available.

The study showed 98.7% of respondents confirmed that there is a policy to addressing the UITs in their organizations and only 1.3% of respondents said that the UITs are no considered in their policy (refers Table 4.13 and Figure 4.7).

Table 4. 13: Policy of Organization Addressing the UIT

Status	Frequency	Percentage (%)
Yes	307	98.7
No	4	1.3
Total	311	100.0

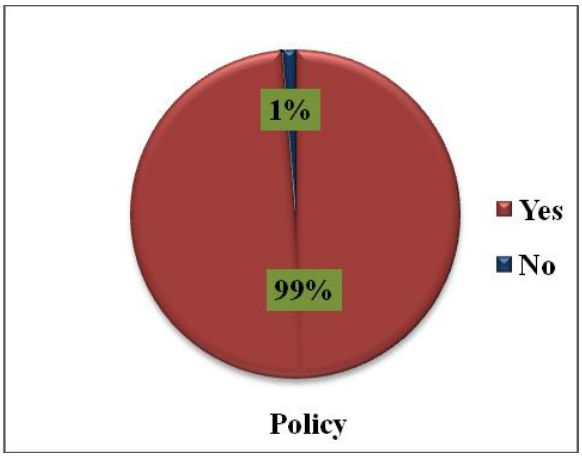

Figure 4. 7: Policy of Organization Addressing the UIT

• Section 2: Respondents' opinions regarding the likelihood level of unintentional insider threats in Malaysian organizations.

The participants of this study were asked to tick only one answer from the options available which started from not likely and ended at most likely as shown in the Table 4.14.

Table 4. 14: The Questions That Were Asked to Determine Likelihood of UITs.

Questions	Not likely	Least likely	Likely	Very likely	Most likely
1. How likely would the organization face unintentional insider threats?					
2. How likely would employees accidentally jeopardizing security of organization through data leaks or similar errors?					
3. How likely would similar organizations face unintentional insider threats?					
4. How likely would the organization not to face unintended insider threats?					
5. How likely would finding employees are not aware of unintended insider threats in the organization?					
6. How likely would employees unintentionally make mistakes affecting the information security of the organization?					

The survey analysis provides a discussion regarding respondents' perceptions of the likelihood of UITs occurrences in their respective organization. Each one of the respondents was asked to indicate his/her opinion by chosen from the available options from ('Not likely' to 'Most likely'). Table 4.15 and Figure 4.8 show the SME's executives' perception on the likelihood of UITs to occur in their computerized organization system. The results revealed that majority of the respondents from all SME's alleged that their organizations were very likely to have faced threats with 634 (34.2%), which constituted approximately one-third of the respondents. Also, 442 (23.9%) believed that their organizations were likely to confront this type of threats while 172 (9.3%) were most likely to have faced such threats. However, 332 (17.9%) and 272 (14.7%) responded that their organizations were not likely or least likely to face such threats respectively.

As a summary of these results, 67% of the participants believed that their organizations were likely to confront UITs while 33% were not likely to have faced UITs. In light of these results, it could be said that the majority of SME's selected were confronted with this type of threats. Table 4.15 and Figure 4.8 show the likelihood of UITs result which calculated from the six questions together .For

example the frequency of (Not likely) in the table =332, that means 332 is the number of times (Not likely) was chosen in the six questions together. Tables (4, 5, 6, 7, 8 and 9 in Appendix D) show managers perception of the UITs likelihood of the six questions separately.

The findings indicated that in total the respondents perceived the likelihood of threats occurrences on a scale of 'likely' in their organizations.

In agreement with the current study, study of security threats of computerized banking systems in Malaysia by (Malami et al., 2012) reported that all banks' branches covered in his study were confronted with UITs. He concluded that this might be the result of lack of technical and/or adequate knowledge among the employees to operate the system. The result of this study was coherent with the previous studies reported human errors as the top ranked security threats (Loch et al., 1992; Whitman, 2004;Cohen, 1998; Baskerville, 2014; Musa, 2011). Studies of (Samy, 2010; Humaidi & Balakrishnan, 2013) agreed with the current study that the human error is one of main internal threats in applying health information system in Malaysia. Research by (Asai & Perez,2012) carried out surveys in nine investee countries and concluded that, US-based companies located in Malaysia have the possibility of facing more risks due to the employees' unintentional sharing of confidential information. In the same context the studies by (Malami et al., 2012; Asai & Perez, 2012; Waluyan,et al,2009) show that UITs comes at the top of security threats to Malaysian organizations. In addition, the review conducted on insider threats status in Malaysian organizations concluded that unintentional human mistakes or errors such as accidentally leaking sensitive company information on social networks are the most common .(Tuor et al.,2017;Isnin & Sedek,2018). Studies of (Asai, & Waluyan, 2008; Waluyan et al, 2010; Asai & Hakizabera, 2010) showed that

"unintentional sharing of confidential information" is the problem with the highest severity among the developed problems which foreign companies may face in Malaysia. In the same aspect, the firms surveyed by Forrester that had experienced a breach in 2015, internal incidents were the leading cause, and more than 50% of those were due to inadvertent misuse or user error, known as the "accidental insider"(Forcepoint,2016).

Table 4. 15: Likelihood of UITs based on Six Questions

Status	Frequency	Percentage (%)
Not likely	332	17.9
Least likely	272	14.7
Likely	442	23.9
Very likely	634	34.2
Most likely	172	9.3
Likely (Total)	1248	67.3
Not likely (Total)	604	32.6

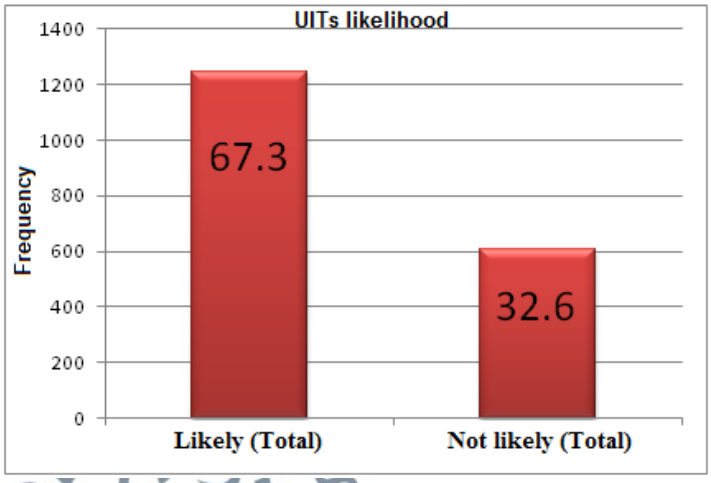

Figure 4. 8: The Likelihood of UITs

Regarding to UITs likelihood questions, each question has five options from ('Not likely' to 'Most likely') which represent UITs likelihood variables. The mean of these five options was calculated to summarize the participant's answers quantitatively for each one of the six questions separately.

UITs likelihood questions were built on (a 5-point scale) and the five options were coded as follows (Not likely with (0), Least likely with (1), Likely with (2), Very

likely with (3), Most likely with (4)). So the data set (participants' answers) is groups of these five numbers. The means of each question were calculated by adding the participants' answers and dividing the total by the number of participants (311).

Table 4.16 shows the mean values for the respondent's answers for each question separately. From Table 4.16 it was noted that, means of participants' answers were tend to 2 which represents 'likely'.

The standard deviation of a data set tells us how dispersed the data is from the mean. Thus the small standard deviation values in Table 4.16 indicate that there are no outliers.

Table 4. 16: Mean and Standard Deviation of the likelihood of UITs

likelihood of UITs	Mean	Std. Deviation
Likelihood1	2.0482	1.25759
Likelihood2	2.0161	1.26353
Likelihood3	1.9775	1.26598
Likelihood4	2.0386	1.25407
Likelihood5	2.0193	1.24937
Likelihood6	2.0257	1.25697

- **Section 3: Respondents' opinions regarding the contributing factors of unintentional insider threats in Malaysian organizations.**

A critical literature review on the contributing factors of UITs was conducted in order to form the research questions. The participants of this study were asked to determine which of the listed factors are the most contributing of UITs in Malaysian organizations. The contributing factors of UITs were listed as shown in the following.

Table 4. 17: Question That Was Provided to Identify UITs Leading Variables.

The Contributing Factors	Tick
Human Error ("I didn't mean to do that.")	
Fatigue And Sleepiness	
Stress And Subjective Mental Workload	
Situation Awareness ("I thought that's what I was supposed to do.")	
Skills And Experience of employees	
Mind Wandering ("I forgot to do that.")	
Apathy ("I don't care")	
Ignorance and negligence ("Nothing will happen")	
Motives and Incentive and Disincentive Policy	

Risk possibility as Personality feature (Recklessness)	
Gender (More likely to take risks, female/male)	
Mood (The influence of mood on making risky choices)	
Age Effects (More likely to take risks, young employees/ older employees)	
Influence of Drugs and Hormones	
Budget of organization	
Culture (Organizational culture)	
Communication (The exchange of messages and ideas between people inside and outside of the organisation)	
Security Policy Enforcement	
Management Support (job pressure, insufficient resources, poor management systems, inadequate security practices ,and work planning /control)	
Design of work environment (illumination, noise, temperature, vibration, the technology and equipment they use is poorly designed and confusing to use, etc.)	

A survey was conducted to identify the most significant contributing factors of UITs in Malaysian organizations. According to the literature reviews, the contributing factors of UITs are varied and the highest percentage of accidental issues comes from ignorance and negligence. The result of this study shows that the majority of respondents (27%) characterized their incidents (UITs) arising from unintentional employee ignorance and negligence followed by situation awareness (26%) and human error (22%). The percentage of the others contributing factors were (mind wandering 2.2%, security policy enforcement 2.2%, mood 2.2%, culture 1.9%, budget of organization 1.6%, design of work environment 1.5%) respectively.

The lowest percentage of UITs contributing factors were presented by management support 1.3%, gender 0.11%, motives and incentive and disincentive policy 0.90%, age effects 0.90%, stress and subjective mental workload 0.68%, risk possibility as personality feature 0.60%, fatigue and sleepiness 0.48%, influence of drugs and hormones 0.40% and apathy 0.30% respectively as shown in (Table 4.17)

In agreement with this work, study by Burke and Christiansen (2009) reported that unintentional data loss through employee negligence had the highest number of incidents in the financial (13.7), public (14.5), and healthcare (14.5) sectors. The majority of organizations (52%) characterized their insider threat incidents as

predominantly accidental. Only 19% believed insider threat incidents were primarily deliberate and 26% believed the incidents were an equal combination. Moreover, unintentional data loss through employee negligence has the greatest financial impact.

As per the Threat Landscape Report 2018 by the ENISA, 27% of data breach incidents were caused by human factors or negligence (Brian & Christiansen, 2009).

Another study by Raytheon (2015) showed that 70 percent of U.S. survey respondents and 64 percent of German respondents said that more security incidents are caused by unintentional mistakes rather than intentional and/or malicious acts.

They proved that that employee negligence can result in insider threats and cost companies millions of dollars each year. They concluded that unintentional employee negligence severely diminishes the productivity of the IT function according to 73 percent of U.S respondents and 67 percent of German respondents. According to (FORCEPOINT, 2016) employee error/negligence was responsible for nearly 15% of data breach incidents in 2015.

