UNIVERSITI TEKNOLOGI MARA
FACULTY OF INFORMATION MANAGEMENT

INDUSTRIAL TRAINING REPORT:
CYBERSECURITY MALAYSIA (SELANGOR)
MENARA CYBER AXIS, JALAN IMPACT 63000 CYBERJAYA

SPECIAL PROJECT: PRIVACY AWARENESS WEBSITES

BY
MUHAMMAD FIRDAUS BIN NAZARUDIN
2016316991

IM245 - BACHELOR OF SCIENCE (HONS.) INFORMATION SYSTEM MANAGEMENT
FACULTY OF INFORMATION MANAGEMENT
UNIVERSITI TEKNOLOGI MARA KELANTAN

01 FEBRUARY 2019 – 28 JUNE 2019

INDUSTRIAL TRAINING REPORT:
CYBERSECURITY MALAYSIA (SELANGOR)

SPECIAL PROJECT: PRIVACY AWARENESS WEBSITES

BY
MUHAMMAD FIRDAUS BIN NAZARUDIN

FACULTY SUPERVISOR
SALLIZA BT MD RADZI

REPORT SUBMITTED IN FULFILLMENT OF THE
REQUIREMENT FOR THE INDUSTRIAL TRAINING
FACULTY OF INFORMATION MANAGEMENT
UNIVERSITI TEKNOLOGI MARA KELANTAN

01 FEBRUARY 2019 – 28 JUNE 2019

List Of Table

DECLARATION

I hereby declare that this is my original work. I have not copied from any other student's work or from other sources. I am also declare that no part of this report has been published or submitted for publication except where due to reference or acknowledgement is made explicitly in text, nor has any part been written for me by another person. I confirm that I have read and understood the UiTM regulations with regards to plagiarism and will be penalized by the university if found guilty.

Signed by

_____

Muhammad Firdaus Bin Nazarudin
20176682435

Date of submission: 4 July 2019

ABSTRACT

The trainee internship at CyberSecurity Malaysia in department Information Security and Assurance started from 2nd February 2019 until 28th June 2019. During the internship program the trainee are involve in development privacy guidance and framework based on ISO 27552. Besides, the trainee also acknowledges ISO 27001, ISO 27002 and ISO 29001. Moreover, the trainee also have involve in several activity which is conduct research, troubleshoot ISMS, charity program, and others. Next, the trainee chooses to develop the privacy awareness websites as a special project. The reasons choose to develop the privacy websites it to ensure the community in Malaysia aware about the privacy and can implements tips to protect the data privacy. The trainee can learn something news during internship program and also can implements the knowledge that learns at faculty towards internship program.

Keywords: *Research, privacy, privacy awareness websites, ISO27552*

ACKNOWLEDGEMENT

First and foremost, I am very grateful to Allah S.W.T for giving me the strength and opportunity to complete my industrial training in 5 months without any difficulty. I do thank for his blessing that granted me good health, healthy mind and long life during my industrial training. The internship opportunity I had with CyberSecurity Malaysia was a great chance for learning and professional development. Therefore, I consider myself as a very fortunate individual as I was provided with an opportunity to be a part of it. I am also grateful for having a chance to meet so many wonderful people and professionals who led me through this internship period.

I am using this opportunity to express my deepest gratitude and special thanks to my Industry supervisor, Mrs Sabariah Bt Ahmad who treat me like his own staff without any discrimination. Furthermore, he always give comments and advice not only about my industrial training but also for my real working in future. She also helped and coached me during my internship by giving me feedback and tips on how to handle and approach situations. Her constant guidance and advice played the vital role in my industrial training. I also indebted to Mrs Naqliyah who always guide me in completing the tasks at the office. Without her continuous guidance, support and idea throughout this industrial training, I might not doing really well. Special thanks to the rest of all staff in Information Security and Assurance Department for their support and guidance which helped me to overcome the obstacles I faced during the past 5 months.

