CHAPTER IV : RESULT AND DICUSSION

4.1 Introduction

This chapter explained the findings obtained based on the research questionnaire and in depth semi-structure interview. The main focus of the study referred to the data generated from the questionnaire for verification of the framework. All the data gathered are analyzed using *Statistical Package For The Social Sciences (SPSS), Version 22 For Windows*. For each research question are discussed in the discussion parts consisted descriptive statistics and statistical test.

Then, for validating the framework, the data gathered from depth semi-structure interview in qualitative approach are analyzed by using SPSS and content analysis. The results of all data analysis in this study will discuss in this chapter 4.

4.2 Response Rate and missing data

In this research, about 272 questionnaires has been distributed to IT experts and the respondents answered all questionnaires. The respondents used for further analysis was 272 according to Krejcie and Morgan table based on the population of 600.

Table 4.1: Survey Response Rate

Survey Return Rate		
	N	Return Rate Percentage
Questionnaire Distributed	600	100%
Usable Questionnaire Collected	272	45.3%
Unable Questionnaire	-	0%

4.3 Demographic profile of respondents

Table 4.2 shows the distribution of company profile. It consisted by university category, full time employees and key stakeholders comprised of 272 respondents. Based on university category showed 64 respondents (23.5%) are research category, 62 respondents (22.8%) are comprehensive university and 146 respondents (53.7%) are technical university. It showed that the highest are technical university and the lowest are comprehensive university.

Then the full time employees showed the majority of the respondents are more than 2000 employees with 134 respondents (49.3%) and followed by between 1001 to 2000 employees with 133 respondents (48.9%). Then the respondents who are between 101 to 500 and between 501 to 1000 are 2 respondents or 0.7%. While the minority of the respondents less than 100 with 1 respondent (0.4%).

Moreover, referring to the key stakeholders showed 149 respondents (54.8%) are CIO or CTO, IT Director with 116 respondents (42.6%), IT Manager are 5 respondents (1.8%) and other key stakeholders are 2 respondents (0.7%). This represented the highest number of respondents are CIO or CTO and the lowest are others key stakeholders.

Table 4.2: Company Profile

Company Profile	Frequency	Percentage
University Category		
Research University	64	23.5
Comprehensive University	62	22.8
Technical University	146	53.7
Full Time Employees		
Less than 100	1	0.4
101-500	2	0.7
501-1000	2	0.7
1001-2000	133	48.9
2000+	134	49.3
Key Stakeholders		
CIO or CTO	149	54.8
IT Director	116	42.6
IT Manager	5	1.8
Others	2	0.7

Table 4.3 below shows the distribution of profile interviewee. Based on job title showed 10 respondents (3.7%) are IT Director/Manager, 2 respondents (0.7%) are IT Consultant/Specialist, 48 respondents (17.6%) are IT Academician/Researcher, 117 respondents (43%) are IT Engineer/Executive/Staff, 30 respondents (11%) are System Administrator and 3 respondents (1.1%) are others. It showed that the highest are IT Engineer/Executive/Staff and the lowest are IT Consultant/Specialist.

Next the years of experience showed the majority of the respondents are between 6 to 10 years with 109 respondents (40.1%) followed by between 11 to 20 years with 92 respondents (33.8%) and more than 20 years with 47 respondents or 17.3%. While the minority of the respondents less than 5 years with 24 respondents (8.8%).

Table 4.3: Profile of Interviewee

Profile	Frequency	Percent
Job Title		
IT Director/Manager	10	3.7
IT Consultant/Specialist	2	0.7
IT Academician/Researcher	48	17.6
IT Engineer/Executive/Staff	117	43.0
System Administrator	30	11.0
IT Technical Assistant	62	22.8
Others	3	1.1
Years of Experience		
Less than 5	24	8.8
6-10	109	40.1
11-20	92	33.8
20+	47	17.3

Table 4.4 shows the distribution of information security environment. Based on company implemented a formalized information Security Management (ISM) showed 163 respondents (59.9%) are implemented but 8 respondents (2.9%) are not implemented ISM. Meanwhile 101 respondents (37.1%) are don't know about ISM. It showed that the highest are implemented and the lowest are do not implemented ISM.

Based on the manages the ISM showed the majority of the respondents are IT Director with 176 respondents (64.7%) followed by CIO or CTO with 59 respondents (48.9%), ISM Manager with 20 respondents (7.4%) and IT Manager with 15 respondents (5.5%). While the minority of the respondents are outsourced to a third party with 2 respondents (0.7%).

Moreover, company adopted of ISM standards or frameworks showed majority of the respondents have company adopted of ISM standards with 151 respondents (55.5%) and 106

respondents (39%) do not know about that. Meanwhile the minority of the respondents are no and were are not planning to adopt of ISM standards with 2 respondents (0.7%), no but we might in the near future with 6 respondents (2.2%) and no but we are in progress with 7 respondents or 2.6%.

Lastly about the ISM standards showed majority of the respondents do not about ISM Standard with 126 respondents (46.3%), ISO 27001 with 106 respondents (39%), ISO 27032 with 16 respondents (5.9%), ITIL with 13 respondents (4.8%) and COBIT with 7 respondents (2.6%). Meanwhile the minority of the respondents are RAKKSSA with 4 respondents or 1.5%.

Table 4.4: Distribution of Information Security Environment

Information Security Environment	Frequency	Percent
Implemented		
Yes	163	59.9
No	8	2.9
Don't Know	101	37.1
Manages		
ISM Manager	20	7.4
IT Director	176	64.7
IT Manager	15	5.5
CIO or CTO	59	21.7
Outsourced to a third party	2	0.7
Company		
Yes	151	55.5
No but we are in progress	7	2.6
No but we might in the near future	6	2.2
No and were are not planning to adopt any of ISM standards	2	0.7
Do Not Know	106	39.0
ISM Standards		
ISO 27001	106	39.0
ISO 27032	16	5.9
COBIT	7	2.6
ITIL	13	4.8
RAKKSSA	4	1.5
Don't know	126	46.3

4.4 Reliability

Table 4.5 showed the result of reliability data. Based on the result, the IT asset identification showed Cronbach's alpha of 0.887, security breach identification is 0.928, IT security offensive protection are 0.881, IT security defensive protection are 0.923 and IT security objectives are 0.978. Every questionnaire items are said to be valid because the Cronbach's alpha greater than 0.7. Please refer to Table 3.2, page 69 in Chapter 3. So, the data in this study can be classified as good and adequate for this research means.

Table 4.5: Test of Reliability

Factors	Cronbach Alpha	No of Items
IT Asset Identification	0.887	4
Security Breach Identification	0.928	3
IT Security Offensive Protection	0.881	3
IT Security Defensive Protection	0.923	7
IT Security Objectives	0.978	3

4.5 Normality Test

Table 4.6 showed normality data for each factors. Based on the results, that all factor have a mean and median are very similar and based on the test of significantly found that each factor showed significant level of $p < 0.05$. This showed that it is not normal distribution and is suitable for further analyzed for this study. However, the skewness and kurtosis showed the result between -2 to 2. Thus, the data is normal.

Table 4.6: Test of Normality for Each Factor

Factors	Mean	Median	Standard Deviation	Skewness	Kurtosis	Significant
IT Asset Identification	8.398	8.500	0.815	-0.213	-0.079	0.000
Security Breach Identification	8.313	8.000	0.966	-0.257	-0.355	0.000
IT Security Offensive Protection	8.631	9.000	0.796	-0.673	1.249	0.000
IT Security Defensive Protection	8.69	8.714	0.727	-0.304	0.244	0.000
IT Security Objectives	9.203	9.000	0.816	-0.869	0.414	0.000

4.6 Descriptive Statistics

Descriptive statistics described the data collection and summary of the data in the simple and easy way such as table, figure, frequency, percentage, mean and standard deviation.

4.6.1 To analyze the factors influencing the IT security Maintenance

There are five factors influence the IT security maintenance such as IT asset identification, security breach identification, IT security offensive protection, IT security defensive protection and IT security objectives.