The two contributing factors (communication between people inside and outside of the organization and skills and experience of employees) represented a percentage of 32% and 30% respectively. In parallel with the current study, Raytheon (2015) noted that workplace stress, multitasking, long hours and a lack of resources and budget are other factors can cause insider threats. In addition they consider the biggest contributor factor is employee negligence. They concluded German organizations do not have the necessary safeguards in place to protect against careless employees (54 percent). U.S. employees are not properly trained to follow data security policies (60 percent) and that senior executives do not consider data security a priority (50 percent). In both the U.S. and Germany, IT security practitioners spend an average of

almost three hours each day dealing with the security risks caused by employee mistakes or negligence.

Table 4. 18:The Contributing Factors of UITs

Contributing Factors of UITs	Code	Frequency	Percentage (%)
Human error	F1	225	22
Fatigue and sleepiness	F2	5	0.5
Stress and subjective mental workload	F3	7	0.7
Situation awareness	F4	274	26
Skills and experience of employees	F5	30	3
Mind wandering	F6	24	2
Apathy	F7	3	0.3
Ignorance and negligence	F8	280	27
Motives and incentive and disincentive policy	F9	9	0.9
Risk possibility as personality feature	F10	6	0.6
Gender	F11	12	0.1
Mood	F12	23	2.2
Age effects	F13	9	0.9
Influence of drugs and hormones	F14	4	0.4
Budget of organization	F15	17	1.6
Culture	F16	20	1.9
Communication between	F17	32	3
Security policy enforcement	F18	24	2
Management support	F19	13	1.3
design of work environment	F20	16	1.5

Table 4.18 presents the means of participants' answers on the questions of the contributing factors of UITs. The selected factor was coded with (1), while the unselected factor was coded with (0). So the data set (participants' answers) is groups of these two numbers. The means of each factor were calculated by adding the participants' answers and dividing the total by the number of participants (311).

Table 4.18 shows the differences between the means of the most selected factors the least selected factors. Where all the means of the most selected factors were approaching to one .On the other hand, the means of the least selected factors equal to zero. The small standard deviation values in Table 4.18 indicate that there are no outliers.

Table 4. 19**: Mean and Standard Deviation of UITs Contributing Factors**

Contributing Factors of UIT	Code	Mean	Std. Deviation
Human error	F1	.7235	.44800

Fatigue and sleepiness	F2	.0161	.12598
Stress and subjective mental workload	F3	.0225	.14857
Situation awareness	F4	.8810	.32428
Skills and experience of employees	F5	.0965	.29570
Mind wandering	F6	.0772	.26729
Apathy	F7	.0096	.09790
Ignorance and negligence	F8	.9003	.30005
Motives and incentive and disincentive policy	F9	.0289	.16791
Risk possibility as personality feature	F10	.0193	.13777
Gender	F11	.0386	.19291
Mood	F12	.0740	.26212
Age effects	F13	.0289	.16791
Influence of drugs and hormones	F14	.0129	.11286
Budget of organization	F15	.0547	.22769
Culture	F16	.0643	.24570
Communication	F17	.1029	.30431
Security policy enforcement	F18	.0772	.26729
Management support	F19	.0418	.20046
design of work environment	F20	.0514	.22126

From the results of this survey, it could be said that majority of the SME's selected were confronted with UITs. Therefore there is urgent need for develop a new model as countermeasure to UITs.

This study determined the most contributing factors of UITs in Malaysian SMEs which are ignorance and negligence, situation awareness and human error in order to give them more focus and concern during development of the second version of the model and to ensure that they are covered from all aspects, then incorporate the countermeasures of the identified factors into the model

4.4.2 Phase 2: Development of Second Version of the model

As discussed above, a survey was conducted in Malaysian SMEs to determine the contributing factors of UIT, which were emphasized in development stage of the second version of the UITCM, where additional attention was given to countermeasures of these factors to ensure covering them. Based on the results from questionnaire and additional information that were extracted from the deep focused

search in the previous studies, more components, elements, and design principles of UITCM were gathered. The relations between the model's components were determined, and the three main domains were divided into subgroups. Thus the initial version of the model (UITCM) was improved based on the data gathered and the second version of the model (UITCM) was developed.

4.4.2.1 Model Validation based on Survey Results

The improvement of the initial version is based component validation and checklist comparison with existing models analysis through qualitative methods. In line with Inglis (2008), the investigation was conducted by referring to appropriate research literature as part of the procedures for investigation the proposed conceptual model. For this purpose, a cross check with existing literature was conducted and a number of UITs contributing factors were listed, starting from broad organizational factors to human factors with a cognitive or psychosocial context, to other behavioural factors relating to risk tolerance, demographic and cultural influences, and even drug- and hormone-related contributing factors. Reference to the literature and existing models was conducted; to know to what extent the Second Version of UITCM is providing countermeasures for all contributing factors against UITs, and whether it outperforms other existing models in that. Table 4.20 shows the selected UIT Mitigation Strategies and Countermeasures in the literatures. The comparison of the Second Version of UITCM and the existing models with the contributing factors of UITs is shown in Table 4.20 for validation purposes.

Table 4. 20:The selected UIT Mitigation Strategies and Countermeasures Recommended

Contributing Factors of UIT Based on Survey	Possible Mitigations	C01	C02	C03	C04	UITCM
Human error	- Improve data flow.	✔	✔	X	X	✔
	- Improve design of work environment.	X	X	X	✔	✔
	- Maintain employee readiness.	X	✔	X	X	✔
	- Effective security practices.	X	✔	X	X	✔
	- Improve work planning and control.	✔	✔	X	X	✔
	-Improve work setting and management practices.	X	✔	X	X	✔
	- Risk analysis, Auditing.	✔	X	X	X	✔
	- Incident-driven reviews (policies, practices, training materials).	X	X	X	✔	✔
	- Periodically, fully re-evaluate risk.	X	X	X	✔	✔
	- Appropriate time off for employees.	X	X	X	✔	✔
	- Security education, Training, awareness.	✔	✔	X	X	✔
	-Instrumental conditioning.	X	X	✔	X	✔
	- Usability of software /security tools.	X	✔	X	X	✔
	- Encourage following of policies.	X	X	X	X	✔
	- Stimulation of risk perception.	X	✔	✔	X	✔
	- Employee assistance programs (EAPs).	X	X	X	X	✔
	- Respectful and calm workplace environments.	X	X	X	X	✔
	- Improve design of user-system interfaces.	X	X	X	✔	✔
	- Trust model.	X	X	✔	X	✔
	- Monitor employee behaviour.	X	X	X	X	✔
	- Collaborative Reinforcement Model.	X	X	✔	X	✔
	- Watermarking forensic, intelligence operation.	✔	X	X	X	✔
	- Backup systems (Spatial /Temporal) Replication.	X	X	✔	X	✔
	- Remote memory wipe for lost equipment.	X	✔	X	X	✔
	- Automation.	X	X	✔	X	✔

	- Data encryption.	✔	X	X	X	✔
	-Password protection.	X	X	X	✔	✔
	- Wireless and Bluetooth safeguards.	X	X	X	✔	✔
	- Standard systems/Email safeguards (anti-phishing, anti-malware etc).	✔	✔	X	✔	✔
	-Prevention system (IDS/IPS,DLP).	✔	✔	X	✔	✔
	-Firewalls.	✔	✔	X	X	✔
	-APT prevention, accesses control.	✔	X	X	X	✔
	-Static and dynamic software code checkers.	✔	X	X	X	✔
	-Data classification, IAM.	✔	X	X	X	✔
	- Security information event management (SIEM) systems ,software to recognize bogus emails.	✔	X	X	✔	✔
	-EDR,UEBA,CCTV,RFID.	✔	X	X	X	✔
Fatigue and Sleepiness	- Maintain employee readiness.	X	✔	X	X	✔
	- Effective security practices.	X	✔	X	X	✔
	- Improve design of user-system interfaces.	X	X	X	✔	✔
	- Appropriate time off for employees.	X	X	X	✔	✔
	- Improve design of work environment.	X	X	X	✔	✔
	- Improve work planning and control.	X	X	X	X	✔
	- Improve work setting and management practices.	X	✔	X	X	✔
	- Monitor employee behaviour.	X	X	X	X	✔
	-Trust model.	X	X	✔	X	✔
	- Employee assistance programs (EAPs).	X	X	X	X	✔
	- Respectful and calm workplace environments.	X	X	X	X	✔
	- Automation.	X	X	✔	X	✔
	- Security information event management (SIEM) systems.	X	X	X	✔	✔
Stress And Subjective Mental Workload	- Maintain employee readiness.	X	✔	X	X	✔
	- Maintain staff values.	X	✔	X	X	✔
	- Effective security practices.	X	✔	X	X	✔
	- Improve design of user-system interfaces.	X	X	X	✔	✔
	- Appropriate time off for employees.	X	X	X	✔	✔

	- Improve design of work environment.	X	X	X	✔	✔
	- Improve work planning and control.	X	X	X	X	✔
	- Improve work setting and management practices.	X	✔	X	X	✔
	- Risk analysis, Auditing.	✔	X	X	X	✔
	- Incident-driven reviews (policies, practices, training materials).	X	X	X	✔	✔
	- Periodically, fully re-evaluate risk.	X	X	X	✔	✔
	- Monitor employee behaviour.	X	X	X	X	✔
	-Trust model.	X	X	✔	X	✔
	- Security information event management (SIEM) systems.	X	X	X	✔	✔
	- Respectful and calm workplace environments.	X	X	X	X	✔
	- Employee assistance programs (EAPs).	X	X	X	X	✔
	- Automation.	X	X	✔	X	✔
Situation Awareness	- Improve design of user-system interfaces.	X	X	X	✔	✔
	- Stimulation of risk perception.	X	✔	✔	X	✔
	- Security education, Training, awareness.	✔	✔	X	X	✔
	-Instrumental conditioning.	X	X	✔	X	✔
	-Usability of software /security tools.	X	✔	X	X	✔
	- Automation.	X	X	✔	X	✔
Skills And Experience	- Stimulation of risk perception.	X	✔	✔	X	✔
	- Security education, Training, awareness.	✔	✔	X	X	✔
	-Instrumental conditioning.	X	X	✔	X	✔
	- Usability of software /security tools.	X	✔	X	X	✔
	- Automation.	X	X	✔	X	✔
Mind Wandering	- Maintain employee readiness.	X	✔	X	X	✔
	- Effective security practices.	X	✔	X	X	✔
	- Appropriate time off for employees.	X	X	X	✔	✔
	- Risk analysis, Auditing.	✔	X	X		✔
	- Incident-driven reviews (policies, practices, training materials).	X	X	X	✔	✔
	- Periodically, fully re-evaluate risk.	X	X	X	✔	✔
	- Monitor employee behaviour.	X	X	X	X	✔
	-Trust model.	X	X	✔	X	✔