I would like to thanks my Lecturer Madam Salliza Bte Md Razi who is the person in charge as my University Supervisor for his valuable guidance and advice. Her always have time in answering my questions regarding the special project. Her always give his critics in helping me to improve my special project from time to time. For sure I also want to express my appreciation to my beloved parents and family who are always give support and prayed for my success in my life and studies. Lastly, I also want to thank all people who are helping me indirectly or directly to finish this assignment. I realized that without the help and support from all those special person, I might not finished this assignment on time and successfully. On other hand, I perceive as this opportunity is a big milestone in my career development. As for me, it helped me discover my potential. I have had so many experiences and opportunities that I personally believe will forever shape and influence my professional life while fostering personal growth and development.

Table of Contents

List of Figure

1. Chapter 1: Introduction

A well-known Chinese Philosopher named Confucious once said, 'I hear and I Forgot, I see and I remember, I do and I understand.' In other words, the process learning in class, sometimes give difficulties to student in remembering and understand about the syllabus. However, they will simply understand and remember when they have their own experience in practicing about what they learn in the class during their industrial training. Moreover, Industrial Training is a platform in giving exposure to the students about the reality in a working environment and preparing the students for a professional career. As a consequences, the students were trained to be job-ready before they graduated and also increase their opportunities to get permanent job in their Industrial Placement.

1.1 Background of organization

Cybersecurity Malaysia is one of the organization that provide cybersecurity innovation led services, programmers and initiatives to help reduce the vulnerability of digital system and at the same time strengthen Malaysia self-reliance in cyberspace. Cybersecurity Malaysia journey started with the creation of the Malaysia Computer Emergency Response Team or MyCERT on the 13th of January 1997 as a unit under MIMOS Berhad. On the 24th of January 1998, the National Information Technology Council or NITC proposed for the establishment of an agency to address emerging ICT security issues in Malaysia. As a result, the National ICT Security & Emergency Response Centre (NISER) was created in 2001 as a department in MIMOS Berhad, and the Malaysia Computer Emergency Response Team (MyCERT) was placed under NISER. On 28th September 2005, the Cabinet decided for NISER to be spun-off from MIMOS Berhad as a separate entity under MOSTI. On 30th March 2007, NISER was registered as a not-for-profit Company Limited by Guarantee.

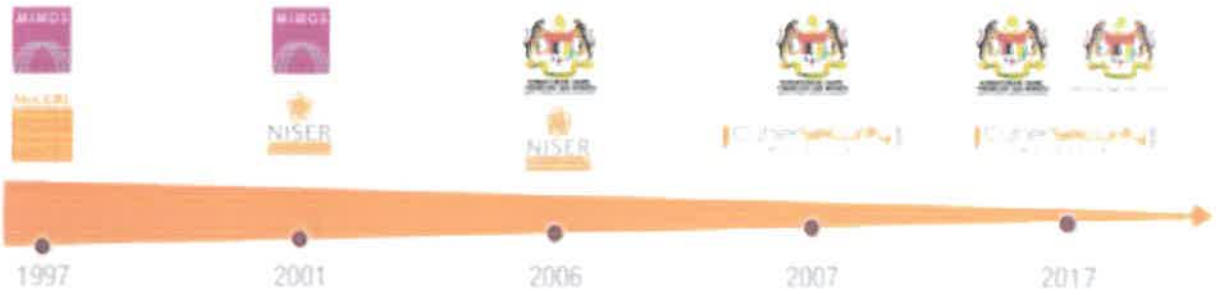


Figure 1. 1 History Timeline

On the 20th of August 2007, the Prime Minister of Malaysia officiated the rebranding of NISER into CyberSecurity Malaysia, and launched the new CyberSecurity Malaysia brand name and logo. Cybersecurity Malaysia provides specialized cyber security services, which is cyber security responsive services, cyber security proactive services, outreach and capacity building strategic study and engagement and Industry and research development.

In this organization have eleven departments which is The Malaysian Computer Emergency Response Team (MYCERT) and Cyber 999, Digital Forensic (Cyber CSI), Malaysian Security Evaluation Facility (MySEF), Malaysian Vulnerability Assessment Centre (MyVAC), Information Security Certification Body, Security Management & Best Practices, Industry Development, Government & International Engagement, Cyber Security Research, Cyber Security Professional Development and Outreach.