4.6.1.1 IT Asset Identification

Table 4.7 represents the frequencies and percentages for the IT asset Identification. As shown in the Table 4.7, a substantial majority of the respondents chooses scale 9 about *"Identification of information generated, consumed, processed or store retrieved by the information system is important"* (41.1%). The respondents also choose scale 8 about *"Identification of information generated, consumed, processed or store retrieved by the computer server is important"* (40.7%) and "*Identification of information generated, consumed, processed or store retrieved by the network technologies is important"* (33.7%)".

As seen in the Table 4.7, the respondents showed various reactions towards the IT Asset Identification. The highest mean showed respondents agree about *"Identification of information generated, consumed, processed or store retrieved by the information system is important"* (M=8.697, SD=0.912). While the lowest mean showed the respondents also agree about *"Identification of information generated, consumed, processed or store retrieved by the network technologies is important"* (M=8.165, SD=1.0412). The overall mean for IT assets identification is 8.398 and standard deviation is 0.815. These shown the respondents **agree** about IT Asset identification.

Table 4.7: Frequencies and Percentages for IT Asset Identification

Statement	1	2	3	4	5	6	7	8	9	10	Mean	SD
Identification of information generated, consumed, processed or store retrieved by the Information System is important	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (0.3%)	3 (1%)	20 (6.7%)	94 (31.6%)	122 (41.1%)	57 (19.2%)	8.697	0.912
Identification of information generated, consumed, processed or store retrieved by the software is important	0 (0%)	0 (0%)	0 (0%)	0 (0%)	2 (0.7%)	1 (0.3%)	29 (9.8%)	114 (38.4%)	125 (42.1%)	26 (8.8%)	8.471	0.85
Identification of information generated, consumed, processed or store retrieved by the computer server is important	0 (0%)	0 (0%)	0 (0%)	1 (0.3%)	0 (0%)	6 (2%)	52 (17.5%)	121 (40.7%)	89 (30%)	28 (9.4%)	8.259	0.96
Identification of information generated, consumed, processed or store retrieved by the network technologies is important	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	19 (6.4%)	58 (19.5%)	100 (33.7%)	95 (32%)	25 (8.4%)	8.165	1.0412
Overall											8.398	0.815

4.6.1.2 Security Breach Identification

Table 4.8 represents the frequencies and percentages for the security breach identification. As shown in Table 4.8, a substantial majority of the respondents chooses scale 8 about "*Requirement of the vulnerabilities analysis to secure IT environment in the organization" (*37.7%). It was followed by "*Requirements of the threats analysis to secure IT environment in the organization"* (33.3%).

As seen in Table 4.8, the respondents showed various reactions towards the security breach identification. The highest mean showed respondents agree about *"Requirements of the threats analysis to secure IT environment in the organization"* (M=8.424, SD=1.047). While the lowest mean showed the respondents also agree about *"Requirements of the possible attack (exploits) analysis to secure IT environment in the organization"* (M=205, SD=1.078).

The overall mean for security breach identification is 8.313 and standard deviation is 0.966. These shown the respondents **agree** about security breach identification.

Table 4.8: Frequencies and Percentages for Security Breach Identification

Statement	1	2	3	4	5	6	7	8	9	10	Mean	SD
Requirement of the threats analysis to secure IT environment in the organization	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	13 (4.4%)	40 (13.5%)	99 (33.3%)	98 (33%)	47 (15.8%)	8.424	1.047
Requirement of the vulnerabilities analysis to secure IT environment in the organization	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	11 (3.7%)	45 (15.2%)	112 (37.7%)	99 (33.3%)	30 (10.1%)	8.309	0.971
Requirement of the possible attack (exploits) analysis to secure IT environment in the organization	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	15 (5.1%)	67 (22.6%)	93 (31.3%)	86 (29%)	36 (12.1%)	8.205	1.078
Overall											8.313	0.966

4.6.1.3 IT Security Offensive Protection

Table 4.9 represents the frequencies and percentages for the IT security offensive protection. As shown in Table 4.9, a substantial majority of the respondents chooses scale 9 about "*The requirement of doing vulnerability assessment to secure IT"* (44.4%) and "*The requirements of doing security audit to secure it environment in the organization"* (43.4%). The respondents also choose scale 8 about "*The requirements of doing penetration testing to secure IT environment in the organization"* (37.4%).

As seen in Table 4.9, the respondents showed various reactions towards the IT security offensive protection. The highest mean showed respondents agree about *"The requirements of doing security audit to secure it environment in the organization"* (M=8.865, SD=0.897). While the lowest mean showed the respondents also agree about "*The requirements of doing penetration testing to secure IT environment in the organization"* (M=8.417, SD=0.897).

The overall mean for IT security offensive protection is 8.631 and standard deviation is 0.796. These shown the respondents **agree** about IT security offensive protection.

Table 4.9: Frequencies and Percentages for IT Security Offensive Protection

Statement	1	2	3	4	5	6	7	8	9	10	Mean	SD
The requirement of doing vulnerability assessment to secure IT environment in the organization	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (0.3%)	2 (0.7%)	23 (7.7%)	99 (33.3%)	132 (44.4%)	40 (13.5%)	8.612	0.863
The requirement of doing penetration testing to secure IT environment in the organization	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (0.3%)	6 (2%)	33 (11.1%)	111 (37.4%)	120 (40.4%)	26 (8.8%)	8.417	0.897
The requirement of doing security audit to secure It environment in the organization	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (0.3%)	2 (0.7%)	15 (5.1%)	75 (25.3%)	129 (43.4%)	75 (25.3%)	8.865	0.897
Overall											8.631	0.796

4.6.1.4 IT Security Defensive Protection

Table 4.10 represents the frequencies and percentages for the IT security defensive protection. As shown in the Table 4.10, a substantial majority of the respondents chooses scale 9 about "*Establishment of IT security awareness program among staffs"* (53.2%) and "*Establishment of IT security parameter, Anti-Malware software to protect any malware activities in the IT environment"* (51.5%).

The respondents also choose scale 8 for *"Establishment of IT security guidelines to handle proper usage of IT services and gadget"* (38.4%) and "*Establishment of IT security parameter, intrusion prevention system/intrusion detection system to pretend any anomaly activities in the digital network"* (35%). As seen in Table 4.10, the respondents showed various reactions towards the IT security defensive protection. The highest mean showed respondents agree about *"Establishment of IT security policy in the organization"* (M=9.04, SD=0.849). While the lowest mean showed the respondents also agree about *"Establishment of IT security education program among the staffs"* (M=8.292, SD=0.995).

The overall mean for IT security defensive protection is 8.69 and standard deviation is 0.727. These shown the respondents **agree** about IT security defensive.

Table 4.10: Frequencies and Percentages for IT Security Defensive Protection

Statement	1	2	3	4	5	6	7	8	9	10	Mean	SD
Establishment of IT security policy in the organization	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	3 (1%)	12 (4%)	47 (15.8%)	143 (48.1%)	92 (31%)	9.04	0.849
Establishment of IT security guidelines to handle proper usage of IT services and gadget	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (0.3%)	4 (1.3%)	41 (13.8%)	114 (38.4%)	102 (34.3%)	35 (11.8%)	8.404	0.936
Establishment of IT security awareness program among staffs	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (0.3%)	0 (0%)	18 (6.1%)	69 (23.2%)	158 (53.2%)	51 (17.2%)	8.804	0.815
Establishment of IT security education program among the staffs	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	8 (2.7%)	61 (20.5%)	95 (32%)	102 (34.3%)	31 (10.4%)	8.292	0.995
Establishment of IT security parameter, Firewall to defend the digital network	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	2 (0.7%)	11 (3.7%)	50 (16.8%)	152 (51.2%)	82 (27.6%)	9.013	0.809
Establishment of IT Security parameter, Intrusion Prevention System /Intrusion Detection System to pretend any anomaly activities in the digital network	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	2 (0.7%)	37 (12.5%)	104 (35%)	113 (38%)	41 (13.8%)	8.518	0.904
Establishment of IT Security parameter, Anti-Malware software to protect any malware activities in the IT environment	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (0.3%)	23 (7.7%)	71 (23.9%)	153 (51.5%)	49 (16.5%)	8.76	0.83
Overall											8.69	0.727

4.6.1.5 IT Security Objectives

Table 4.11 represents the frequencies and percentages for the IT security objectives. As shown in Table 4.11, a substantial majority of the respondents chooses scale 10 about "*The requirements of confidentiality achievement on IT security for organization is important"* (42.8%). It was followed by "*The requirements of integrity achievement on IT security for organization is important"* and *"The requirements of a availability achievement on IT security for organization is important"* (39.7%).