	- Stimulation of risk perception.	X	✔	✔	X	✔
	- Employee assistance programs (EAPs).	X	X	X	X	✔
	- Respectful and calm workplace environments.	X	X	X	X	✔
	- Automation.	X	X	✔	X	✔
	- Security information event management (SIEM) systems.	X	X	X	✔	✔
Apathy	- Monitor employee behaviour.	X	X	X	X	✔
	- CCTV, RFID.	✔	X	X	X	✔
	- Security information event management (SIEM) systems.	X	X	X	X	✔
	- Effective security practices.	X	✔	X	X	✔
	- Maintain staff values.	X	✔	X	X	✔
	-Trust model.	X	X	✔	X	✔
	- Collaborative Reinforcement Model.	X	X	✔	X	✔
	- Stimulation of risk perception.	X	✔	✔	X	✔
	-Security education, Training, awareness.	✔	✔	X	X	✔
	-Instrumental conditioning.	X	X	✔	X	✔
	-Encourage following of policies.	X	X	X	X	✔
	- Automation.	X	X	✔	X	✔
Ignorance and Negligence	- Monitor employee behaviour.	X	X	X	X	✔
	- CCTV, RFID.	✔	X	X	X	✔
	- Security information event management (SIEM) systems.	X	X	X	✔	✔
	- Effective security practices.	X	✔	X	X	✔
	- Maintain staff values.	X	✔	X	X	✔
	-Trust model.	X	X	✔	X	✔
	- Collaborative Reinforcement Model.	X	X	✔	X	✔
	- Stimulation of risk perception.	X	✔	✔	X	✔
	-Security education, Training, awareness.	✔	✔	X	X	✔
	-Instrumental conditioning.	X	X	✔	X	✔
	-Encourage following of policies.	X	X	X	X	✔
	- Automation.	X	X	✔	X	✔
Motivation and	- Maintain staff values.	X	✔	X	X	✔

Incentive and Disincentive Policy	- Team-building activities to enhance mood.	X	X	X	✔	✔
	- Employee assistance programs (EAPs).	X	X	X	X	✔
	- Respectful and calm workplace environments.	X	X	X	X	✔
	- Monitor employee behaviour.	X	X	X	X	✔
	- CCTV.	✔	X	X	X	✔
	- Improve design of work environment.	X	X	X	✔	✔
	- Improve work planning and control.	X	X	X	X	✔
	- Improve work setting and management practices.	X	✔	X	X	✔
	- Stimulation of risk perception.	X	✔	✔	X	✔
	- Collaborative Reinforcement Model.	X	X	✔	X	✔
Risk Possibility as Personality Feature	- Security education, Training, awareness.	✔	✔	X	X	✔
	- Instrumental conditioning.	X	X	✔	X	
	- Security information event management (SIEM) systems.	X	X	X	✔	✔
	- Improve design of user-system interfaces.	X	X	X	✔	✔
	- Stimulation of risk perception.	X	✔	✔	X	✔
	-Monitor employee behaviour.	X	X	X	X	✔
	- Effective security practices.	X	✔	X	X	✔
	- Improve work setting and management practices.	X	✔	X	X	✔
Gender	-Incident-driven reviews (policies, practices, training materials).	X	X	X	✔	✔
	- Security education, Training, awareness.	✔	✔	X	X	✔
	-Instrumental conditioning.	X	X	✔	X	✔
	- Stimulation of risk perception.	X	✔	✔	X	✔
	-Improve work setting and management practices.	X	✔	X	X	✔
	-Trust model.	X	X	✔	X	✔
Mood	- Appropriate time off for employees.	X	X	X	✔	✔
	- Maintain employee readiness.	X	✔	X	X	✔
	-Team-building activities to enhance mood.	X	X	X	✔	✔
	- Employee assistance programs (EAPs).	X	X	X	X	✔
	- Affordable access to mental health/drug treatment services.	X	X	X	✔	✔
	- Respectful and calm workplace environments.	X	X	X	X	✔
Age Effects	- Incident-driven reviews (policies, practices, training materials).	X	X	X	✔	✔

	- Improve work setting and management practices.	X	✔	X	X	✔
	-Trust model.	X	X	✔	X	✔
	- Stimulation of risk perception.	X	✔	✔	X	✔
	-Security education, Training, awareness.	✔	✔	X	X	✔
	- Instrumental conditioning.	X	X	✔	X	✔
Influence of Drugs and Hormones	-Automation.	X	X	✔	X	✔
	-Improve work setting and management practices.	X	✔	X	X	✔
	-Employee assistance programs (EAPs).	X	X	X	X	✔
	- Affordable access to mental health/drug treatment services.	X	X	X	✔	✔
	- Mental problems test.	X	X	X	X	✔
	- Drug testing.	X	X	X	X	✔
Budget	-Improve work planning and control.	X	X	X	X	✔
	-Improve work setting and management practices.	X	✔	X	X	✔
Culture	-Security education, Training, awareness.	✔	✔	X	X	✔
	-Instrumental conditioning.	X	X	✔	X	✔
	-Improve work setting and management practices.	X	✔	X	X	✔
	-Incident-driven reviews (policies, practices, training materials).	X	X	X	✔	✔
	-policy enforcement.	X	X	X	X	✔
Communication	-Law &regulation, policy enforcement, Procedure, standard, best practise, baseline.	✔	X	X	X	✔
	- Standard Operating Procedure (SOP).	X	X	✔	X	✔
	-Improve data flow.	✔	✔	X	X	✔
	- Maintain staff values.	X	✔	X	X	✔
	- Stimulation of risk perception.	X	✔	✔	X	✔
	-Security education, Training, awareness.	✔	✔	X	X	✔
	- Instrumental conditioning.	X	X	✔	X	✔
	-Usability of software /security tools.	X	✔	X	X	✔
	-Encourage following of policies.	X	X	X	X	✔
Security Policy Enforcement	-Law &regulation, policy enforcement, Procedure, standard, best practise, baseline.	✔	X	X	X	✔
	-Standard Operating Procedure (SOP).	X	X	✔	X	✔
	-Encourage following of policies.	X	X	X	X	✔

	-Monitor employee behaviour.	X	X	X	X	✔
	- CCTV.	✔	X	X	X	✔
	- Collaborative Reinforcement Model.	X	X	✔	X	✔
Management Support	-Law &regulation, policy enforcement, Procedure, standard, best practise, baseline.	✔	X	X	X	✔
	-Standard Operating Procedure (SOP).	X	X	✔	X	✔
	-Maintain employee readiness.	X	✔	X	X	✔
	- Improve data flow.	✔	✔	X	X	✔
	- Effective security practices.	X	✔	X	X	✔
	- Maintain staff values.	X	✔	X	X	✔
	- Improve design of user-system interfaces.	X	X	X	✔	✔
	- Affordable access to mental health/drug treatment services.	X	X	X	✔	✔
	- Appropriate time off for employees.	X	X	X	✔	✔
	- Team-building activities to enhance mood.	X	X	X	✔	✔
	- Improve design of work environment.	X	X	X	✔	✔
	- Improve work planning and control.	X	X	X	X	✔
	-Improve work setting and management practices.	X	✔	X	X	✔
	- Risk analysis, Auditing.	✔	X	X	X	✔
	-Incident-driven reviews (policies, practices, training materials).	X	X	X	✔	✔
	- Periodically, fully re-evaluate risk.	X	X	X	✔	✔
	-Monitor employee behaviour.	X	X	X	X	✔
	-Trust model.	X	X	✔	X	✔
	- Collaborative Reinforcement Model.	X	X	✔	X	✔
	-Mental problems test.	X	X	X	X	✔
	-Drug testing.	X	X	X	X	✔
	-Stimulation of risk perception.	X	✔	✔	X	✔
	-Security education, Training, awareness.	✔	✔	X	X	✔
	-Instrumental conditioning.	X	X	✔	X	✔
	-Usability of software /security tools.	X	✔	X	X	✔
	-Encourage following of policies.	X	X	X	X	✔
	-Employee assistance programs (EAPs).	X	X	X	X	✔

	-Respectful and calm workplace environments.	X	X	X	X	✔
	-Watermarking forensic, intelligence operation.	✔	X	X	X	✔
	-Backup systems (Spatial /Temporal) Replication.	X	X	✔	X	✔
	- Remote memory wipe for lost equipment.	X	✔	X	X	✔
	-Automation.	X	X	✔	X	✔
	-Data encryption.	✔	X	X	X	✔
	-Password protection.	X	X	X	✔	✔
	-Wireless and Bluetooth safeguards.	X	X	X	✔	✔
	- Standard systems/Email safeguards (anti-phishing, anti-malware etc).	✔	✔	X	✔	✔
	-prevention system (IDS/IPS,DLP).	✔	✔	X	✔	✔
	-Firewalls.	✔	✔	X	X	✔
	-APT prevention, accesses control.	✔	X	X	X	✔
	-Static and dynamic software code checkers.	✔	X	X	X	✔
	-Data classification, IAM.	✔	X	X	X	✔
	-Security information event management (SIEM) systems ,software to recognize bogus emails.	✔	X	X	X	✔
	-EDR,UEBA,CCTV,RFID.	✔	X	X	X	✔
Design Of Work Environment	- Improve design of user-system interfaces.	X	X	X	✔	✔
	-Improve design of work environment.	X	X	X	✔	✔

The comparison of the UITCM with the contributing factors of UITs proved that UITCM managed to cover all contributing factors of UITs. However, the comparison showed that, none of the existing models and strategies has covered all contributing factors of UITs and they focused on specific aspects of UITs countermeasures.

4.4.2.2 Model Development based on Component Validation

The elements in second version of the UITCM has been refined into groups and components is divided into three major domains: ‘the organizational countermeasures’, ‘the human factor's countermeasures’, and ‘the automated defence

tools countermeasures. The three main domains and the nine groups of UITCM components are shown in Table 4.21.

Table 4. 21: UITCM Groups and Components

UITCM Main Domains	UITCM Groups
Organizational Countermeasures.	Process
	Managerial
	Monitoring
Human Factor's Countermeasures.	Psychological
	Behaviour
	Culture
Automated Defence Tools	Detection
	Prevention
	Incident response

The UITCM is formulated on the basis that the components in each group support each other's, for example in the prevention group the DLP (Data Loss Prevention) system, which as a prevention tool, needs support and integrates with other detection solutions, such as APT (Advanced Persistent Threat) and IAM (Identity Access Management), to optimize its functions. In behaviour group, monitoring employee behaviour supports segregation of duties through Trust Model to reduce employee errors. While in managerial group, policies are insufficient and need to be supported by the others components. Policies are much like a strategic plan because they outline what should be done but don't specifically dictate how to accomplish the stated goals. They are generic, the policy are there to serve as a guide but do not provide detailed specifics in implementation. Those decisions are left for standards, baselines, and procedures, and implementing security best practices throughout the organization, as defined by widely tested and implemented security norms in the industry. Figure 4.9 shows the second version of (UITCM) with main components and its subgroups.

