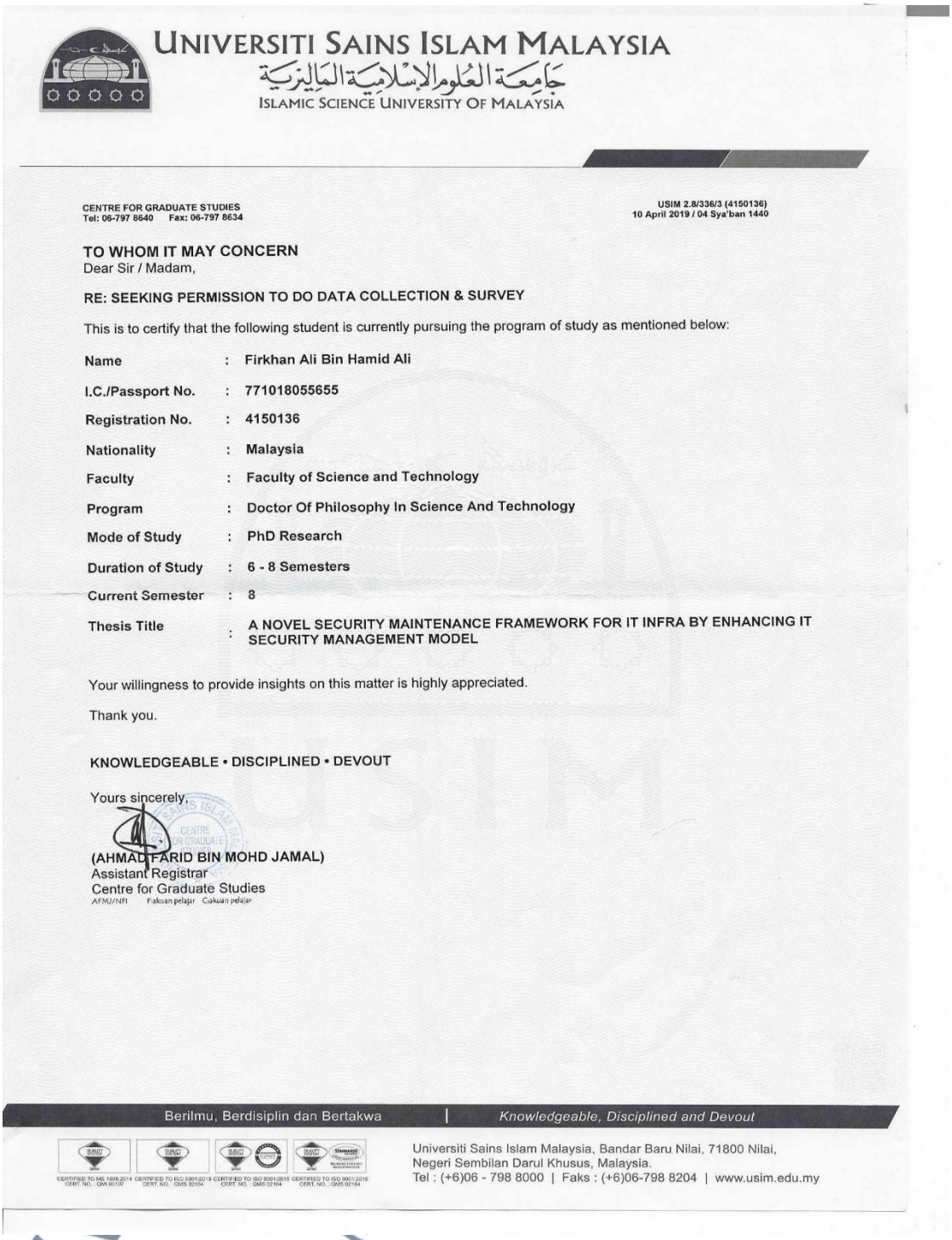
APPENDIX A: Formal Letter for Doing Research Activity