As seen in Table 4.11, the respondents showed various reactions towards the IT security objectives. The highest mean showed respondents agree about "The requirements of confidentiality achievement on IT security for organization is important" (M=9.212, SD=0.825). While the lowest mean showed the respondents also agree about "*The requirements of integrity achievement on IT security for organization is important"* (M=9.191, SD=0.846).

The overall mean for IT security objectives is 9.203 and standard deviation is 0.816. These shown the respondents **agree** about IT security objectives.

Table 4.11: Frequencies and Percentages for IT Security Objectives

Statement	1	2	3	4	5	6	7	8	9	10	Mean	SD
The requirement of confidentiality achievement on IT security for organization is important	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (0.3%)	9 (3%)	43 (14.5%)	117 (39.4%)	127 (42.8%)	9.212	0.825
The requirement of integrity achievement on IT security for organization is important	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	2 (0.7%)	8 (2.7%)	47 (15.8%)	114 (38.4%)	126 (42.4%)	9.191	0.846
The requirement of availability achievement on IT security for organization is important	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (0.3%)	10 (3.4%)	42 (14.1%)	118 (39.7%)	126 (42.4%)	9.205	0.831
Overall											9.203	0.816

4.7 Statistical Test

Statistical test used to investigate the relationship between the variables studied. Correlation tests used to determine the relationship between variables

4.7.1 The Relationship between the Factors Influencing the IT Security Maintenance

Table 4.12 showed the relationship between factors influencing the IT security maintenance. The result showed IT asset identification is significant relationship with security breach identification (r=0.650, p=0.000), IT security offensive protection (r=0.580, p=0.000), IT security defensive protection (r=0.624, p=0.000) and IT security objectives.

Besides security breach identification showed significant relationship with IT security offensive protection (r=0.706, p=0.00) IT security defensive protection (r=0.689, p=0.000) and IT security objectives (r=0.356, p=0.000). Next, IT security offensive protection showed significant relationship with IT security defensive protection (r=0.713, p=0.000) and IT security objectives (r=0.512, p=0.000). Lastly IT security defective protection is significant relationship with IT security objectives (r=0.580, p=0.000).

Table 4.12: Correlation the Variables

	IT Asset Identification	Security Breach Identification	IT Security Offensive Protection	IT Security Defensive Protection	IT Security Objectives
IT Asset Identification	1	.650**	.580**	.624**	.415**
		0.000	0.000	0.000	0.000
Security Breach Identification	.650**	1	.706**	.689**	.356**
	0.000		0.000	0.000	0.000
IT Security Offensive Protection	.580**	.706**	1	.713**	.512**
	0.000	0.000		0.000	0.000
IT Security Defensive Protection	.624**	.689**	.713**	1	.580**
	0.000	0.000	0.000		0.000
IT Security Objectives	.415**	.356**	.512**	.580**	1
	0.000	0.000	0.000	0.000	

4.8 Validity of Measurement Model

Table 4.13 below shows the factor analysis of IT Asset Identification. The Keiser-Meyer-Olkin result showed the value is 0.671. Based on the result, Bartlett's Test of Sphericity give $\chi^2 = 701.669, p < 0.05$. This means all variables are statistically significant and correlated between the items.

Table 4.13: Factor Analysis of IT Asset Identification

Statement	Factor
Identification of information generated, consumed, processed or store retrieved by the Information System is important	0.743
Identification of information generated, consumed, processed or store retrieved by the software is important	0.903
Identification of information generated, consumed, processed or store retrieved by the computer server is important	0.892
Identification of information generated, consumed, processed or store retrieved by the network technologies is important	0.808
Kaiser Meyer Olkin	**0.671**
Chi Square	**701.669**
Sig	**0.000**

Table 4.14 below shows the factor analysis of Security Breach Identification. The Keiser-Meyer-Olkin result showed the value is 0.740. Based on the result, Bartlett's Test of Sphericity give $\chi^2 = 530.777, p < 0.05$. This means all variables are statistically significant and correlated between the items.

Table 4.14: Factor Analysis of Security Breach Identification

Statement	Factor
Requirement of the threats analysis to secure IT environment in the organization	0.902
Requirement of the vulnerabilities analysis to secure IT environment in the organization	0.936
Requirement of the possible attack (exploits) analysis to secure IT environment in the organization	0.909
Kaiser Meyer Olkin	**0.74**
Chi Square	**530.777**
Sig	**0.000**

Table 4.15 shows the factor analysis of IT Security Offensive Protection. The Keiser-Meyer-Olkin result showed the value is 0.642. Based on the result, Bartlett's Test of Sphericity give $\chi^2 = 343.051, p < 0.05$. This means all variables are statistically significant and correlated between the items.

Table 4.15: Factor Analysis of IT Security Offensive Protection

Statement	Factor
The requirement of doing vulnerability assessment to secure IT environment in the organization	0.924
The requirement of doing penetration testing to secure IT environment in the organization	0.841
The requirement of doing security audit to secure It environment in the organization	0.818
Kaiser Meyer Olkin	**0.642**
Chi Square	**343.051**
Sig	**0**

Table 4.16 shows the factor analysis of IT Security Defensive Protection. The Keiser-Meyer-Olkin result showed the value is 0.826. Based on the result, Bartlett's Test of Sphericity give $\chi^2 = 1497.53, p < 0.05$. This means all variables are statistically significant and correlated between the items.

Table 4.16: Factor Analysis of IT Security Defensive Protection

Statement	Factor
Establishment of IT security policy in the organization	0.666
Establishment of IT security guidelines to handle proper usage of IT services and gadget	0.838
Establishment of IT security awareness program among staffs	0.843
Establishment of IT security education program among the staffs	0.767
Establishment of IT security parameter, Firewall to defend the digital network	0.732
Establishment of IT Security parameter, Intrusion Prevention System/Intrusion Detection System to pretend any anomaly activities in the digital network	0.847
Establishment of IT Security parameter, Anti-Malware software to protect any malware activities in the IT environment	0.833
Kaiser Meyer Olkin	**0.826**
Chi Square	**1497.53**
Sig	**0**

Table 4.17 shows the factor analysis of IT Security Objectives. The Keiser-Meyer-Olkin result showed the value is 0.760. Based on the result, Bartlett's Test of Sphericity give $\chi^2 = 1120.855, p < 0.05$. This means all variables are statistically significant and correlated between the items.

Table 4.17: Factor Analysis of IT Security Objectives

Statement	Factor
The requirement of confidentiality achievement on IT security for organization is important	0.983
The requirement of integrity achievement on IT security for organization is important	0.967
The requirement of availability achievement on IT security for organization is important	0.97
Kaiser Meyer Olkin	**0.76**
Chi Square	**1120.855**
Sig	**0**

4.9 Confirmatory Factor Analysis (CFA)

Factor analysis denotes to a set of mathematical techniques that have been established to examine the relationships amongst the studied variables and their underlying concepts, which are also known as factors. The functionality of factor analysis has become well known in various contemporary scientific investigations. It has also been described as "one of the most powerful tools yet devised for the study of complex areas of behavioral scientific concern". CFA can be utilized for a range of objectives, such as psychometric evaluation, construct validation, and the evaluation of measurement invariance (Shek & Yu, 2014).

CFA is one of two basic types of factor analysis, with another type being exploratory factor analysis. CFA is theory-driven and intends to ascertain the capability of a predefined factor model (specified on the basis of theory) to fit an observed data set. In other words, CFA analyzes whether a specific set of factors (i.e., defined by a theory in a priori method) actually defines the variations in the examined variables in the manner that was hypothesized earlier (Shek & Yu, 2014).