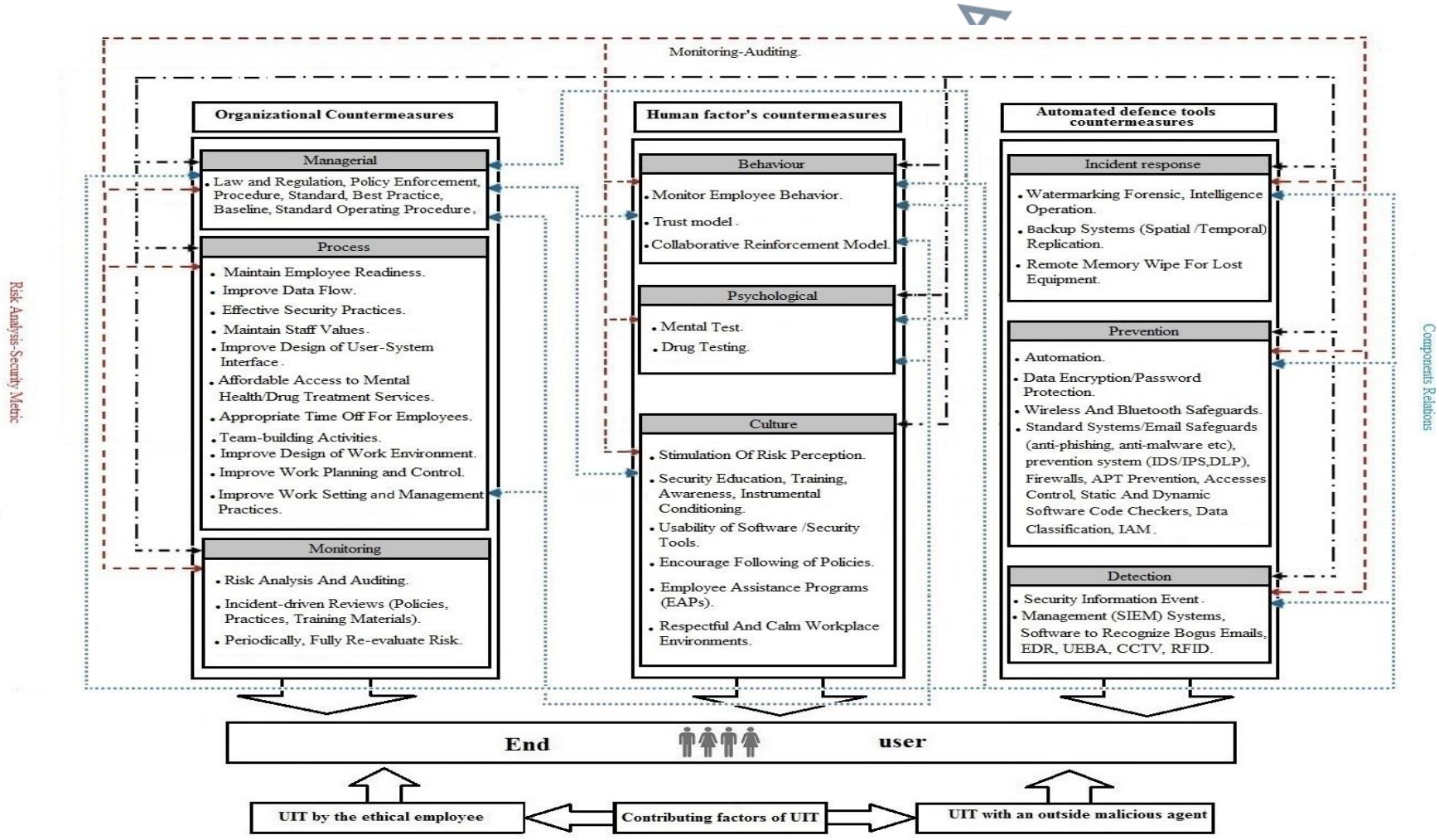

Figure 4. 9: Second Version of UIT Countermeasure Model (UITCM)

Defining and clarifying terminologies and components used in the UITCM is a crucial process. It is important to help the users on how to read and understand the model clearly. The details explanation of countermeasures components in each domain of the (UITCM) are described in (Appendix E) Table 1, Table 2 and Table 3.

4.2.2.3 Relations for the Second Version of (UITCM)

It is also important to delineate the relations, flows and connections between components in the second version of the UIT countermeasure model. This relation shows the communication pattern of components with each other. According to this version, there are three relations that connect between UITCM groups and components. These relations can be known as the relations of the components to risk analysis and security metrics, the relations between components to monitoring and auditing processes, and the relations among subgroups of UITCM.

I. Relations between Group of Components and Monitoring and Auditing Processes

In general, monitoring is normally focused on daily project management issues. Monitoring tries to assess whether activities are implemented effectively and efficiently (Olubode-Awosola et.al, 2008). According to (Binnendijik, 1999) monitoring focus mostly on whether or not results were achieved as planned or not.

In UITCM (Figure 4.9), the dash-dotted line in black colour -·-·-·-·-· shows the connection between groups of components and monitoring and auditing processes.

Organizations can monitor inbound and outbound communications traffic in their information systems with taking employees' privacy rights into consideration. Organizations can follow various methods to monitor employees' behaviour for

recognizing the potential indicators of concern, then conducting an information systems auditing. Monitoring and auditing activities involve collecting and analysing information and evaluating evidences. Monitoring/auditing processes are crucial element for ensure the achievement of the organization's' information security goals.

Therefore, UITCM proposed that all components of the model should be monitored and audited periodically, particularly those pertaining to technology, management, organizational culture, people, and job processes. The integration of all these actions enables a holistic information security management. Figure 4.9 shows that monitoring/auditing processes are connected to all groups of components in the model.

Security monitoring, sometimes referred to as "Security Information Monitoring (SIM)" or "Security Event Monitoring (SEM)," involves collecting and analysing information to detect suspicious behaviour or unauthorised system changes on organization's network, defining which types of behaviour should trigger alerts, and taking action on alerts as needed(Trost, 2011). Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions (Dempsey et.al.,2011). Monitoring is an on-going process usually directed by management to ensure processes are working as intended (Ruppert, 2005). Top management needs to monitor and control the job process that is specifically related to confidential data. Data flow, data classification, access control and job rotation are important processes used to identify the root cause of why things go wrong and how to correct them (Liginlal et.al, 2009). If user behaviour activities show abnormal behaviour compared to normal baseline behaviour, potential threats could occur. For example, when the logs history show the user login into system with abnormal from

actual, the user profiling method can be used to observe user behaviour and forecast possible threats (Millset.al.,2017). Incorporating psychosocial data (mental problem, espionage, and disgruntlement) along with the cyber data (user behaviour activities) into the behavioural analysis offers an additional dimension to assess potential threats (Greitzer & Hohimer, 2011).

Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, scanning tools, network monitoring software and CCTV). These devices are used to track the impact of security changes to the information system. There are technologies for error interception, such as artefacts that can be controlled by RFID tags to monitor delays in the workflow, can also track employee movements and help provide them access to secure locations. An example of RFID tags tracking employees can be an organization's basic attendance system. Usually, organization give each employee an ID badge and the use of CCTV, periodical audit and isolating the location of certain information assets are the practical solutions used to reduce lost computer equipment and disposal of documents (Liginlal et.al., 2009).

The granularity of the information collected is determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities. Organizations consult appropriate legal counsel with regard to all information system monitoring activities. Organizations heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information (Trost, 2011).

Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Monitoring devices are strategically deployed within the information system. Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs (Trost, 2011). To monitor employees' behaviour there are various methods can help recognize or infer potential indicators of concern. Some are surveillance methods (such as monitored electronic communications), while others require more intrusive testing and/or accessing of personnel records (including medical records in some cases). These methods should be identified with regard to possible legal constraints or boundaries, which must be considered.

In monitoring field, legal and ethical issues constitute a major topic that deserves more attention. Potential indicators that are measured using some type of psychological testing (e.g., tests assessing risk tolerance, personality traits) may be deemed mental health testing, which may be limited by the Acts and laws of the country. Monitoring electronic communications may implicate the Electronic Communication Privacy Act's protections, requiring an employer to obtain consent or fall within one of the law's exceptions (United States Code, 1964). Differential treatment based on gender, age, culture, or subculture may be limited by the Civil Rights Act or the Age Discrimination in Employment Act. Similarly, workplace drug testing is subject to the country legal restrictions (United States Code, 1967). Approaches to mitigation of insider threats must take privacy and ethical issues into

account (Kiser, 2010;Greitzer et.al., 2010). Privacy rights advocates seek to ensure that employees will not suffer unwanted intrusions and that potentially harmful information will not be acquired about them. On the other hand, to the employer, the cost and damage of one incident may warrant data monitoring, collection, and analysis. To alleviate adverse effects of monitoring, employers should communicate the reasons for electronic monitoring and find a balance between such monitoring and employee privacy. Disclosure of monitoring policies also may remove the expectation of privacy, from a legal perspective (Kiser, 2010). If the process is disclosed, explained, and managed equitably across employees, it may not be considered unfair by employees, and the mutual trust relationship required for a healthy organization may remain intact (Greitzer et.al, 2010).

Information system audit (IS audit) mainly refer to truly analytical part of IT Governance by which the level of IS performance and maturity can be measured and assessed. The information system auditing is conducted to evaluate the readiness level of organization in managing information technology (IT) (Mashour, & Zaatreh, 2008). The information systems auditing is the process of conducting analytical test and evaluating evidence to be determine in monitoring and evaluating computer system, maintain data integrity, achieve the organizational goals effectively, and use resources efficiently (Ron, 1999).

The organization employs automated tools to support near real-time analysis of events. Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems. Unusual/unauthorized activities or conditions related to information system inbound and outbound

communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or propagating among system components, the unauthorized exporting of information, or signalling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components (NIST, 2015). The information system monitors inbound and outbound communications traffic at organization-defined frequency for unusual or unauthorized activities or conditions. Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers. Anomalies within organizational information systems include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses. The organization analyses outbound communications traffic at the external boundary of the information system and selected organization-defined interior points within the system e.g., subnetworks and subsystems to discover anomalies (NIST, 2015). Indications of increased risk from individuals can be obtained from a variety of sources including, for example, human resource records, intelligence agencies, law enforcement organizations, and/or other credible sources. The monitoring of individuals is closely coordinated with management, legal, security, and human resources officials within organizations conducting such monitoring and complies with legislation, Executive

Orders, policies, directives, regulations, and standards, The organization implements organization-defined additional monitoring of individuals who have been identified as sources as posing an increased level of risk , privileged users and individuals during organization-defined probationary period (NIST,2015).

Figure 4.9 shows the relations between group of components and monitoring and auditing processes which discussed above.

II. Relations between Group of Components and Risk Analysis and Security Metrics

In UITCM (Figure 4.9), the dashed line in red - - - - - - - colour shows the connection between group of components and risk analysis and security metrics.

Risk analysis is the process of identifying and analysing potential issues that could negatively impact key business initiatives or projects. This process is done in order to help organizations avoid or mitigate those risks. Performing a risk analysis includes considering the possibility of adverse events caused by either natural processes, like severe storms, earthquakes or floods, or adverse events caused by malicious or inadvertent human activities. An important part of risk analysis is identifying the potential for harm from these events, as well as the likelihood that they will occur (Trost, 2011).

Security metrics are set of precepts and rules necessary for a real way to measure the security level of an organization; security metrics involve the application of a method of measurement to one or more entities of a system that possess an assessable security property to obtain a measured value. From an organizational perspective, security measures and metrics should enable an organization to gauge how well it is meeting its security objectives. Security metrics are tools to facilitate

decision making and to improve performance and accountability, to achieve the aim of information security which is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents (Trost, 2011).Pro-active security metrics are essential in information security management especially to aid decision-making on security management and risk assessment (Johnson & Goetz, 2007). The metrics aims to provide risk scores so that different groups within the organization can set security targets and help identify acceptable risk levels (Johnson & Goetz, 2007). Metrics are based on facts and quantifiable measurable information. The measurements are used to analyse organization's strengths, weakness' and possibilities and to track progress and compliance. Security metrics are used to measure whether or not an organization's security program is accomplishing goals and maintaining compliance. Security metrics determine what is and isn't working within an organization's information security framework so improvements can be made to policies, systems, or processes and any gaps in data security can be addressed. The metrics should be quantifiable and hold influence over behaviour and strategy. Hard numbers and benchmarks help avoid confusion and efficiently highlight areas for improvement (Trost, 2011). There is no hard metrics list all organizations should be tracking. Organizations can define their measurement criteria and carry out measurements themselves, based on the metrics that help organization understand its current security posture and identify any gaps. The metrics that organization chooses depend on organizations' needs (Trost, 2011).