UNIVERSITI SAINS ISLAM MALAYSIA
جَامِعَة العُلوم الإسْلامِيَة المَالِيزِيَة
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

CENTRE FOR GRADUATE STUDIES
Tel: 06-797 8640 Fax: 06-797 8634

USIM 2.8/336/3 (4150136)
10 April 2019 / 04 Sya'ban 1440

TO WHOM IT MAY CONCERN
Dear Sir / Madam,

RE: SEEKING PERMISSION TO DO DATA COLLECTION & SURVEY

This is to certify that the following student is currently pursuing the program of study as mentioned below:

Name	:	Firkhan Ali Bin Hamid Ali
I.C./Passport No.	:	771018055655
Registration No.	:	4150136
Nationality	:	Malaysia
Faculty	:	Faculty of Science and Technology
Program	:	Doctor Of Philosophy In Science And Technology
Mode of Study	:	PhD Research
Duration of Study	:	6 - 8 Semesters
Current Semester	:	8
Thesis Title	:	A NOVEL SECURITY MAINTENANCE FRAMEWORK FOR IT INFRA BY ENHANCING IT SECURITY MANAGEMENT MODEL

Your willingness to provide insights on this matter is highly appreciated.

Thank you.

KNOWLEDGEABLE • DISCIPLINED • DEVOUT

Yours sincerely,

(AHMAD FARID BIN MOHD JAMAL)
Assistant Registrar
Centre for Graduate Studies
AFMJ/NFI Fakuan pelajar Cakuan pelajar

Berilmu, Berdisiplin dan Bertakwa | *Knowledgeable, Disciplined and Devout*

CERTIFIED TO MS 1900:2014 CERT. NO.: QMS 00107 CERTIFIED TO ISO 9001:2015 CERT. NO.: QMS 02164 CERTIFIED TO ISO 9001:2015 CERT. NO.: QMS 02164 CERTIFIED TO ISO 9001:2015 CERT. NO.: QMS 02164

Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Nilai,
Negeri Sembilan Darul Khusus, Malaysia.
Tel : (+6)06 - 798 8000 | Faks : (+6)06-798 8204 | www.usim.edu.my

APPENDIX B: Survey Questionnaire

RESEARCH TITLE:

A Novel Conceptual Security Maintenance Framework for ICT Infrastructure By Enhancing IT Security Management Model

LEAD RESEARCHERS:

Firkhan Ali Bin Hamid Ali – Department of Computer Security, Faculty of Science and Technology, Universiti Sains Islam Malaysia.

BACKGROUND OF RESEARCH:

Security management of Information and Communication Technology (ICT) infrastructure has gained tremendous popularity in recent years according to the diversity of the types of organizations involved from a small company to the government. However, the benefits in terms of flexibility, scalability and low upfront investment in this matter overshadowed by security challenges that hinder its adoption.

In particular, the ICT infrastructure is highly flexible but complex has been exposed to various types of security threats from minor problems such as mis-configure up to lead to a security incident information technology infrastructure and others. This study will present a novel conceptual security maintenance framework model for ICT infrastructures by enhancing Information Technology (IT) security management model.

In order to implement this model, the focus on ICT infrastructure is a combination of several existing security processes, matrices and IT security model for extracting the maintenance of security infrastructure including existing information services and technology within its practicality. Proposals for analysis and perform a security maintenance in the conceptual framework and evaluate it in terms of practical and theoretical scenario. Moreover, the proposed conceptual framework backed allow configuration changes in the environmental assessment of the ICT infrastructure made quickly and

dynamically, taking into account characteristics such as weakness or expected availability. In the case of weakness perspective, this framework can be used to monitor the security maintenance of ICT infrastructure throughout its life and to demonstrate appropriate levels of life expectancy.