Model Type: In a CFA model, if the differences among the examined variables are found to be affected by only one level of latent variables (first-order factors), such model is known as primary factor model or first-order model. In reality, as models frequently permit the first-order factors to be associated, it occasionally makes sense to consider a second order or higher-order models, which can explain the relationships amongst the first-order factors. These CFA models that encompass second or higher-order factors are called hierarchical or higher-order factor models (Shek & Yu, 2014). IT Infra Security has been a first order model based on the correlations of the variables and as per the categorization explained above.

Steps in CFA: CFA usually progresses across the following stages: literature review, model specification, model identification, data collection and primary examinations, model fitness measurement, models comparisons and modifications, and report and explanation of results. Here, model modification and comparison are being discussed which will follow the model fitness measurement.

Model Modification: If the primarily hypothesized model does not fit the data well, researchers often want to re-specify the model in a post-hoc manner. Based on fitness diagnostics and theoretical reasoning, the model is revised and fit to the data again in order to improve its goodness of fit or the parsimony and interpretability of the model. One approach to model modification is to delete the existing factors which is known as model trimming. Paths in the model that are not significant ($p > 0.05$) often suggest wrong factor loadings. With theoretical explanation, these paths can be deleted. The benefit of model trimming is that we can achieve a simple model and / or larger degree of freedom (df), which usually result in better model fit.

Another and more common method of model modification is to add more factors into the model, namely, model building. Two sets of statistics help researchers decide

which parameters can be added. The first one is called "Modification Indices" (MIs). All freely estimated parameters are set as having MI values equal to zero by default. For each fixed parameter specified, there is an MI and its value represents the expected drop in chi-square if the parameter is to be freely estimated. A fixed parameter with the largest modification index should be freed provided that this parameter can be theoretically justified. There are different criteria as to what MI value indicates significant specification error (e.g., 4, 15 etc.).

Model Comparisons: When there are numerous theoretically competing models, researchers must recognize which model fits the data well. This involves model comparisons. There are basically two types of model comparisons: nested model comparison and non-nested model comparison. Our IT model specifications were mainly non-nested as the items pertaining to the different factors were related differently, although number of items were same for all models.

Model Evaluation: There are some certain major characteristics of the results that should be examined to evaluate the acceptability of the CFA models. Like, overall goodness of fit and the interpretability, size, and statistical significance of the estimates. Goodness of fit pertains to how well the parameter estimates of the CFA solution (i.e., factor loadings, factor correlations, error co variances) are able to imitate the relations that were examined in the sample data.

There are a range of goodness of fit statistics that offer a global descriptive summation of the ability of the model to replicate the input covariance matrix. The classic goodness of fit index is chi^2, according to Hair et al. (2017), chi^2 is an essential measure for understanding a measurement model's goodness-of-fit. The chi^2 value refers to the mathematical difference between the hypothesized measurement model based on a priori knowledge and theory and observed measurement model based on

sample data. A low chi^2 value represents that the hypothesized and observed measurement models comply with each other, which can be commented as high fit exists between the measurement model and the sample data.

In addition to a low chi^2 value, a good fit between hypothesized and observed models originates from a non-significant p value for chi^2 (i.e., higher than .05). Despite the fact that it is considered an essential measure for understanding the model fit, the literature states that chi^2 value should not be used as the sole measure for this purpose. This is because $\chi 2$ is sensitive to sample size and, a larger sample size may increase the chi^2 value (Hair et al., 2017). However, chi^2 is used for the calculation of other goodness of fit indices.

Other the most widely accepted global goodness of fit indices are the standardized root mean square residual (SRMR), root mean square error of approximation (RMSEA), Tucker-Lewis index (TLI), and the comparative fit index (CFI). Both CFI and TLI are defined as incremental fit indices where the fit of a hypothesized model is assessed relevant to an alternative model (i.e., null model where the observed indicators do not have any correlation with each other).

RMSEA is a statistic that eliminates the problems relevant to sample size by assessing the model's fit based on the population rather than a narrower sample data. In practice, it is suggested that each of these fit indices be reported and considered because they provide different information about model fit. Considered together, these indices provide a more conservative and reliable evaluation of the fit of the model (Brown & Moore, 2012).

The final major aspect of CFA model evaluation pertains to the interpretability, strength, and statistical significance of the parameter estimates. The parameter estimates (e.g., factor loadings and factor correlations) should only be interpreted in context of a

good-fitting solution. If the model did not provide a good fit to the data, the parameter estimates are likely biased (incorrect). In context of a good-fitting model, the parameter estimates should first be evaluated to ensure they make statistical and substantive sense.

The parameter estimates should not take on out-of-range values (often referred to as *Heywood cases*) such as a negative indicator error variance. These results may be indicative of model specification error or problems with the sample (Brown, 2006). From a substantive standpoint, the parameters should be of a magnitude and direction that is in accord with conceptual or empirical reasoning (e.g., each indicator should be strongly and significantly related to its respective factor, the size and direction of the factor correlations should be consistent with expectation).

Small or statistically non-significant estimates may be indicative of unnecessary parameters (e.g., cross loading). Small and non-significant primary loading may suggest that the indicator should be removed from the measurement model. On the other hand, extremely large parameter estimates may be substantively problematic.

For example, if in a multifactorial solution the factor correlations approach 1.0, there is strong evidence to question whether the latent variables represent distinct constructs (i.e., they have poor discriminant validity). If two factors are highly overlapping, the model could be re-specified by collapsing the dimensions into a single factor. If the fit of the re-specified model is acceptable, it is usually favored because of its better parsimony.

Model Respecification: CFA model will often have to be revised, the most common reason for respecification is to improve the fit of the model because it may have inadequate global goodness of fit, large modification indices, or the parameter estimates are not uniformly interpretable. Modification indices and standardized residuals are often useful for determining the particular sources of strain in the solution

when the model contains minor misspecifications. However, it cannot be over-emphasized that revisions to the model should only be made if they can be strongly justified by empirical evidence or theory.

Model Estimation: AMOS, which stands for "analysis of moment structures", is one of the most popular software packages developed for performing SEM in top-tier journals [17]. Hence, to test dimensionality of study scales, respective items of all scales were factor analysed via CFA using AMOS version 24. CFA determines how well sample supports the factor structure of the scales. CFA relies on numerous statistical tests to determine model fitness with the collected data. Pooled CFA (PCFA) was used following Zainudin (2012).

To achieve the best fit of the model, Byrne (2010) has suggested to delete the problematic items from the structural model. Yet it was ensured that after deletion of the unwanted items there were at-least four items for each factor to measure the final model (Zainudin, 2012). Nazim and Ahmad (2013) rather recommended that to achieve the acceptable model fitness, the redundant items existing in a model must be either removed or constrained.

Following Byrne (2010) model was re-specified to include correlated errors. Following Hair et al. (2017) only those error terms were co variated whose modification index (MI) values were high i.e., 4 and above. Worthy to mention that Holmes-Smith (2006) recommended to use minimum three fit indexes. Those indices were absolute fit, incremental fit, and parsimonious fit (Chong, Nazim and Ahmad, 2014), while Hair et al. (2017) also advised to use multiple indices with minimum one index from each category, same recommendations were used in this research (see Table 1).

Our results fully met the criteria except TLI which was marginally below the threshold value.

KMO Bartlett Test: Since CFA is based on theory and other standard requirements such as sufficiency of the data, therefore KMO test was performed by incorporating all the items of all scales to measure the sufficiency of the sample on the collected data, which scored 0.879 (> 0.5), and Bartlett's test of sphericity of the sample was also significant (p <.001), see Table 4.18, which indicated that the study variables have been correlated sufficiently to impact the mutual variance. Taken together this indicated that data is suitable for conducting the CFA.