The model of (Ismail & Yusof, 2019) excluded managerial, psychological and cultural components from undergoing processes of risk analysis and security metrics. In contrast, UITCM set all groups of components including managerial, psychological

and cultural groups to be linked to risk analysis and security metrics so that they can be monitored and audited periodically.

Most of the security metrics focused on technical aspects such as access requests, intrusion attempts, virus logs, and traffic information. This is because human behaviour is difficult to study, thus information system security violations are not readily observable or objectively measurable (Guo, et al, 2011).

It is possible to use the security metrics to assessment of employee behaviour. Since the job processes are related to human behaviour, psychology and technical support, the introduction of the security metrics is important to assessment of employee behaviour and integration of findings in security manage (Michelle, 2020).

Therefore, UITCM proposed that security metrics are not only related to technology, they are also related to human characters, including psychological issues. Security metrics in psychological field could be identified as follows:-

- The number of employees that have conducted (mental / drug / hormones / risk possibility) test.
- The number of times the tests are performed per year.
- Data on security incidents can be analysed to determine numbers of incidents (psychological field-related, work environment design-related, fatigue and sleepiness-related and employee mood-related).
- Questionnaires can used to measure employee satisfaction associated to work load, design of work environment and employee mood and the effects of these factors on employee performance and behaviour.

Regarding to cultural field, UITCM proposed that security metrics are not only related to technology, they are also related to cultural field. Creating security awareness programs and establishing best practices, must be accompanied by the

creation of metrics to gauge the effectiveness of such organizations wide effort. Many organizations implement security awareness measures, but do not know whether the measures have brought about a change in employees behaviour (Michelle, 2020).

Awareness of and compliance with security best practices throughout an organization can be measured with metrics, just as security technology metrics measure uptime and downtime, intrusion attempts, malware, and vulnerabilities. A study in Norway found that measuring this awareness can elevate security best practices within organizations, leading to fewer security incidents due to carelessness or neglect (Cisco, 2007).

Security metrics in cultural field could be identified as follows:-

• The number of employees that have completed a security training program and whether they understand the material or not.

• The number of breach and incidents notifications documented.

• The number of users who have administrative access.

• The time take data controllers to report personal data breaches after becoming aware of the incident.

• The frequency of security awareness training can be measured and the number of hits to a Webpage offering security best practices or video training as well.

• Employee satisfaction surveys can be done to know how aware they of security policies and procedures are.

• Data on security incidents can be analysed to determine how many employee-related incidents.

• Managers can submit ongoing reports with behavioural metrics that may include the frequency of passwords left exposed in work areas, failure to

activate a secure screensaver when an employee has left their desk, and other instances of lack of compliance with security policies.

- Security personnel can measure and report on the quantity and content of interactions with employees to see where vulnerabilities may exist.
- Customer, supplier, and partner surveys can solicit and measure feedback related to the organization's security controls (Cisco, 2007).

In addition to psychological and cultural fields, UITCM proposed that security metrics are also related to managerial domain. Organization regulations and standards require constant monitoring to effectively ensure compliance within the organization. That's why it's important to establish a list of security metrics to measure effectiveness and maintain compliance. Without a quantifiable security metric program in place Law and regulation, policy and, standards become more susceptible to violation, which can led to accidents happen (Maximilian et.al, 2018). Security metrics in managerial field could be identified as follows:-

- Number of incidents reported that related to policy and law violation.
- Data on security incidents can be analysed to determine how many policy and law violation-related incident.
- Questionnaires can used to know if organization employees understand the material of (Law & Regulation, Policy, Procedures, Standards, Best Practise, Baselines, and Standard Operating Procedure) that used in the organization.

Using security metrics in managerial, psychological and cultural fields enhances the processes of errors intercepting and avoiding mistakes and negligent actions. Figure 4.9 shows the relations between groups of components and risk analysis and security metrics which discussed above.

III. Relations between Groups in UITCM

The model was developed so that each group in the model is related to other groups. Groups are dependent and complement each other. In UITCM, the dotted line in blue colour ..... shows the connection between groups in UITCM. The relations among the groups of UITCM are described in (Appendix E) Table 4.

4.5 Step 3: Development of Final Version of UITCM

Development of Final version of UITCM was carried out in two phases:

Phase 1: evaluation of the initial (UITCM)/ Second Version by Delphi method round

Phase 2: evaluation of the (UITCM)/Revised Version by Delphi method round 2.

The activities conducted in the first phase include, selecting a group of experts based on special criteria then, sending the second version of the initial UITCM, with an open-ended questionnaire to evaluate the model. In phase two, the second version of the initial UITCM was revised based on the suggestions of experts in the first phase, then the revised version of the model was sent with a closed-ended questionnaire to evaluate the model.

Table 4. 22: (UITCM) / Final Version development activities

Input	Second Version of UIT Countermeasure Model (UITCM)
Process	Phase 1: Evaluation of the Second Version of (UITCM) by Delphi method round 1. Phase 2: Evaluation of the Revised Second Version of (UITCM) by Delphi method round 2.
Output	Final version of Unintentional Insider Threats Countermeasures Model (UITCM)/ The validated Version

4.5.1 Expert Validation and Expert Review

This study proposed the expert review process to evaluate the proposed conceptual model .An expert review is a process asking the opinions, suggestions,

feedback or comments from experts on new developed works, such as evaluation of questionnaires, frameworks, and its contents, appropriateness of wording and terminology of items. (Ramirez, 2002).The expert validation is one of the methods that can be utilize to validate the propose model and it is a significant way to improve the quality of the work (Aziz et al., 2015; Bocconi et al., 2007).

4.5.1.1 Selection of Experts

In this study, a group of expert were chosen to look at different aspects of validation and reviewing the UITCM. The experts were selected based on their experience in the study area to represent both the theorists (academicians) and professionals (practitioners).

The identified experts, from Malaysia and the Middle East, were chosen due to their credibility and knowledge in unintentional insider threats. The invitations were sent to the identified experts through email. Out of the 9 experts, 5 accepted to join. This number of the experts is sufficient as supported by (Chang et.al, 2012).

These five experts represent different fields of expertise from different international and local academic institutions and cybersecurity industry. This is important for this study to have established suggestions and comments.

The experts' panel consisted of five experts in the study area. The profile of the experts' panel is shown in Table 4.23.

Table 4. 23: Profile of Experts

Traits	**Values**
Gender	100% Male
Country	60 % Malaysian - 40% International
Work experience	19-32 Years
Role	60% Practitioner - 40%Academic

Besides this profile, demographic data about these experts was also obtained. The demographic information has been tabulated in Table 4.23. See samples of expert response via email (Appendix G)

Table 4. 24: Participants' Information.

Expert	Gender	Country	Position /Affiliations	Work experience
A	Male	Malaysia	Senior Lecturer, Department of System & Computer Communication, Faculty of Information & Communication Technology, Universiti Teknikal Malaysia Melaka.	20 Years
B	Male	Jordan	Senior Lecturer, Senior Lecturer. Faculty of Huson.Al-Balqa Applied University.	21 Years
C	Male	Malaysia	Senior Vice President. Government & Multilateral Engagement.CyberSecurity Malaysia.	32 Years
D	Male	Malaysia	Deputy Manager - EPF Malaysia –KWSP. Employees Provident Fund Technology Risk & Analytics.Risk Management Department.	22 Years
E	Male	Saudi Arabia	Project management consultant Information Technology Agency at the Ministry of Health.	19 Years

This research study adopted the Delphi method to achieve the experts' evaluation procedure. The Delphi method is a technique to get experts' feedback, harnessing and organizing judgment, particularly in problems that are complex and require intuitive interpretation of evidence or informed guesswork. Delphi has been used in a wide variety of research areas and most studies use only two or three rounds (WIlliams & Webb,1994).

Accordingly, in this work, a two-round questionnaire was developed. The purpose of first round is to review the design of the proposed model and getting the experts' comments on the suitability of the components, while the purpose of second round is to proof the expert consensus on the updated version of the model based on previous comments and suggestions in the first round.

The group of experts was asked to review the UITCM by two-round questionnaire. The questions of round one were open-ended while the questions of round two were close-ended. Thus, the results of the two rounds were qualitative and quantitative respectively. The validation process was done on-line (electronic mail) with two attachments, questionnaire and model. The experts were invited to participate in the model evaluation through email. The appropriate time (1-2 months) were given to the experts to see the proposed model so they can give more suggestions or comments about how to improve the initial version. The experts were focused on the reviewing the main and sub-components of the UITCM.

In the first round, an open-ended questionnaire was circulated to the panel of experts, to obtain specific information about the proposed model and to increase the richness of input for the model. The responses to the open-ended questions were analysed qualitatively by content analysis technique; sorting, categorizing and searching for common themes to identify the key points resulted from the first round of the questionnaire. These responses were summarized and then used to construct the second questionnaire and to improve the proposed model.

In the second round, the questions were asked in a way that leads to either a positive consensus or negative consensus on the proposed model in order to get stability. The second round was more specific by employing close-ended questions. The questionnaire adopted the rating or ranking techniques. The researcher used the first round results as a base to the second round questionnaire and converted the open-ended questions of the first round into close-ended questions for the second round to reaching to a consensus of opinion. Then the results were analysed using quantitative methods by calculating the mean of the experts' answers for each question. Finally, the final version of UITCM was presented.

A three-point Likert scale was used to measure the extent of agreement on the suitability of the UITCM components. The scale range consists of 3 points which are; not relevant (1), relevant (2) and strongly relevant (3). While a two-point Likert scale was used to measure the extent of agreement on the usability of UITCM and the extent of agreement on the readability and understandability of UITCM. The scale range consists of two points which are; yes (1), and no (2).

In a Delphi technique, experts must know the results of the previous rounds, till reaching consensus of opinions or stability of results. Since the main objective of the Delphi study is to obtain consensus, it is important to firstly define the concept of consensus. A consensus is in essence, a general agreement, an unanimity, the majority of opinion of a determined group.

(Gallotta et al; 2016; Filyushkina, et al, 2018) consider different types of majority, such as greater than one half (more than 50%), three fifths (60%), two thirds (66%) and three quarters (75%). Therefore, any question with a score of acceptance higher than 75% was considered as a consensus. If expert agreement percentage in Delphi is 75%, that means, more than 75% of participants agreed with the proposed postulates. For this study 75% was chosen as a threshold of agreement on each item in the proposed model (Christie & Barela, 2005; Tigelaar et.al, 2016).

Accordingly, consensus is reached in Round 2 if at least 75% of participants rate the suitability of each components of the UITCM at 2 or greater (relevant or strongly relevant), and if 75% of them rate the usability of UITCM and the readability and understandability of UITCM at 1 as Yes.