Headquarters CyberSecurity Malaysia is located at The Mines Resort Seri Kembangan Selangor from 2007 until April 2019. On April 2019, CyberSecurity Malaysia moved out to new building at Menara Cyber Axis Cyberjaya Selangor. In this building have four organization which Cybersecurity Malaysia, National Cyber Security Agency (Nacsa), Standard Malaysia and MYNIC.

Figure 1. 2 The Mines Business Park

Figure 1. 3 Menara Cyber Axis

Vision

Our vision is to be a globally recognised National Cyber Security Reference and Specialist Centre by 2020.

Mission

Our mission is to create and sustain a safer cyberspace to promote National Sustainability, Social Well-Being and Wealth Creation.

Core Values

- **Trust**

  By maintaining social, ethical and organizational norms, we firmly adhere to codes of acceptable conduct and professional ethical principles.

- **Impartiality**

  By providing consultation, advice and decision making with professionalism based on established facts and rationale, and devoid of any personal or conflict of interest and bias.

- **Proactive**

  By taking prompt action to accomplish objectives; anticipating challenges and identifying early solutions; taking action to achieve goals beyond what is required or expected.

1.2 Organizational Structure

Board of Directors

General Tan Sri Dato' Seri Panglima Mohd Azumi Bin Mohamed (Retired)