Table 4.18: Sampling Adequacy and Sphericity

KMO Measure		.879
Bartlett's Test	Approx. Chi-Square	5277.184
	df	190
	Sig.	.000

Common Method Variance (CMV) – As our data came from one common source in a self-rated mode, so it was prone to have priming effects, evaluation apprehension, and socially desirable responses that might contribute to CMV (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). To address this issue, we pooled all the items of the five constructs into a single factor for factor analysis, the outcomes of the one-factor model displayed a poor model fit (chi^2 = 3170 / df = 170 yielded 18.65, CFI = .43, TLI = .36, RMR = .099, RMSEA = .255). So, it was implied that CMV was not a pervasive issue with our data.

Table 4.19: Collinearity Statistics

Scale	Tolerance	VIF
Asset Identification	.642	1.558
Security Breach Identification	.448	2.231
Security Offensive Protection	.467	2.142
Security Defensive Protection	.451	2.217
Security Objectives	.793	1.262

We also consulted the VIF (variance inflation factor) values which if exceeding the 3.3 threshold indicate of common method bias and collinearity as well (Kock, 2015), on the other hand Tolerance value below 0.2 is an indication of multi collinearity (Menard, 1995). We can note from Table 4.19, that both VIF and Tolerance values were within the criteria ranges, which further ruled out the possibility of method bias / variance.

CFA – To test dimensionality of study scales, respective items of all scales were factor analysed via CFA using AMOS version 24. CFA determines how well sample supports the factor structure of the scales. CFA relies on numerous statistical tests to determine model fitness with the collected data. Pooled CFA (PCFA) was used following Zainudin (2012).

To achieve the best fit of the model, Byrne (2010) has suggested to delete the problematic items from the structural model. Nazim and Ahmad (2013) rather recommended that to achieve the acceptable model fitness, the redundant items existing in a model must be either removed or constrained. Following Byrne (2010) model was re-specified to include correlated errors. Following Hair et al. (2017) only those error terms were covariated whose modification index (MI) values were high i.e., 4 and

above. Table 4.20 contains different criteria to be referred for CFA. Before conducting CFA for our measurement model, CFA for each individual factor was carried out.

Table 4.20: CFA Cut Off Values

Index	Criteria	Literature
Chi^2 / df	< 5	Marsh and Hocevar (1985)
RMSEA	< .08	MacCallum et al. (1996)
SRMR	< .08	Hu and Bentler (1999)
CFI	> .90	Bentler (1990)
TLI	> .90	Bentler and Bonett (1980)

It is pertinent to mention that before finalizing the 5-factor model, we first conducted a series of CFAs to ensure discriminant validity of the five types of IT Security related scales. We used self-reported resilient indicators to cross-validate these five scales. Hence, five measurement models were assessed, detail of each is given below.

Asset Identification CFA: Table 4.21 shows the factor loadings (FL) for all the items of Asset Identification scale. Since all factors loadings were above very good (≥.63) criteria, except item-4 which marginally met the good (≥.55) criteria (Comery & Lee, 1992), so it was established that Asset Identification measure was reliable (Hair et al., 2017).

Table 4.21: FL, AVE, CR and Discriminant Validity of Asset Identification Scale

Item No.	FL	Discriminant Validity				AVE	CR
AssetID1	0.69	***.768***				0.59	0.96
AssetID2	1.09	.755	***.768***				
AssetID3	0.65	.451	.705	***.768***			
AssetID4	0.52	.362	.566	.805	***.768***		

Convergent Validity: It's the extent of agreement in the several trials at quantifying exactly the same theory using varied approaches (Bagozzi, 1980). For convergent validity, the AVE (average variance explained) should be greater than 0.5 (Hock & Ringle, 2006). The AVE value for Asset Identification scale was well above the criteria (see Table 4.21).

Discriminant Validity: AVE (average variance explained) is also used to assess the discriminant validity (Fornell & Larcker, 1981). Square-root value of AVE is used to compare with inter-item correlations of the factors or scales. As can be seen in Table 4.21, square root values of AVE (diagonal, bold and italic) were higher than the inter-construct correlations except for item-3, so discriminant validity was approximately established.

Construct Reliability: composite reliability (CR) nowadays is considered to estimate the true reliability of the scale as compared with Cronbach alpha (Garson, 2012). As shown in Table 4.21, our 4 items model of Asset Identification scale adequately met the acceptable values of CR i.e., > 0.7 for confirmatory purposes (Hair et al., 2017).

Model Fitness: Table 4.22 indicated that 4 items model showed an excellent fit on the data, hence establishing that parsimony and substantiality sense of the model was according to the established standards.

Table 4.22: Model Fit Statistics for Asset Identification Scale

Chi^2	**DF**	**Chi^2 / df**	**RMR**	**TLI**	**CFI**	**RMSEA**
1.41	1	1.41	.008	.996	.999	.039

Security Breach Identification CFA: Table 4.23 shows the factor loadings (FL) for all the items of Security Breach Identification scale. Since all factors loadings were above excellent (≥.71) criteria (Comery & Lee, 1992), so reliability of this measure was established (Hair et al., 2017).

Table 4.23: FL, AVE, CR and Discriminant Validity of Security Breach Identification Scale

Item No.	**FL**	**Discriminant Validity**			**AVE**	**CR**
SBID1	0.83	***.866***			0.75	0.98
SBID2	0.93	.776	***.866***			
SBID3	0.85	.707	.793	***.866***		

Convergent Validity: It's the extent of agreement in the several trials at quantifying exactly the same theory using varied approaches (Bagozzi, 1980). For convergent validity, the AVE (average variance explained) should be greater than 0.5 (Hock & Ringle, 2006). The AVE value for Security Breach Identification scale was well above the criteria (see Table 4.23).

Discriminant Validity: AVE is also used to assess the discriminant validity (Fornell & Larcker, 1981). Square-root value of AVE is used to compare with inter-item correlations of the factors or scales. As can be seen in Table 4.23, square root values of AVE (diagonal, bold and italic) were higher than the inter-construct correlations, so discriminant validity for Security Breach Identification Scale was established.

Construct Reliability: composite reliability (CR) nowadays is considered to estimate the true reliability of the scale as compared with Cronbach alpha (Garson, 2012). As shown in Table 4.23, our 3 items model of Security Breach Identification scale adequately met the acceptable values of CR i.e., > 0.7 for confirmatory purposes (Hair et al., 2017).

Model Fitness: Table 4.24 indicated 3 items model showed the excellent fit on the data, hence establishing that parsimony and substantiality sense of the model was according to the established standards.

Table 4.24: Model Fit Statistics for Security Breach Identification Scale

Chi²	**DF**	**Chi² / df**	**RMR**	**TLI**	**CFI**	**RMSEA**
2.62	2	1.31	.035	.998	.999	.034

Security Offensive Protection CFA: Table 4.25 shows the factor loadings (FL) for all the items of Security Offensive Protection scale. Since all factors loadings were above excellent (≥.71) criteria (Comery & Lee, 1992), so reliability of this measure was established (Hair et al., 2017).

Table 4.25: FL, AVE, CR and Discriminant Validity of Security Offensive Protection Scale

Item No.	FL	Discriminant Validity			AVE	CR
Offence1	0.83	***.825***			0.68	0.97
Offence2	0.83	.691	***.825***			
Offence3	0.82	.682	.467	***.825***		

Convergent Validity: It's the extent of agreement in the several trials at quantifying exactly the same theory using varied approaches (Bagozzi, 1980). For convergent validity, the AVE (average variance explained) should be greater than 0.5 (Hock & Ringle, 2006). The AVE value for Security Offensive Protection scale was (see Table 4.25) was well above the criteria.

Discriminant Validity: AVE is also used to assess the discriminant validity (Fornell & Larcker, 1981). Square-root value of AVE is used to compare with inter-item correlations of the factors or scales. As it can be seen in Table 4.25, square root values of AVE (diagonal, bold and italic) were higher than the inter-construct correlations, so discriminant validity for Security Offensive Protection Scale was established.

Construct Reliability: composite reliability (CR) nowadays is considered to estimate the true reliability of the scale as compared with Cronbach alpha (Garson, 2012). As shown in Table 4.25, our 3 items model of Security Offensive Protection scale adequately met the acceptable values of CR i.e., > 0.7 for confirmatory purposes (Hair et al., 2017).