4.5.1.2 Expert Questionnaire

This study adopted complete approach to validate the proposed model, by evaluate its suitability and usability from three high level aspects including ,first, if

the model is theoretically valid that is, whether the model is logical consistent with the basic theories of UIT countermeasures. Second, the model is evaluated in terms of usability, that is, whether the model can be used in an intended exact setting by organizations. Finally, the model is evaluated in terms of readability and understandability, that is, whether the model is clear and understood by organizations.

In the evaluation procedure of the proposed model, all experts were asked to check the proposed model and then answer the required questions.

In the first round, a set of open questions were provided, to get feedback about the design, usefulness and understanding of the UITCM components. The experts were asked to provide qualitative feedback on the UITCM components. There were four sections provided for the experts to answer.

The first section in round one of the questionnaire contains demographic information of the respondents, namely, gender, position and total years of working experience.

In sections two, three and four the experts were asked to assess content validity including:

1) Section Two: Theoretical validity.

In this section the aim of the open questions were asking the responders about whether they thought that any important component was missing and whether they thought any component should be removed or improved. They were asked to suggest what is missing to be added. Further, experts were asked whether they had other comments.

2) Section Three: Usability.

The experts were asked whether the proposed model can be used in the organizations, and how can it be used. The experts were asked whether the model is useful to the

organizations or not. The experts were urged to address their additional remarks in the given instrument.

3) Section Four: Readability and Understandability.

This section was designed to get the experts suggestions on the design of the model. The asked questions in this section were about whether the participants understand the proposed components, terms used in the model, connections and flows of all components. The participants were asked whether the relationships between components of the model are logical, and whether the model is readable, understandable. Moreover, participants were asked their opinion and suggestions to improve the content.

Based on the analysis results of the first round of Delphi method, the UITCM were revised and improved. Then, the second round of the questionnaire was sent.

In the second round, a set of closed questions were provided, with two or three options to select from. There were three sections provided for the experts in round 2:

1) Theoretical Validity: this section shows a list of the revised UITCM components. The UITCM components are shown in a table with three rating scales to rate the relevancy of the components. The experts were asked to rate the relevancy of the model components from scores 1 to 3 with "Not Relevant, Relevant and Strongly Relevant". The questions focus on the relevance of the proposed components been included in the conceptual model.

2) Usability: The goal of this section was to review the usability of the model. The experts were asked whether the model can be used and adopted in organizations with providing of two choices (Yes and No).

Based on the experts' suggestions in the first round to how the model can be used, they were asked if they agree or not, through two options (Yes and No).

3) Readability and Understandability: In this section the experts were asked whether the terms used are clear and easy to understand, by two options (Yes and No). The experts were asked whether the connections and flows of all components are logical, by two options (Yes and No) as well. In addition, (Yes and No) question was used to ask whether the design of model is readable.

The first and the second rounds of the validation questionnaire are shown in Appendix F.

4.5.1.3 Results of Round I Delphi Method

After the data has been collected, qualitative analysis was used to summarize the experts' feedback. Understanding and categorizing the experts' suggestions was an essential step to improve the model and develop round 2 of the questionnaires.

There were key comments and suggestions raised by the experts. Table 4.25 shows the experts' comments and suggestions provided according to three criteria (Theoretical Validity, Usability and Readability and Understandability).

Table 4. 25: The comment /suggestion of the experts

Expert	Theoretical validity	Usability	Readability and Understandability
A	- More concern on an insider threats such as originate from phishing activity because most of an insider threats are driven from phishing activity.	-This is depending on the nature of an industry itself. For example, healthcare sector is not similar as manufacturing and many more. Justification is needed, and highlight on which industry such solution can be applied.	- The connections and flows of all the components of the model are acceptable and the terms used in the model are Clear. -The proposed model is readable and easy to understand. When deal with an insider threats, one of the major concern are relate to three component such as (machine, human and, system processes). In this model, all three components are exist and covered.
B	-IQ testing: Adding IQ testing separate from mental problems testing can improve psychological evaluation and monitoring. -Ethical hacking: Ethical hacking can be added improve employee response to different types of security. -Trust model: Can be improved by adding permission authentication from higher level employee. -Drug testing: Must be described clearly to distinguish between legal and illegal drugs. Also it must be related to a good health insurance system that manages drug usage.	- The model can be used in organizations that deal with confidential information related to their type of work or employee.	- The terms used in the model are clear an easy to understand. Abbreviations can be added to some known terms like user system interface etc. - The relationships between the model components logical. But the source and destination of the relation arrows are not clear. - The model is readable and understood easily.
C	-ISO / IEC 27001: The ISO/ IEC 27001 Information Security Management System is a standard for information security that is highly considered in any Cybersecurity policies and guidelines. This standard must be mentioned in this model.	-The model can be used as a guide to all the employees of the organization in being safe online. Awareness sessions need to be conducted to educate the entire organization about the	-To be use in an organization, the terms used must be less technical and less specific. The model will be used by all level of the organization. Using highly technical terminology, jargon, and acronym will provide difficulties for the management to understand thus rendering the model to be ineffective. Information security in an organization is a top-down approach, thus if the management do not have a full understanding, the

	-ISO/IEC15408: This is the Common Criteria Standard with regards to certified security function of the ICT product. One of the way for organization to minimize cyber threats is to procure Common Criteria certified ICT products. -Use generic terms: This is a model that will be referred by various parties thus a generic and easily understood terms are vital. Refer to the comments on the diagram; the Process has some proposed generic terms to be used that are more suitable for a model (Use the proposed terms). -Under the Human factor: add the element of Capability & Capacity This aspect is about having the right people with the skills who know how to be safe online. This includes having the necessary training and awareness on managing online information. -Incident response: This element is about responding to cyber incidents where there is a need to establish a team of information security professionals i.e. CERT team. The team will provide advisories of potential threats or on how to mitigate threats being faced by the organization. There is a need for a command-and-control centre or a security operation centre.	content of the model.	message will not get through. - Difficult to read and understand. Use less technical and specific terminologies and change it to generic and management terms. - Use less flow lines and connections.
D	-It is necessary to focus on fishing. -All employees' activities need to be monitored by a higher level employee.	-The model can be used as guidelines in Malaysian organizations.	-The terms used, relationships, and flows are clear and easy to understand.
E	-All application software and operating systems should be updated regularly.	- The current model could serve as guidance for creating a	- The terms are in general clear and easy to understand, at least for

	Network is vulnerable when programs aren't patched and updated regularly. There are applications that can regularly check to ensure all programs are patched and up to date to strengthen networks before attacks happen. -Regular vulnerability scans. To identify potential weaknesses in system configurations. -Default settings. It's possible for default settings to open the way for cyber attacks. While these settings might promote operational efficiency, they can prove dangerous for system. I recommend turning off legacy settings when possible. - Incident response plan. It is unacceptable to wait till an incident occurred. Incidents response plan should be ready when needed. - The Cognitive Reflection Test (CRT).Users with higher Cognitive Reflection Test (CRT) scores in comparison to lower CRT scores are, more likely to be phishing' victims perhaps due to their curiosity. So they should be aware.	checklist that could help organisations assess the status of their UIT mitigation measures. Organizations would still need further advice on the measures that are appropriate in their specific situation. Without such further advice, a checklist will have little impact on the actual resilience to UITs. In this respect, the model is similar to security management standards like those from the ISO 27000 series.	someone with a background in information security.

A sample of experts' response (Round 1) is shown in Appendix H. The experts' suggestions were achieved as following:

A. Theoretical Validity.

Regarding the comments of experts in the section of (Theoretical validity).Expert A suggested that the model should involves more concern on an insider threats that originate from phishing activity because a lot of an insider threats are driven from phishing activity. This is consistent with study by (CERT, 2014). A survey of literature on phishing countermeasures was achieved and a comparison to what is already in the model, and then more phishing countermeasures were added in different groups in both the diagram of the model and in the table of components' description. One of the experts (B) also pointed out his suggestions separating IQ testing from mental problems testing to improve psychological evaluation and monitoring. The separating was done in the Psychological group in both the diagram and in the diagram of the model and in the table of components' description.

The second suggestion by expert B that ethical hacking can be added improve employee response to different types of security which is consistent with study of (Pandey,et al,2015).Ethical hacking was added in Monitoring group in both the model diagram and in the description table .

The third suggestion by expert B that trust model can be improved by adding permission authentication from higher level employee .The importance of obtaining permission from a higher level has been raised by a study of (Kont et al,2018). This suggestion was achieved in Behaviour group in both the diagram of the model and in the description table.

In addition, expert B suggested clearly distinguishing between legal and illegal drugs in Drug testing component. The researcher has done in Psychological group in the description table of the model components.

Considering comments from Expert C that ISO / IEC 27001 and ISO/IEC15408 must be mentioned in the model because they are highly considered in any Cybersecurity policies and guidelines .Some studies such as (Siregar,2014), (Hoang & Pham 2018), emphasized the importance of these two standards in information security. The standards were added in the description table of model components within (Law & regulation, policy enforcement, procedure, standard, best practices, baseline, and Standard Operating Procedure).

Another suggestion from expert C, adding incident logs, advisories and command and control centre in Incident response group due to its big role in UITs mitigation. Witch was raised by (Creasey & Glover, 2013). These three components were added to Process group not to Incident response group because this group is under automated tools while the three components are not automated tools. They are shown in the model diagram and in the description table.

Managerial group name was changed to Governance based on expert C suggestion. On the other hand, the explanation has been provided to expert C regarding to his suggestions for moving, incorporating or changing some components or groups, which were not implemented due to its inappropriateness. Also, the explanation has been provided to him regarding to his suggestion for adding some components that already in the model.

Expert D agreed with expert A on the need to focus on the threats arising from phishing. In line with the study of (Kont et al,2018) , expert D also pointed out the necessity of obtaining permission from a higher-level employee in all employee

critical activities .This point was added within the description of the effective security practices in the description table.

About the comments from expert E. He indicated to keeping all application software and operating systems updated regularly , which was recommended by (Vaniea & Rashidi,2016) and turning off default setting which was recommended by (Kraus et al ,2010) to enhance the system Defenceagainst cyber- attacks. These two remarks have been included within the description of the Effective security practices in the description table of the model components.

Performing regular vulnerability scans and developing incident response plan were subtracted by expert E, that were recommended by (Sommestad ,et al,2011) and (DeVoe & Rahman,2015).The study took this remarks into account and they were inserted in Monitoring group in both the model diagram and in the description table.

In the last comments from expert E regarding to theoretical validity section. He suggested adding The Cognitive Reflection Test (CRT) ,as users with higher (CRT) scores in comparison to lower CRT scores are, more likely to be phishing' victims.

This is consistent with study by (Kumaraguru et al.2007). This suggestion was added in Psychological group in the both diagram and description table.

B. Usability

About the comments on the usability of the proposed model. All the experts agreed that the model can be used in organizations particularly Malaysian as a guidelines and a checklist that help organizations assess the status of their UIT mitigation measures. In addition it can be used to guide all the employees of the organization in being safe online.

However expert A commented that justification is needed, and highlighting on which industry the model can be applied. Expert B comment has highlighted on which organizations the model can be applied. He stated that the model can be used in organizations that deal with confidential information related to their type of work or employee. Expert C recommended conducting awareness sessions to educate the entire organization about the content of the model.