PROCEDURES OF THIS STUDY:

The lead researcher invites you to participate in this research based on the fact that you are an IT/ICT professional. You are required to read and agree to the terms and conditions in the Participant Consent Form. It is important to advise that your participation is voluntary, confidential and you can withdraw from this research at any time and for any reason without penalty.

In the research, you will be requested to complete a set of questionnaires in an anonymous online survey which should not be more than 15 minutes. Each question is optional. Please do not name third parties in any open text field of the questionnaire. Any such replies will be anonymised. Data will only be collected through an anonymous online survey. No interviews, recordings or videos will be required. It will be appreciated if all questions are completed. However, do feel free to omit any question you are unwilling to complete as there is no penalty whatsoever. The topics covered in the questionnaires include, but not limited to, company profile (company name is not required), interviewee profile (interviewee name, contact details and any other personally identifiable information are not required), information security environment, challenges and barriers of adopting information security standards or frameworks, benefits of adopting information security management and maintenance standards or frameworks, and plans for future.

All information obtained will be treated confidentially and no name of individuals or organisations will be saved in any format throughout the process. There are no anticipated risks to your participation in this research. However, please be aware that if you make illicit activities known, these will be reported to appropriate authorities.

CONFLICT OF INTEREST:

This research is conducted in partial fulfilment of Firkhan Ali Bin Hamid Ali's Doctor of Philosophy in Science and Technology, to be awarded by the Department of Computer Security, Faculty of Science and Technology, Universiti Sains Islam Malaysia. The lead researcher has no conflict of interest in relation to the topics covered in the research or in relation to any individual or organisation contributing to the research.

PUBLICATION:

The information gathered from online survey will form the basis of the analysis and findings section in the completed research. By participating in this research, you agree that this data may be used for such scientific purpose, and that you have no objection that the data is published in research and scientific publications in a way that does not reveal your specific identity. A completed copy of the research can be made available to you upon request. Should you wish to clarify any aspect of the research processes please feel free to contact the lead researcher. Individual results may be aggregated anonymously and research reported on aggregate results.

DECLARATION:

I am 18 years or older and am competent to provide consent.

I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.

In the extremely unlikely event that illicit activity is reported I will be obliged to report it to appropriate authorities.

I agree that my data is used for scientific purposes and I have no objection that my data is published in scientific publications in a way that does not reveal my identity.

I freely and voluntarily agree to be part of this research study, though without prejudice to my legal and ethical rights.

I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.

I understand that my participation is fully anonymous and that no personal details about me will be recorded.

I have received a copy of this agreement.

☐ I accept the terms and conditions in the form

☐ I do not accept the terms and conditions in the form

Statement of investigator's responsibility:

The lead researcher has explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. The lead researcher has offered to answer any questions and fully answered such questions. The lead researcher believes that the participant understands his explanation and has freely given informed consent.

RESEARCHERS CONTACT DETAILS:

Firkhan Ali bin Hamid Ali (firkhan.uthm@yahoo.com) Phone: +6013 730 5358

Investigator's Signature:

Date: 10 April 2018

Research Questionnaire

Before you start the survey, please note the following: Each question is optional. To ensure replies are anonymised, please do not name third parties in any open text field of the questionnaire

Part 1 Company Profile

1. What is your university category?

	Research university
	Comprehensive university
	Focused university

2. How many full time employees in your university?

	Less than 100
	101-500
	501-1000
	1001-2000
	2000+

3. Who are the key stakeholders for making ICT decisions in your university?

	CIO or CTO (Globally or Locally)
	IT Director
	IT Manager

	Other

If other, please specify:

Part 2 Interviewee Profile

4. What is your job title?

	CIO or CTO (Globally or Locally)
	IT Director/ Manager
	IT Consultant / Specialist
	IT Academician/ Researcher
	IT Engineer/Executive/Staff
	System Administrator
	IT Technical Assistant
	Other

If other, please specify:

5. How many years of experience do you have in ICT management?

	Less than 5
	6-10
	11-20

	20+

Part 3 Information Security Environment

6. Has your company implemented a formalised Information Security Management (ISM)?

	Yes
	No
	Don't know

7. Who manages the ISM in your company?

	ISM Manager
	IT Director
	IT Manager
	CIO or CTO
	Outsourced to a third party
	Other

If other, please specify:

8. Has your company adopted any of ISM standards or frameworks?

	Yes
	No, but we are in progress

	No, but we might in the near future
	No, and we are not planning to adopt any of ISM standards or frameworks
	Don't know

9. Which of the following ISM standards or frameworks have been adopted/are in implementation in your company?

	ISO 27001
	ISO 27032
	ISO 27018 (Cloud)
	COBIT
	PCI DSS
	ITIL
	Cyber Essentials
	NIST security framework
	CIS Critical Security Controls
	RAKKSSA (Rangka Kerja Keselamatan Siber Sektor Awam)
	Don't know
	Other

If other, please specify:

Part 4 IT Assets Identification

		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Please indicate the level of agreement with the following statements in relation to implement IT assets identification of university		**10**	**8**	**6**	**4**	**2**
A	**Identification of information generated, consumed, processed or store retrieved by the Information System is important.**					
B	**Identification of information generated, consumed, processed or store retrieved by the software is important.**					
C	**Identification of information generated, consumed, processed or store retrieved by the computer server is important.**					

D	**Identification of information generated, consumed, processed or store retrieved by the network technologies is important.**					

Part 5 IT Security Breach Identification

Please indicate the level of agreement with the following statements in relation to implement IT security breach identification of the university.		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
		10	**8**	**6**	**4**	**2**
A	**Requirement of the threats analysis to secure IT environment in the organization.**					
B	**Requirement of the vulnerabilities analysis to secure IT environment in the organization.**					
C	**Requirement of the possible attack analysis to secure IT environment in the organization.**					

Part 6 IT Security Offensive Protection

		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Please indicate the level of agreement with the following statements in relation to implement IT security offensive protection of the university		**10**	**8**	**6**	**4**	**2**
A	**The requirement of doing vulnerability assessment analysis to secure IT environment in the organization.**					
B	**The requirement of doing penetration testing analysis to secure IT environment in the organization.**					
C	**The requirement of doing security audit analysis to secure IT environment in the organization.**					

Part 7 IT Security Defensive Protection

Please indicate the level of agreement with the following statements in relation to implement IT security defensive protection of university		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
		10	**8**	**6**	**4**	**2**
A	**Establishment of IT security policy in the organization.**					
B	**Establishment of IT security guidelines to handle proper usage of IT services and gadget.**					
C	**Establishment of IT security awareness program among the staffs.**					
D	**Establishment of IT security education program among the staffs.**					

E	**Establishment of IT security parameter, Firewall to defend the digital network.**					
F	**Establishment of IT security parameter, Intrusion Prevention System / Intrusion Detection System to pretend any anomaly activities in the digital network.**					
G	**Establishment of IT security parameter, Anti-Malware software to protect any Malware activities in the IT environment.**					

Part 8 IT Security Objective

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Please indicate the level of agreement with the following statements in relation to implement IT security objective of university	**10**	**8**	**6**	**4**	**2**

A	**The requirement of confidentiality achievement on IT security for organization is important.**					
B	**The requirement of integrity on IT security for organization is important.**					
C	**The requirement of availability achievement on IT security for organization is important.**					

Please share any comments you have on the topics addressed in this survey.

Thanks for helping out with our survey. We appreciate your feedback.

APPENDIX C: Expert Report for Questionnaire Items

Laporan Pakar Item Soal Selidik

Tajuk Kajian: "Secured Information Technology Infrastructure Maintenance".