Model Fitness: Table 4.26 indicated that 3 items model showed an excellent fit of the data, hence establishing that parsimony and substantiality sense of the model was according to the established standards.

Table 4.26: Model Fit Statistics for Security Offensive Protection Scale

Chi^2	**DF**	**Chi^2 / df**	**RMR**	**TLI**	**CFI**	**RMSEA**
.968	1	.968	.018	1.00	1.00	.000

Security Defensive Protection CFA: Table 4.27 shows the factor loadings (FL) for all the items of Security Defensive Protection scale. Since most of the factor loadings were near or above good (≥.63) criteria, except one item was marginally good (≥.55) and one item was marginally fair (≥.45) as per the criteria defined by Comery and Lee (1992), since AVE was above the threshold of 0.5 so no item was dropped, which implied that reliability of this measure was also established (Hair et al., 2017).

Convergent Validity: It's the extent of agreement in the several trials at quantifying exactly the same theory using varied approaches (Bagozzi, 1980). For convergent validity, the AVE (average variance explained) should be greater than 0.5 (Hock & Ringle, 2006). The AVE value for Security Defensive Protection scale was (see Table 4.27) was well above the criteria.

Discriminant Validity: AVE is also used to assess the discriminant validity (Fornell & Larcker, 1981). Square-root value of AVE is used to compare with inter-item correlations of the factors or scales. As can be seen in Table 4.27, square root values of AVE (diagonal, bold and italic) were higher than the inter-construct correlations except item number 2 and 4. Since majority of the items' AVEs were

discriminant so it was implied that Security Defensive Protection Scale approximately achieved an overall discriminant validity.

Table 4.27: FL, AVE, CR and Discriminant Validity of Security Defensive Protection Scale

Item No.	FL	Discriminant Validity							AVE	CR
Defence1	0.40	***.728***								
Defence2	0.89	.354	***.728***							
Defence3	0.60	.669	.616	***.728***						
Defence4	0.90	.171	.803	.535	***.728***				0.53	0.94
Defence5	0.54	.755	.369	.654	.310	***.728***				
Defence6	0.89	.353	.800	.533	.802	.480	***.728***			
Defence7	0.70	.490	.624	.653	.625	.552	.623	***.728***		

Construct Reliability: composite reliability (CR) nowadays is considered to estimate the true reliability of the scale as compared with Cronbach alpha (Garson, 2012). As shown in Table 4.27, our 3 items model of Security Defensive Protection scale adequately met the acceptable values of CR i.e., > 0.7 for confirmatory purposes (Hair et al., 2017).

Model Fitness: Table 4.28 indicated that 3 items model showed the excellent fit on the data, hence establishing that parsimony and substantiality sense of the model was according to the established standards.

Table 4.28: Model Fit Statistics for Security Defensive Protection Scale

Chi^2	DF	Chi^2 / df	RMR	TLI	CFI	RMSEA
6.145	4	1.54	.009	.992	.999	.044

Security Objectives CFA: Table 4.29 shows the factor loadings (FL) for all the items of Security Objectives scale. Since all factors loadings were above excellent (≥.71) criteria (Comery & Lee, 1992), so reliability of this measure was established (Hair et al., 2017).

Table 4.29: FL, AVE, CR and Discriminant Validity of Security Objectives Scale

Item No.	FL	Discriminant Validity			AVE	CR
Objectives1	0.99	***.964***			0.93	.998
Objectives2	0.95	.933	***.964***			
Objectives3	0.95	.937	.898	***.964***		

Convergent Validity: It's the extent of agreement in the several trials at quantifying exactly the same theory using varied approaches (Bagozzi, 1980). For convergent validity, the AVE (average variance explained) should be greater than 0.5 (Hock & Ringle, 2006). The AVE value for Security Objectives scale was (see Table 4.29) was well above the criteria.

Discriminant Validity: AVE is also used to assess the discriminant validity (Fornell & Larcker, 1981). Square-root value of AVE is used to compare with inter-item correlations of the factors or scales. As can be seen in Table 4.29, square root values of AVE (diagonal, bold and italic) were higher than the inter-construct correlations, so discriminant validity for Security Objectives Scale was established.

Construct Reliability: composite reliability (CR) nowadays is considered to estimate the true reliability of the scale as compared with Cronbach alpha (Garson, 2012). As shown in Table 4.29, our 4 items model of Security Objectives scale adequately met the acceptable values of CR i.e., > 0.7 for confirmatory purposes (Hair et al., 2017).

Model Fitness: Table 4.30 indicated that 3 items model showed an excellent fit of the data, hence establishing that parsimony and substantiality sense of the model was according to the established standards.

Table 4.30: Model Fit Statistics for Security Objectives Scale

Chi^2	**DF**	**Chi^2 / df**	**RMR**	**TLI**	**CFI**	**RMSEA**
1.58	1	1.58	.010	.998	.999	.046

Measurement Model CFA: Subsequently, an overall CFA was run to examine the fitness of the five-factor model including Asset Identification, Security Breach Identification, Security Offensive Protection, Security Defensive Protection and Security Objectives, which showed the best possible fit (Chi^2 = 649 / df = 138 yielded 4.71, CFI = .902, TLI = .866, RMR = .067, RMSEA = .117) between the measurement and the data collected (see Table 4.31).

Table 4.31: Model Fit Statistics for Measurement Model

Chi^2	**DF**	**Chi^2 / df**	**RMR**	**TLI**	**CFI**	**RMSEA**
649	138	4.71	.067	.902	.866	.117

Worthy to mention that Holmes-Smith (2006) recommended to use minimum three fit indexes. Those indices were absolute fit, incremental fit, and parsimonious fit

(Chong, Nazim and Ahmad, 2014), while Hair et al. (2017) also advised to use multiple indices with minimum one index from each category, same recommendations were used in this research (see Table 4.31). Our results met the criteria except the additional indices taken from these fit categories i.e., TLI (marginally below the acceptable value) and RMSEA (a little above the acceptable value), since the globally acceptable indices i.e., Chi^2, CFI and RMR produced acceptable values, so it was implied that our model was fitting the data.

As shown in Figure 4.1 factor loadings (FL) for all the scales were above very good (≥.63) criteria (Comery & Lee, 1992), except two to three items were meeting the fair (≥.45) criteria, so reliability of our measures / model was established (Hair et al., 2017).

Table 4.32: AVE, CR and Discriminant Validity of the Measurement Model

Scale	Discriminant Validity					AVE	CR
Asset Identification	***.768***					0.59	0.96
Security Breach Identification	.664	***.866***				0.75	0.98
Security Offensive Protection	.532	.798	***.824***			0.68	0.97
Security Defensive Protection	.608	.736	.718	***.728***		0.53	0.94
Security Objectives	.095	.111	.297	.273	***.964***	0.93	0.99

Convergent Validity: It's the extent of agreement in the several trials at quantifying exactly the same theory using varied approaches (Bagozzi, 1980). For convergent validity, the AVE (average variance explained) should be greater than 0.5 (Hock & Ringle, 2006). The AVE value for all the measures included in our model (see Table 4.32) was well above the criteria.

Discriminant Validity: AVE is also used to assess the discriminant validity (Fornell & Larcker, 1981). Square-root value of AVE is used to compare with inter-item correlations of the factors or scales. As can be seen in Table 4.32, square root values of AVE (diagonal, bold and italic) were higher than the inter-construct correlations, so discriminant validity of our model was established.

Construct Reliability: composite reliability (CR) nowadays is considered to estimate the true reliability of the scale as compared with Cronbach alpha (Garson, 2012). As shown in Table 4.32, our 5-factor model adequately met the acceptable values of CR i.e., > 0.7 for structural confirmatory purposes (Hair et al., 2017).