C. Readability and Understandability

As for the experts' remarks on the readability and understandability. The majority of the experts agreed that the proposed model is readable and easy to understand. The connections, relationships and flows of all the components of the model are acceptable and logical and the terms used in the model are clear. Expert A stated that the three major concerns of UITs which are machine, human and system processes were exist and covered in the model. Expert B recommended clarifying the source and destination of the relation arrows in the diagram and adding abbreviations to some known terms to enhance the model understandability. The model flows and connections were clarified by adding the arrows. Abbreviations were added. Expert C disagreed that the model was clear enough and suggested using less technical and specific terminologies and changing them to generic and management terms, so that the model can be use by all level of the organization. The idea was accepted and taken in consideration when improving the model.

In addition, expert C stated that using acronyms will provide difficulties for the management to understand and suggested using less flow lines and connections. Improvements were made by reducing the flows and incorporating the relations between the model components.

A table of abbreviations was created to clarify the acronyms used in the model.

4.5.1.4 Results of Round II Delphi Method

Based on the qualitative analysis of round 1 result, the model has been refined and improved. The revised model is shown in Figure 4.13 with the description of components and relations in Table 1, Table 2, Table 3, Table 4 and Table 5 (APPENDIX I).

After revising the model, the second round was continued. The questionnaire for the second round was distributed. Then the results of the second round were quantitatively analysed. The gathered data were recorded in tables based on the questions asked in the instrument.

The mean of the experts' answers was calculated in each question to determine whether the results of round two were stable. The results have been shown as charts to illustrate the different frequency of responses.

In order to investigate the stability of the experts' answers, regarding to the theoretical validity of the model. The components of the model were listed in a table with its IDs as shown in Table 4.41. Then the mean of the experts' answers for the relevancy of each one of the components was calculated as shown in Table 4.42.

A sample of experts' response (Round 2) is shown in appendix H.

Table 4. 26: The proposed components of UITCM with its IDs

ID	Element
OC01	Law and Regulation, Policy Enforcement, Procedure, Standard, Best Practice, Baseline, Standard Operating Procedure (SOP), Guidelines.
OC02	Maintain Employee Readiness.
OC03	Improve Data Flow.

OC04	Effective Security Practices.
OC05	Maintain Staff Values.
OC06	Improve Design of User-System Interface (UI).
OC07	Affordable Access to Mental Health/Drug Treatment Services.
OC08	Appropriate Time Off For Employees.
OC09	Team-building Activities.
OC10	Improve Design of Work Environment.
OC11	Improve Work Planning and Control.
OC12	Improve Work Setting and Management Practices.
OC13	Command And Control Centre.
OC14	Incident Logs.
OC15	Advisories.
OC16	Risk Analysis And Auditing.
OC17	Incident-driven Reviews (Policies, Practices, Training Materials).
OC18	Periodically, Fully Re-evaluate Risk.
OC19	Ethical Hacking.
OC20	Regular Vulnerability Scans.
OC21	Developing Incident Response Plan.
HC01	Monitor Employee Behaviour.
HC02	Trust model With Permission Authentication From Higher Level Employee.
HC03	Collaborative Reinforcement Model.
HC04	Mental and IQ Test.
HC05	Drug Testing.
HC06	The Cognitive Reflection Test (CRT).
HC07	Stimulation Of Risk Perception.
HC08	Security Education, Training, Awareness, Instrumental Conditioning.
HC09	Usability of Software /Security Tools.
HC10	Encourage Following of Policies.
HC11	Employee Assistance Programs (EAPs).
HC12	Respectful And Calm Workplace Environments.
AC01	Watermarking Forensic, Intelligence Operation.

AC02	Backup Systems (Spatial /Temporal) Replication.
AC03	Remote Memory Wipe For Lost Equipment.
AC04	Automation.
AC05	Data Encryption/Password Protection.
AC06	Wireless And Bluetooth Safeguards.
AC07	Standard Systems/Email Safeguards (anti-phishing, anti-malware etc), prevention system (IDS/IPS,DLP), Firewalls, APT Prevention, Accesses Control, Static And Dynamic Software Code Checkers, Data Classification, IAM, Website Controls.
AC08	Security Information Event Management (SIEM) Systems, Software to Recognize Bogus Emails, EDR, UEBA, CCTV, RFID.

Table 4. 27: Experts' answers on relevancy of the proposed components of the UITCM

Element ID	Expert A	Expert B	Expert C	Expert D	Expert E	Mean
OC01	3	2	3	3	3	2.8
OC02	3	2	3	2	3	2.6
OC03	3	3	2	2	3	2.6
OC04	3	3	3	3	3	3
OC05	3	3	2	2	3	2.6
OC06	3	3	2	2	3	2.6
OC07	3	2	1	2	3	2.2
OC08	3	2	1	2	3	2.2
OC09	3	2	2	2	3	2.4
OC10	3	3	1	2	3	2.4
OC11	3	3	2	2	3	2.6
OC12	3	3	2	2	3	2.6
OC13	3	3	3	2	3	2.8
OC14	3	3	3	2	3	2.8
OC15	3	2	2	2	3	2.4
OC16	3	3	3	2	3	2.8
OC17	3	3	2	3	3	2.8
OC18	3	3	3	3	3	3

OC19	3	2	2	2	3	2.4
OC20	3	2	2	3	3	2.6
OC21	3	3	2	3	3	2.8
HC01	3	3	2	2	3	2.6
HC02	3	3	2	3	3	2.8
HC03	3	2	2	2	3	2.4
HC04	3	3	2	2	3	2.6
HC05	3	2	1	2	3	2.2
HC06	3	3	2	2	3	2.6
HC07	3	3	2	2	3	2.6
HC08	3	3	3	3	3	3
HC09	3	3	2	3	3	2.8
HC10	3	3	3	2	3	2.8
HC11	3	2	2	2	3	2.4
HC12	3	2	1	2	3	2.2
AC01	3	3	2	2	3	2.6
AC02	3	2	2	2	3	2.4
AC03	3	3	2	2	3	2.6
AC04	3	3	2	2	3	2.6
AC05	3	3	2	3	3	2.8
AC06	3	3	2	2	3	2.6
AC07	3	3	2	3	3	2.8
AC08	3	3	2	2	3	2.6

Not Relevant = 1; Relevant = 2; Strongly relevant = 3

Table 4.27 shows the results of Delphi study round two regarding relevancy of the model components. According to the literature, consensus is reached, and the results are stable if at least 75% of participants choose 2 or greater in a three-point Likert scale questions, then the Delphi tours are stopped. To calculate threshold of the mean of the participants' answers using a three-point Likert scale.

75/100×3 =2.2 (Christie & Barela, 2005; Tigelaar et.al, 2016).

Accordingly, this study determined 2.2 as a minimum percentage of agreement based on the three-choice questions. The results of round two were stable, where each of the components scored 2.2 or above, which mean 75% of agreement on the relevancy of the components. Therefore, there is no need to do a third round.

From Table 4.27 results of round two were stable, where each of the components scored 2.2 or above, which mean 75% of agreement on the relevancy of the components. Therefore, there is no need to do a third round. From the table (which table), it can be seen that the all components has been evaluated as relevant or strongly relevant by all experts except expert C who has evaluated five of the model components as not relevant which are, affordable access to mental health/drug treatment services, appropriate time off for employees, improve design of work environment, drug testing and respectful and calm workplace environments. The experts' agreement on the relevancy of the components can be clearly seen in the Figure 4.10 it can be seen that the all components has been evaluated as relevant or strongly relevant by all experts except expert C who has evaluated five of the model components as not relevant which are, affordable access to mental health/drug treatment services, appropriate time off for employees, improve design of work environment, drug testing and respectful and calm workplace environments.

The experts' agreement on the relevancy of the components can be clearly seen in the Figure 4.10.

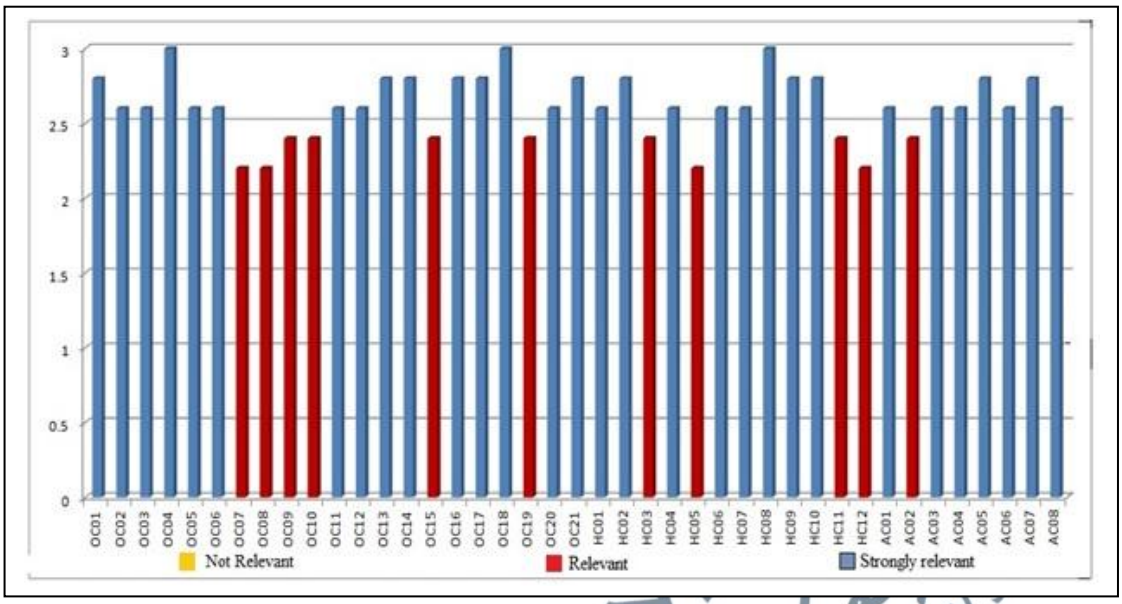

Figure 4. 10: Relevancy of the proposed components of the UITCM

According to the literature, consensus is reached, and the results are stable if at least 75% of participants choose Yes (1) in a two-point Likert scale questions, then the Delphi tours are stopped. To calculate threshold of the mean of the participants' answers using a two-point Likert scale.

75/100×2=1.5 (Christie & Barela, 2005; Tigelaar et.al, 2016).

Accordingly, this study determined 1.5 as a minimum percentage of agreement based on the two-choice questions that were used to measure the usability, readability and understandability of UITCM. That means 75% of participants rate the usability of UITCM and the readability and understandability of UITCM at 1 as Yes.For testing the usability of the model, the questions that asked to the experts were listed in Table 4.28 with its IDs and the means of the experts' answers are shown in Table 4.29

Table 4. 28: Usability Questions with its IDs

Question	ID
The model can be used and adopted in organizations.	U01
The model can be used in organizations that deal with confidential information. It can be used as a guidelines and a checklist that help organizations assess the status of their UIT mitigation measures. In addition it can be used to guide all the employees of the organization in being safe online.	U02

As exhibited in Table 4.28 and Figure 4.11. All of the experts agree that the model the model can be used in the Malaysian organizations.

Moreover, all of the experts agree that the model can be used in organizations that deal with confidential information. It can be used as a guidelines and a checklist that help organizations assess the status of their UIT mitigation measures and it can be used to guide all the employees of the organization in being safe online.

From the above we can note the results' stability of round two on the usability of the model.