Ulasan berikut merupakan laporan bagi item soal selidik bagi tajuk seperti dinyatakan di atas,

1. Soal Selidik yang dikemukakan adalah kemas dan jelas.
2. Soal Selidik adalah memadai dengan masa yang diperuntukkan secara online iaitu 15 minit.
3. Profil responden adalah memadai kajian dengan merujuk kepada pihak pengurusan yang lebih memahami isu '*secured information technology infrastructure maintenanc*'.
4. Bahagian 3 soal selidik adalah mendapatkan makluman berkaitan dengan 'security information environment'. Saolan yang dikemukakan adalah memadai dengan persekitaran sasaran responden.
5. Bahagian 4 merupakan pandangan responden berkaitan dengan IT Assets idenfication. Saolan yang dikemukakan adalah memadai dengan skop kajian dan IT Assests. Soalan adalah seiring dengan literature yang dikemukakan.
6. Bahagian 5 merupakan pandangan responden terhadap IT Security Breach Identification. Saoalan adalah jelas dan padat tumpuan fokus pada isu threat analysis, vulnerabilities analysis dan possible attach analysis.
7. Bahagian 6 adalah isu berkaitan dengan security offensive protection. Tiga aspek dalam analisi ini iaitu vulnerabilities assessment, penetration testing analysis dan security audit analysis. Ketiga-tiga elemen ini adalah memadai kajian literatur serta isu semasa dalam secured information technology.
8. Bahagian 7 berkaitan dengan IT security defensive protection. Kajian mengupas 7 aspek berkaitan isu ini iaitu security policy, IT security guidelines, ICT awareness, ICT educational programme, security parameter / prevention, dan software protection. Ketujuh-tujuh elemen ini ada mencakupi kajian dalam aspek IT security defensive protection.
9. Bahagian 8 berkaiatan isu IT security objective. Tiga isu utama dalam organisasi iaitu confidential, integrity and available achievement on IT security. Isu yang ingin dikaji adalah jelas seperti yang dihurai dalam kajian lepas.
10. Bahagian 9, merupakan bahagian open question. Adalah baik bagi responden mengemukakan soalan yang terbuka untuk isu yang tertinggal atau pandangan lain daripada responden.
11. **Keseluruhan soal selidik** adalah memadai masa yang digunakan serta cara pengutipan data secara ONLINE. Keseluruhan soalan adalah fokus pada isu yang ingin dikaji berlandaskan kepada kerangka serta literatur di Bab 2 tesis.
12. Saya percayai dengan soal selidik ini **mampu mencapai objektif kajian dan analisis kajian** dengan jelas dan tepat pada peringkat Kedoktoran Falsafah.

Sekian, sahaja.

Yang Benar,

ASSOC. PROF. DR. SEOW TA WEE
Faculty of Technology Management & Business
Universiti Tun Hussein Onn Malaysia

Prof. Madya. Dr. Seow Ta Wee
Fakulti Pengurusan Teknologi dan Perniagaan
Universiti Tun Hussein Onn Malaysia

G	**Establishment of IT security parameter, Anti-Malware software to protect any Malware activities in the IT environment.**					

Item yang relevan dan bertepatan dengan tujuan kajian.

Part 8 IT Security Objective

Please indicate the level of agreement with the following statements in relation to implement IT security objective of university		Strongly Agree **10**	Agree **8**	Neutral **6**	Disagree **4**	Strongly Disagree **2**
A	**The requirement of confidentiality achievement on IT security for organization is important.**					
B	**The requirement of integrity on IT security for organization is important.**					
C	**The requirement of availability achievement on IT security for organization is important.**					

Please share any comments you have on the topics addressed in this survey.

Item-item yang dibina adalah sesuai dan relevan dengan objektif kajian dan keperluan analisis. Tahniah.

Sedikit sahaja disarankan untuk ditambah.