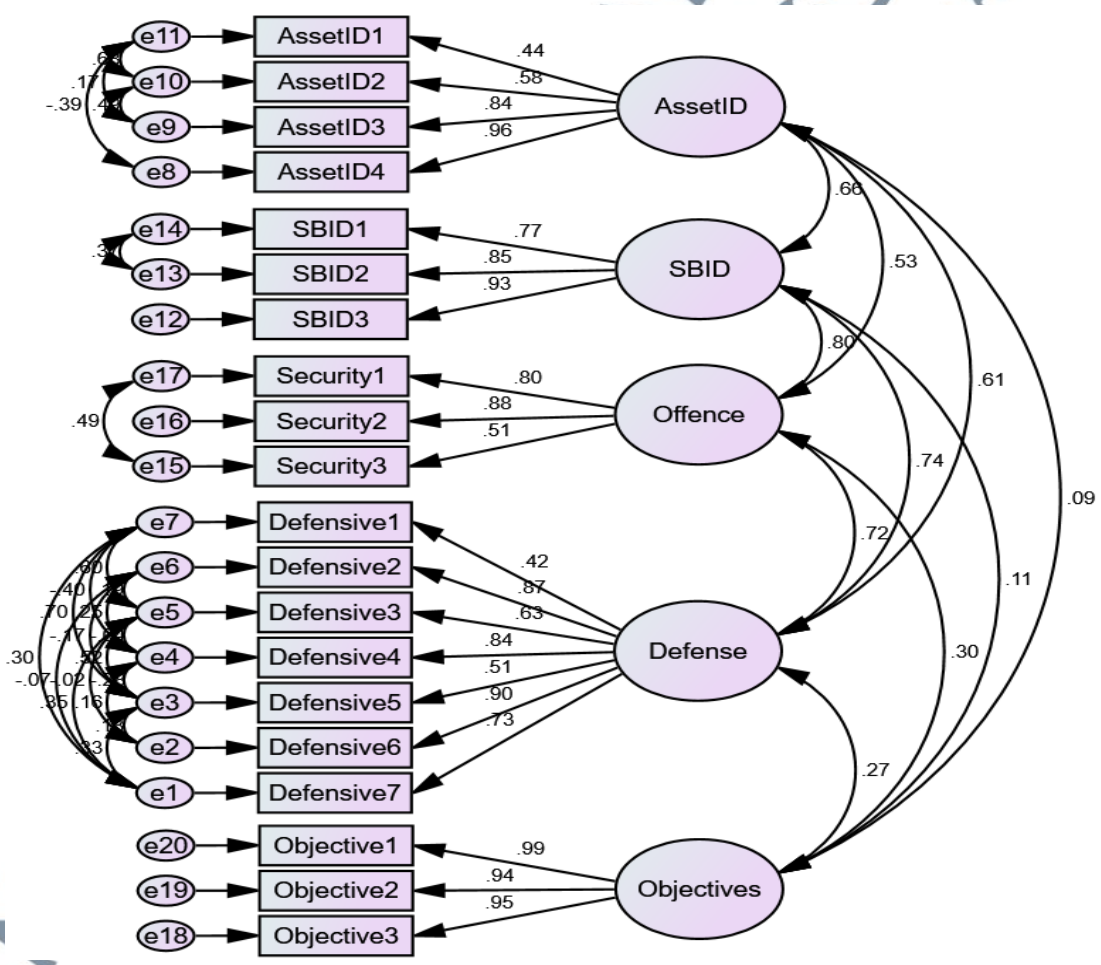

Figure 4.1: CFA Graphic Model

4.10 Factors Influencing IT Security Maintenance

4.10.1 IT Asset Identification

Due to the advancement of interconnected networks, organizations are facing information security risks on a daily basis. Therefore, it is important for the organization to manage the risk which can jeopardize the security of their valuable information (Boltz, 1999; Mouw, 2013). According to International standard of ISO/IEC, information security risks can be defined as consequence of incertainty on information security objectives, specifies the control as a measure from the international best security practices to modify information security risks. A control can decrease the risk by reducing the possibility of an event, the impact or both.

According to Jeffrey L.W et al. (2007) an information system (IS) is the arrangement of people, data, processes and information technology that interact to collect, process, store and provide as output the information needed to support an organization. The system is a collection of components that interact to perform the functions aforementioned. Currently most IS are interconnected and thus internet is playing a major role in information collection, storage, processing and retrieving. IS could be divided into four categories which are data or transaction processing information system, management information system, decision support information system and executive information system. In most organization including the public sector organizations, information systems are mostly grouped in these four categories. Though this are the most common information systems, change in technology is bringing in other most specialized information systems that includes expert systems, enterprise system and geographical information systems. Due to the importance show

by the information system towards the organization, it is crucially important to provide proper security towards the system.

The security of an information system involves the confidentiality, availability and integrity of its data and its functionality (INFOSEC, 1993). The aim of developing and using an Information system in any organization is for the organization to effectively and efficiently collect, store, process and retrieve data for use. For this reason, data is a critical asset in an organization. Information security is an organization's approach to maintaining, non-repudiation, accountability, authenticity and reliability of its IT systems. Thus when information of an organization is secure then IT systems are secure. It is therefore necessary to consider information security while studying information system security.

In this part, to ensure the security well concern, IT asset identification investigated. Majority of the respondents stated that identification of information generated, consumed, processed or store retrieved by the Information system is important (Mean=8.697, SD=0.912). In addition, identification of information generated, consumed, processed or store retrieved by the software is important (Mean=8.471, SD=0.85). Both information system and software are important to ensure the information successfully generated, consumed, processes and store retrieve. The information gained able to ensure the asset being identify.

The identification of information processed on an information system is essential to the proper selection of security controls and ensuring the confidentiality, integrity, and availability of the system and its information (NIST SP800-60, 2008). Since information processing is unique to organization, different organization need

therefore to adopt and implement an information security systems framework that is will securely protected its IT system and in turn organization's information.

4.10.2 Security Breach Identification

Information security risk management is very important for business, government and also for individual in order to protect their information. Since a decade ago, the organizations are paying more attention to their information assets against any possible security threats (Bojanc, 2012). This is important for the survival of organization and to gain competitive advantage. However, due to lack of proper security risk management, it has been reported that organization experiencing security breach identification.

Based on the finding obtained, security breach identification could be seen as the requirement of the threats analysis to secure IT environment in the organization (Mean=8.424, SD=1.047). Besides the security breach identification could be measure through the requirement of the vulnerabilities analysis to secure IT environment in the organization (Mean=8.309, SD=0.971). Hence, it proved that to manage security breach identification, organization need to access the security risks in their valuable assets and plan for mitigating control actions to address these risks.

4.10.3 IT Security Offensive Protection

IT security represent a process to ensure that the appropriate security measures are identified and applied to meet the management expectations for a secure and trusted computing environment. However, a principal challenge that many organizations are facing is identifying and evaluating the IT security risks to their operations. Therefore, careful selection of IT security protection methods important to identify, manage and

evaluate the risks to their assets. It informs organizations about information security threats that may affect the organizations' assets and exploit their vulnerabilities.

Referring to the finding obtained in Chapter 4, IT security offensive protection could be conducted as the requirement of doing security audit to secure IT environment in the organization (Mean=8.865, SD=0.897). In addition, the protection is available when the requirement of doing vulnerability assessment to secure IT environment in the organization (Mean=8.612, SD=0.863). These aspects are important to ensure any viruses could not attack the security system. The expertise in the respective field is important to ensure all those aspects could be well-manage. It is in line with the advancement of IT where it is required an intelligent decision making approaches when it comes to protection of information resources (Bojanc and Jerman-Blažič, 2013). The use of digital data and the evolution of information system expose business to threat that attack the organizational assets which can lead to economic losses.

4.10.4 IT Security Defensive Protection

An effective risk management and protection requires the probability analysis of events and the impact of the threats to the information assets (Iacob, 2014). In recent years, IT security defensive protection have been widely become the major consideration as it could give harm and threat towards the security system. IT system could be at risk from unintentional operator errors as well as from natural and instrumental disaster. These are mostly caused by the interconnection of the computers and accessibility by many people. It may due to the number of people with computer skills is increasing, so that the hacking skills and techniques also increase. IT security risk management is the precondition of information security management, it is

perceived as a way to reduce uncertainty and its consequences. In turn, successful risk management meaningful understanding of the whole security profile of organizations.