Table 4. 29: Results of usability of the UITCM

Question ID	Expert A	Expert B	Expert C	Expert D	Expert E	Mean
U01	1	1	1	1	1	1
U02	1	1	1	1	1	1

Yes = 1; No = 2

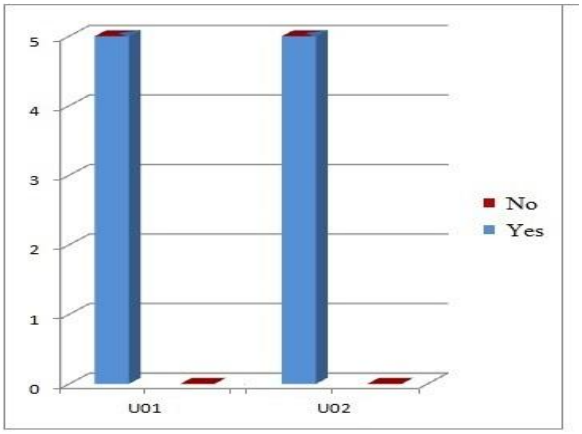

Figure 4. 11: Usability of UITCM in organization

Finally, to measure the experts' agreement on the readability and understandability of the model, the questions asked were listed with its IDs and then the mean of each question was calculated as shown in Tables 4.30 and 4.31.

Table 4. 30: The readability and understandability questions with its IDs

Question	ID
The terms used are clear and easy to understand.	R01
The connections and flows of all of the components are logical.	R02
Overall, the conceptual design model is readable	R03

Table 4. 31: Results of readability and understandability of the UITCM

Question ID	Expert A	Expert B	Expert C	Expert D	Expert E	Mean
R01	1	1	1	1	1	1
R02	1	1	1	1	1	1
R03	1	1	1	1	1	1

Yes = 1 No = 2

The results of round two were stable, where each of the questions scored more than 1.5. Based on that, the researcher decided to stop at round two. All of the experts agree that the terms used in the model are clear and easy to understand, the connections and flows of all of the components are logical and the conceptual design model is readable. Figure 4.12 illustrates the results of the readability and understandability of the model.

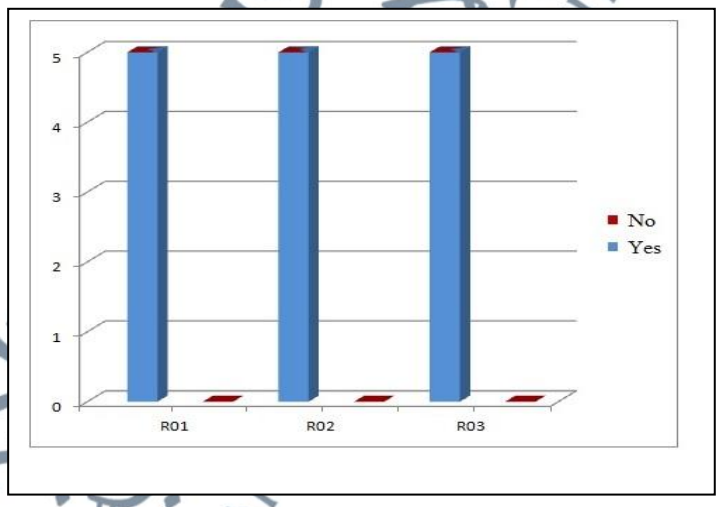

Figure 4. 12: Understanding of the terms, flows, connections, and readability of the UITCM.

The validated conceptual model is shown in Figure 4.14 with the description of components in Table 1, Table 2 ,Table 3 , Table 4 and Table 5(APPENDIX I).

The modifications have been added in both the model diagram and the model components description tables. The modifications in the model and description tables have been colored in different colors to be clear and to see what is new.

- Modifications according to expert A comments are colored red.
- Modifications according to expert B in blue.
- Modifications according to expert C in green.
- Modifications according to expert D in yellow.
- Modifications according to expert E in brown.
- In the case that two experts have the same comments, they are colored in grey.

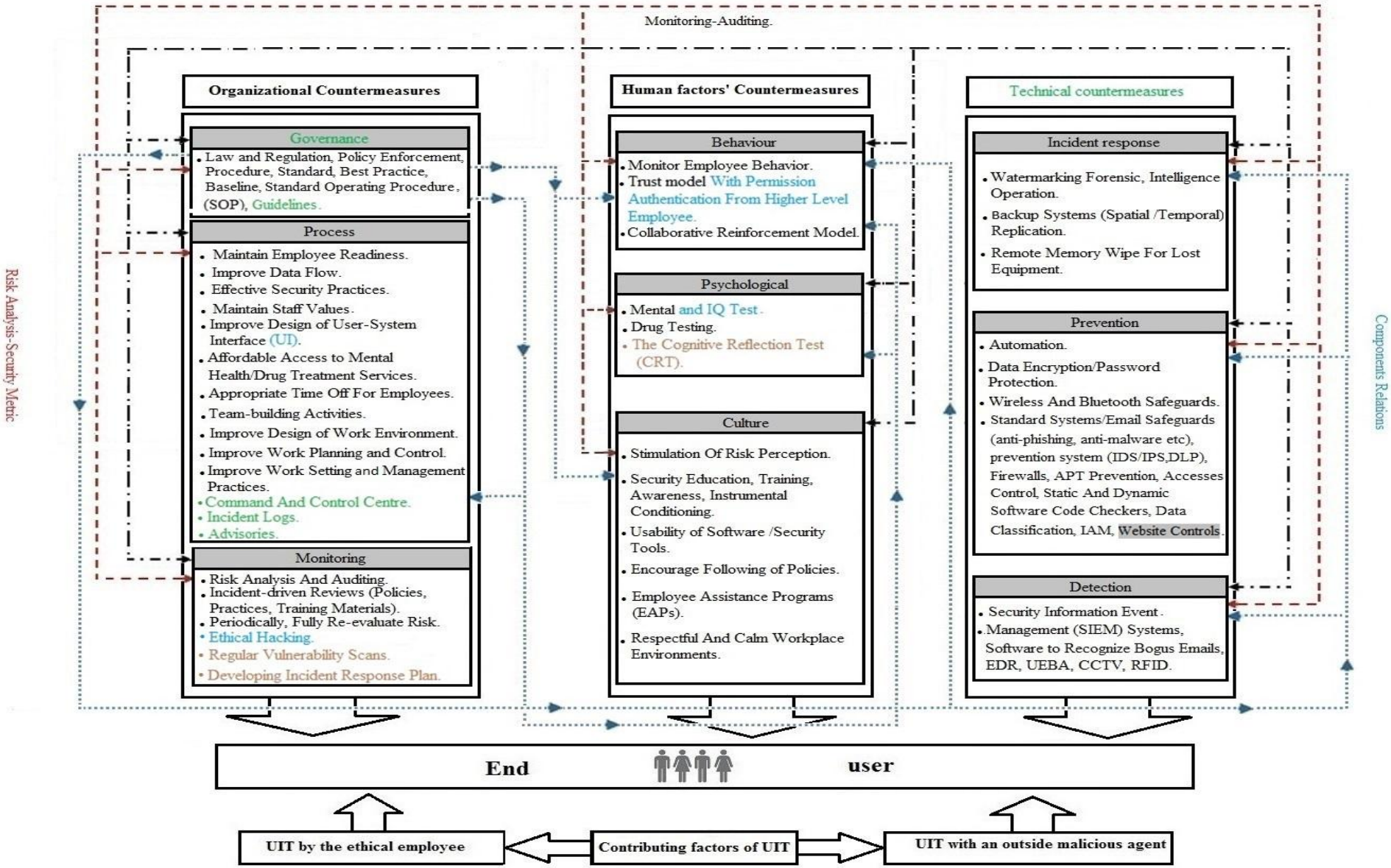

Figure 4. 13: The Final Version of unintentional insider threats countermeasures model (UITCM)/ Validated Model

Expert's validation was chosen as evaluation method to the proposed model because this method provides useful feedback on the quality of developed model and a way to elicit expert's knowledge (Inglis, 2008). With using expert intuition to validate a model will not need revision it in a future study (Coombes, 2001). This study has adopted expert's validation as the most appropriate method to determine the suitability and usability of the proposed model to be used in organizations as cannot evaluate the suitability and usability of the model without the accumulated experience. Suitability means theoretical validity that is, whether the model is logical consistent with the basic theories of model purpose. While usability means; Is the model able to be used, how to use it and Is it useful, in addition to the understandability of the model (Rouly et al., 2014).

The outcomes of the validation process show that the expert's panel acknowledged that the proposed factors included in proposed conceptual model are relevant also they acknowledged that the proposed model includes logical connections, flows, and reasonable terms and it is understandable. However, wit was concluding based on the expert review that the UITCM can be used and adopted in organizations. All experts acknowledged that the model can be used in organizations that deal with confidential information as a guidelines and a checklist that help organizations assess the status of their UIT mitigation measures. In addition it can be used to guide all the employees of the organization in being safe online. Thus, the validation process proved that the model is valid from three main aspect, theoretical validity, usability and readability and understandability.

4.6 Summary

This chapter addressed the development of the (UITCM) in its' initial and second version and the proposed components and relations in the (UITCM). The initial version of UITCM was developed based on the literature review of existing countermeasure models. The (UITCM) has proposed mitigation approaches in three domains which namely organizational, human factors and automated defence tools countermeasures.

Then this chapter discussed the development of the second version of UITCM which conducted based on a survey towards IT Executives of Malaysian SMEs. The results of the reliability and validity tests of the pilot and actual study in this work revealed that the questionnaire was reliable and valid. Furthermore, the questions were consistent. As a summary of these study results, 67% of the participants believed that their organizations were likely to confront UITs while 33% were not likely to have faced UITs. In light of this study results, it could be said that majority of the SME's selected were confronted with this type of threats. This study work concluded that the most contributing factors in UITs in Malaysian organizations are ignorance and negligence (27%), situation awareness (26%) and human error (22%)' respectively.

The importance of this survey is to confirm the need for the proposed model by determining the UITs likelihood level. In addition, this survey discovered the most contributing factors of UITs which were emphasized in the model development stage. Where, additional concern was given to the countermeasures of these factors to ensure covering them.

The second version of UITCM extends and combines the ideas of the existing models of UITs countermeasures. Most of the ideas are used as the basis in constructing the proposed model because a combination of these solutions together

creates a comprehensive defence strategy. However, it has to be stressed that the content of the second version of UITCM is different with the existing models that are missing some important aspects, because it addresses all aspects of human error problems, through a layered defence strategy consisting of policies, procedures, training and technical controls, in addition to protective measures at multiple stages before, during and after the attack. Moreover, the second version of UITCM proposed that security metrics are not only related to technology, they are also associated to managerial, psychological and cultural domains which should be monitored and audited periodically.

In the demonstration stage of the development, the comparison of the second version of UITCM with the contributing factors of UITs proved that it's managed to cover all contributing factors of UITs. However, the comparison shows that none of the existing models and strategies has covered all contributing factors of UITs and they focused on specific aspects of UITs countermeasures.

This study has chosen expert's validation as evaluation method. A Delphi method was used to find out whether the experts could reach consensus on the proposed model. After two rounds, the Delphi results were stable. The results indicate that the experts have reach consensus of mean scores more than 75% on the theoretical validity, usability and readability and understandability of the model.