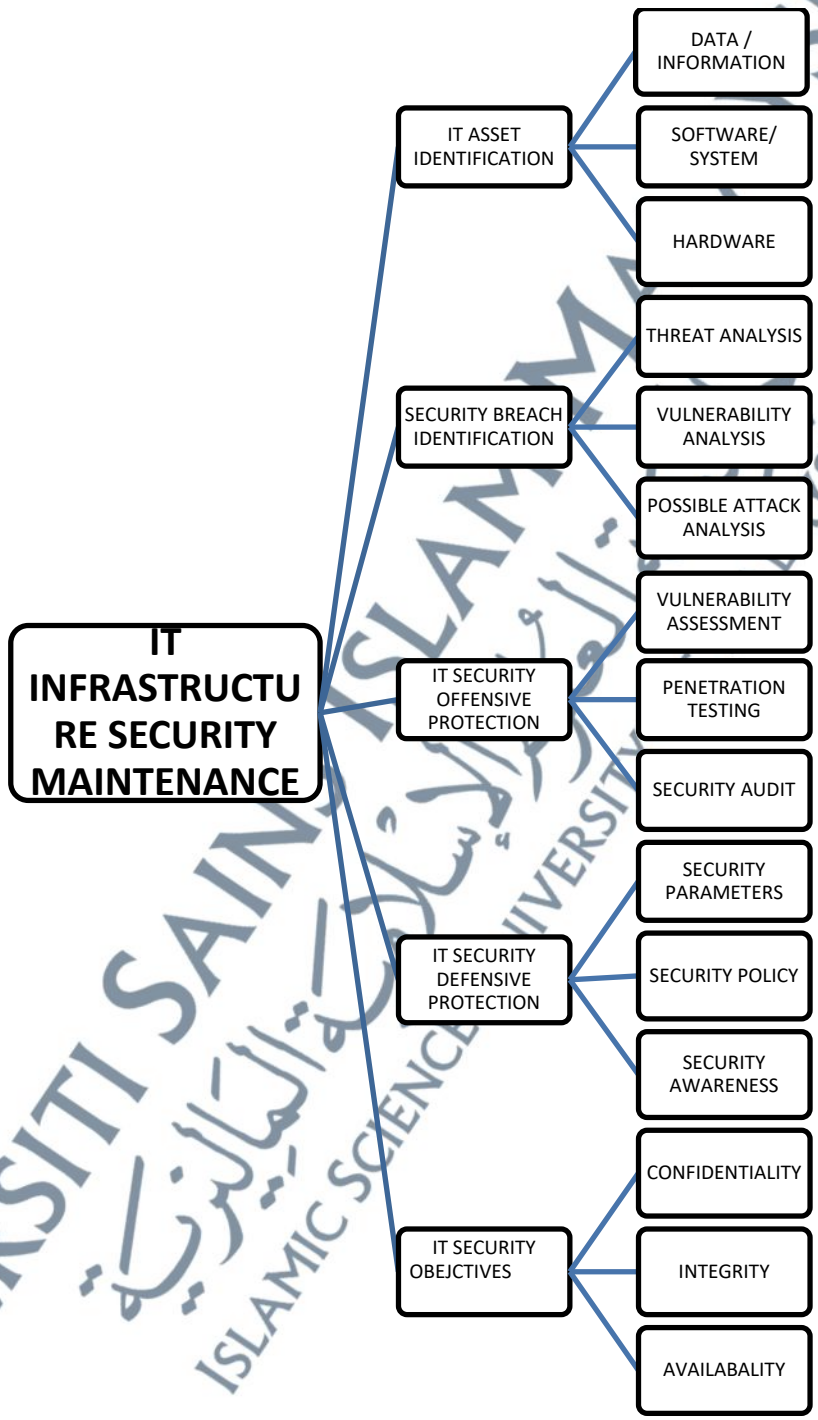
21/12/2021

DR. MOHD NORAZMI BIN NORDIN
Penyarah Universiti DS51
Fakulti Pendidikan
Universiti Kebangsaan Malaysia

Thanks for helping out with our survey. We appreciate your feedback.

APPENDIX D: Interview Form for Framework Validation

SECTION A: Framework of IT Security Maintenance.