Information security can be viewed as including three functions: Access control, secure communications, and protection of private data (Sehgal N.K., 2011). These areas if well considered while designing an Information system, the systems will be more secure. The Storage, processing and transmission of business information has been greatly facilitated by the development of computers and computer networks and the widespread implementation of such information technology (IT) resources. These developments have enabled organizations to perform business transactions with their customers, suppliers and other business partners with greater efficiency and speed (Solms, 2005)

A successful IT security system requires an affective risk management process, which intends to provide an appropriate protection system. In terms of IT security defensive protection, the finding showed that it is necessary to establish IT security policy in the organization in order to ensure security system is in top condition (Mean=9.04, SD=0.849). With the proper security policy, it able to secure the system from being hacked and hijacked by irresponsible party for their own benefit. Besides that, it also require to establish IT security parameter, firewall in order to defend the digital network (Mean=9.013, SD=0.809). Thus, it proved that proper IT security defensive protection able to mitigate security risk.

4.10.5 IT Security Objectives

In the current information age, the issue of information technology security has become a vital entity because organization across the globe conduct business as well as their organization in an interconnected and information rich environment, information

security risk assessment which enables the government, private and public organization to identify their own risk and also provide a measured, analyzed security profile of critical information assets to develop effective and economically viable control strategies (Shedden et al., 2011, 2010; Baskerville, 1991; Braber et al., 2007).

The necessity of information security in organizations has increased because of the enormous changes in structure and type of information technologies applied to information creates risks. IS security effectiveness is the ability of IS security measures to protect against the unauthorized and deliberate misuse of assets of the local organizational information system by individuals, including violations against hardware, programs, data, and computer service (Straub, 1990). An effective security program would reduce risks, protect IT infrastructure from vulnerabilities, would achieve what it is intended to do and institute the right controls to prevent security breaches (Sushma Mishra et al, 2011). Risks to assets are identified in terms of confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability. The criticality of each risk is rated according to potential impact and likelihood of occurrence.

The organization wanting to eliminate the possible risks in the organization by conducting IT security risk assessment in order to determine the potential threat and risk associated with IT system (Syalim et al., 2009). Risk identification is basically a systematic procedure undertaken to discover and select an organization's most critical information assets as well as the identification of the threats and vulnerabilities of each of these assets. The reasons why the IT security is important could be seen based on the objectives proposed. The finding shows that the requirement of confidentiality achievement on IT security for organization is important (Mean=9.212, SD=0.825).

Besides that, the requirement of availability achievement on IT security for organization also important (Mean=9.205, SD=0.831). As the results of study in IT security maintenance framework implemented, all the objectives stated had been achieve.

4.11 Result of Hypothesis Testing

1. IT ASSET IDENTIFICATION intention in IT Infrastructure Security maintenance.
2. SECURITY BREACH IDENTIFICATION intention in IT Infrastructure Security maintenance.
3. IT SECURITY OFFENSIVE PROTECTION intention in IT Infrastructure Security maintenance.
4. IT SECURITY DEFENSIVE PROTECTION intention in IT Infrastructure Security maintenance.
5. IT SECURITY OBEJCTIVES PROTECTION intention in IT Infrastructure Security maintenance.

Based on the result, all of the hypothesis are accepted. That means all variables (IT Asset Identification, Security Breach Identification, IT Security Offensive Protective, IT Security Defensive Protection and IT Security Objectives Protection) is have relationship with IT Infrastructure Security Maintenance.

Table 4.33: Result of Hypothesis

NO	Hypothesis	Result
H1	IT ASSET IDENTIFICATION intention in IT Infrastructure Security maintenance.	Accepted
H2	SECURITY BREACH IDENTIFICATION intention in IT Infrastructure Security maintenance.	Accepted
H3	IT SECURITY OFFENSIVE PROTECTION intention in IT Infrastructure Security maintenance.	Accepted
H4	IT SECURITY DEFENSIVE PROTECTION intention in IT Infrastructure Security maintenance.	Accepted
H5	IT SECURITY OBEJCTIVES PROTECTION intention in IT Infrastructure Security maintenance.	Accepted

4.12 The Result of Framework Validation

The following Table 4.34 show from the validation of framework of questionnaire survey during in-depth interview session with the selected respondents. The respondents were asked to rate five criteria of framework based on Likert scale of 1 to 5. A score with above three would represent satisfactory performance for that framework criteria matter. The results showed that all criteria were rated above three.

In particular, appropriateness, reliability and suitable in current practice of the framework has been rated with the higher score in each at mean 4.8. Following by the practicality/feasibility and objectivity of the framework with the score in each at mean 4.3.

Table 4.34: Rating Results of the Framework Validation

Validation Criteria	Respondent's Score						Mean
	R1	R2	R3	R4	R5	R6	
1.Appropriateness	4	5	5	5	5	5	4.8
2. Objectivity	4	5	5	5	4	3	4.3
3.Practicality/Feasibility	4	5	5	4	4	4	4.3
4.Reliability	4	5	5	5	5	5	4.8
5.Sutiable of Framework in current practice	4	5	5	5	5	5	4.8

The data collected from the interview shows all 6 respondents said that this framework can be applicable in current practice of the IT security maintenance for IT infrastructures. However, some of the respondents highlighted that this framework implementation can have a problem with the constraint of budget and skill of the staffs. With that, the framework still require improvement.

Table 4.35 shows the summary of respondent's response on the validation questions. Respondent R2 has pointed out to equip this framework with suitable analysis against any information security management model especially in ISMS (Information Security Management System). Every governance issues that have been identified in framework implementation should go suitable analysis with any information security management model use by the company.

In addition, respondents R6 also have highlighted to use or state the tools and technologies for this framework's implementation. However, the tools and technologies usage requires improvement in the context of its accountability.

Table 4.35: Summary of Respondent's Response on Validation Framework's questions

	Questions			
	Can the framework be applicable into current practices?	Can this framework address the current issues?	What are the problems arising from the framework?	Any recommendations to enhance the quality of the framework?
Respondent's Response	All the respondents agreed that this framework is applicable for the current practice.	All the respondents agreed that this framework can address the current issues.	• 2 of respondents highlighted about the budget and skill of the staff. • 2 of respondents highlighted about the policy. • 2 of respondents highlighted about the technology used.	• Put in the security policy. • Look into Information Security quality model. • Put services as inventory. • Staff's training and awareness. • Put technology used.

In summary, this validation result indicates that the newly developed good governance framework was authenticated to be appropriate, objective, reliable, practical and suitable to be used to enhance the good practice of IT security maintenance for IT

infrastructure in IPTA. The feedbacks from the respondents in detail are attached in the Appendix D.

4.13 Chapter Summary

The analysis results of the study focused mainly in determining and developing the IT security maintenance framework for IT infrastructure of the small-mid enterprise. The analysis assists in identifying the (1) components of IT security maintenance framework, (2) verification of the IT security maintenance framework and (3) validation of the IT security maintenance framework which supported the hypothesis using the analysis. The quantitative results help to establish statistical evidence on the strengths of the relationship between constructs and provide directions of the relationship when combined with theory and literature.

This chapter presented the results of the analysis of the questionnaire survey to identify the components, dimensions and characteristics for IT security maintenance framework for IT infrastructure. The quantitative analysis has helped to establish statistical evidence to provide the following results:

a) There were 20 items significantly included in the IT security maintenance framework for IT infrastructure were agreed upon and accepted.

b) The findings indicated that 5 hypotheses were significantly supported. It has been revealed that five information security dimensions were positively related to IT security maintenance framework for IT infrastructure.

After the inferential statistical analysis, the results from the data analysis will be further discussed in qualitative data analysis in order to provide synthesis of IT security maintenance framework for IT infrastructure parameters and to validate the proposed framework with expertise.

Having all data presented, it can suggest that the IT security maintenance framework for IT infrastructure is already verify with the experts and practitioners. With that, its also ready for validation with the experts and practitioners to ensure it capability of implementation.