SECTION B: Rating

Please tick to the relative score for each validation aspect below to represent the extent of satisfaction (from 1 = very poor, 2 = poor, 3 = medium, 4 = good, 5= very good).

Validation Criteria	Scoring Scale				
	Very Poor	Poor	Medium	Good	Very Good
	1	2	3	4	5
1. Appropriateness (Kewajaran)					
2. Objectivity (Kebolehcapaian)					
3. Practicality / Feasibility (Kebolehlaksanaan)					
4. Reliability (Kebolehpercayaan)					
5. Suitability of model in current practice					

SECTION C: Questions

1. Can this framework be applicable in current practice?
   Bolehkah kerangka ini diguna pakai dalam amalan semasa?
   Answers:

2. Can this framework address the governance issues in IT security maintenance implementation?
   Bolehkah kerangka ini menangani isu-isu tadbir urus dalam penyelenggaraan keselamatan IT?
   Answers:

3. What are the problems arising if this framework been used in IT security maintenance implementation? If any, how can these problems are addressed?
   Apakah masalah yang boleh timbul jika kerangka ini digunakan dalam perlaksanaan penyelenggaraan keselamatan IT? Jika ada, bagaimana masalah ini dapat ditangani?
   Answers:

4. Any recommendations to enhance the quality of the framework so that it can applicable in current practice?
   Cadangan untuk meningkatkan kualiti kerangka ini supaya ia boleh diguna pakai dalam amalan semasa dan pada masa akan dating?
   Answers:

APPENDIX E: Respondent's Response on Framework Validation

Respondents	Questions			
	Can this framework be applicable in current practice?	Can this framework address the governance issues in IT security maintenance implementation?	What are the problems arising if this framework been used in IT security maintenance implementation? If any, how can these problems are addressed?	Any recommendations to enhance the quality of the framework so that it can applicable in current practice?
R1	This model can be used but must do early stage study and must consider other factors.	It's depend on the government environment issues.	The problem that might occur is the enforcement of the IT security. Some time, policy that been created is not 100% follow.	The organization must ensure the security policy must go along the implementation.
R2	Yes, especially with the requirement	Yes, this model incorporate security breach identification, offensive	Any potential problems can be addressed by a systematic execution and	Please look into ISO 27001 components.

	of ISO 27001(ISMS)	protection and defensive protection that are able to support IT security maintenance implementation on the governance matters.	consistence enforcement.	
R3	Sure. Model should implement in current practice. However, it depend on the budget constraint and readiness of technical teams. (training)	Yes. But model should consider how to control the security operations to achieve the objectives.	Budget, the readiness of the technical teams and the resources.	Consider to add on services as inventory and how to control the measurement of operations.

R4	Ya, dengan pemahaman yang jelas berkenaan konsep dan peranan setiap sub model dan bajet.	Ya, dengan struktur yang jelas.	Bajet dan sumber kewangan. Latihan dan kesedaran.	Melihat dari segi latihan kepada staf IT. Keselamatan ICT adalah tanggung jawab semua.
R5	Boleh guna.	Boleh dan perlu dipraktiskan di semua agensi.	Perlu ada 2 jenis kawalan luran (Daripada internet) dan dalaman (Rangkaian dalaman seperti LAN,WLAN)	Penerangan kepentingan keselamatan yang perlu dilaksanakan di semua organisasi.
R6	Boleh dan amat praktikal.	Boleh. Ia adalah satu model yang baik.	Perkembangan teknologi yang pesat menjadi cabaran utama kerana tools yang bertukar-tukar. Masalah	Menyatakan teknologi dan solution/tools yang boleh digunakan semasa model ini disediakan.

			ini boleh diatasi dengan penyediaan pelan latihan kepada staf secara berterusan, Disamping itu, peruntukan kewangan juga perlu disediakan dengan konsisten dan bersesuaian dengan keperluan.	