Chairman Board of Directors

YBhg. Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab

Director / Chief Executive Officer

Datuk Dr. Abdul Raman Bin Saad

Director

Dr. Suhazimah Binti Dzazali

Director

Haji Suip @ Kanik bin Saniman @ Kadad

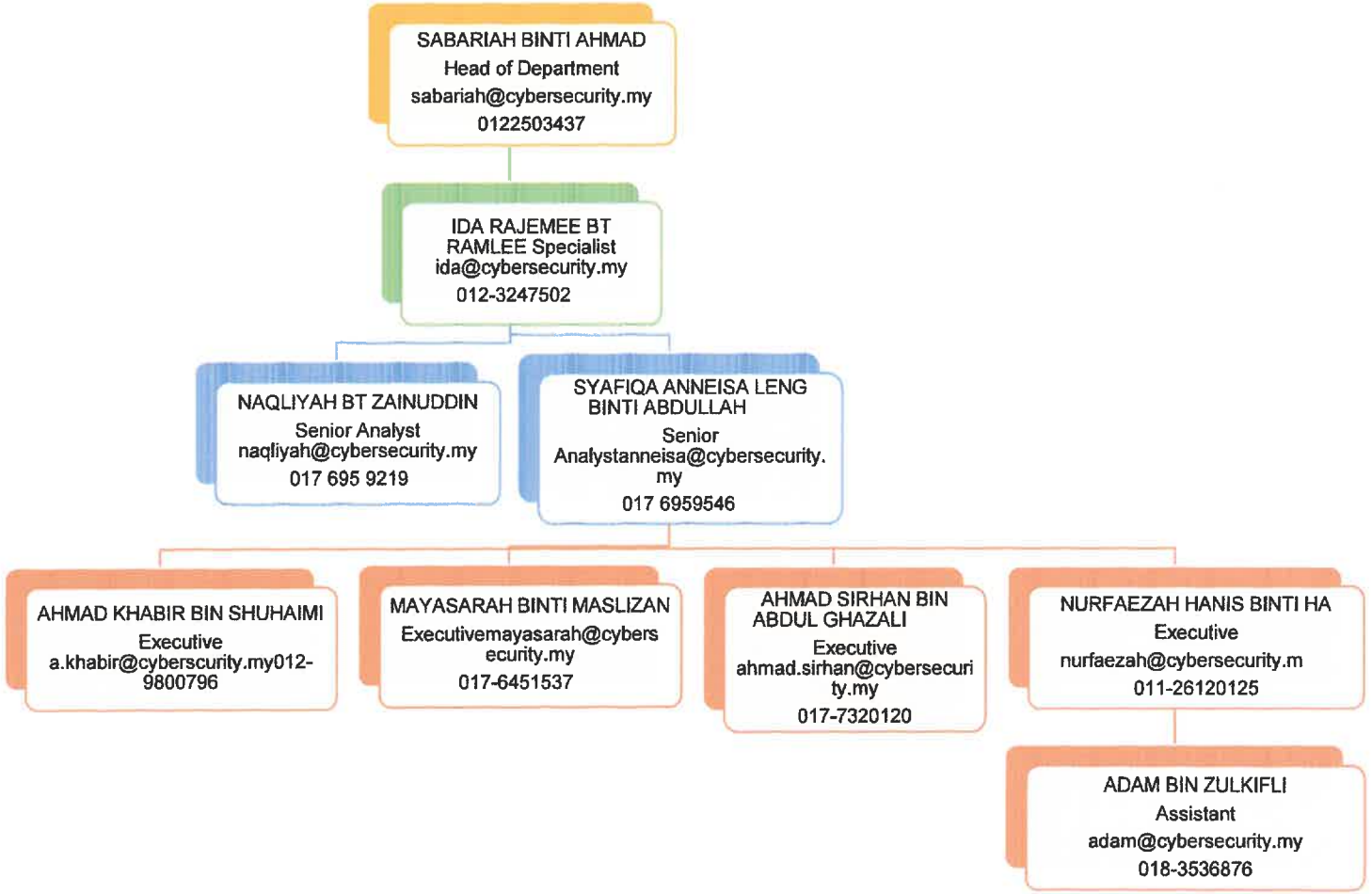
Director

Puan Azizatul Yusna Binti Yusuf

Director

2. Chapter 2: Organization Information

2.1 Departmental Structure (Security Management and Best Practices)



Security Management and Best Practices (SMBP) is one of the departments in CyberSecurity Malaysia that manage and provide the guideline that use by CyberSecurity Malaysia or their client. In this Department, there are eight staffs which are one head of department, one specialist, two senior analyst, four Executive staff and one assistant. On February 2019, the name of Security Management and Best Practices department had been change to Information Security Management and Assurance (ISMA). However, the roles and job scopes for this department are not changing. ISMA department can be divided into three units which are research, Information security management system (ISMS) and Business Continuity plan (BC). All units have their own responsibilities and job scopes that set by Head of department in ISMA.

Table 2. 1 List of Group

No	Name	Group
1	Naqliyah bt Zainuddin	Research
2	Mayasarah binti Maslizan	Research
3	Ida Rajemee bt Ramlee	ISMS
4	Nurfaezah Hanis binti Halim	ISMS
5	Ahmad Sirhan bin Abdul Ghazali	ISMS
6	Syafiqa Anneisa Leng binti Abdullah	BC
7	Adam bin Zulkifli	BC
8	Ahmad Khabir bin Shuhaimi	BC

2.2 Department Function

2.2.1 Security Management & Best Practices (SMBP)

The primary role of Security Management & Best Practices (SMBP) department is to drive information security management based on ISO/IEC 27001 Information Security Management System (ISMS) for CyberSecurity Malaysia. This includes planning, developing, implementing and monitoring ISMS such as information security risk management, information security awareness programs, information security management review, development of information security policies and procedures and Business Continuity Management (BCM). This department is also entrusted in giving trainings and awareness talks about ISMS to external organizations. In addition, this department also develops information security guidelines with its best practices to the public. Therefore, it can assist them in securing their information security environment.

This department also give contribution towards standardization development in information security at both local and international level. Moreover, this department is glad to invite everyone in visiting their published guidelines and best practices. Otherwise, ISMA also lead the internal auditor of ISO 27001 in Cybersecurity Malaysia. There are 4 auditors who have authority and certificate in ISO 27001. Those 4 staffs will lead the external and internal auditor activities in the whole building of Cybersecurity Malaysia.

3. Chapter 3: Industrial Training Activities

As a trainee in ISMA for 5 months, trainee had opportunities in using the skills and knowledge as Information System Students. In addition, trainee had experienced the reality in managing and controlling all the active documents and correspondences in the department and understand and practice ISO 27001, 27002, 27552 and 29001.

3.1 Training Activity

Industrial Training can provide a chance to trainee in applying theoretical knowledge gained from the classroom with practical application of knowledge in performing tasks. Thus, these are several activities during internship program in CyberSecurity Malaysia which is research, auditor checklist, cafe ilmu, develop research paper, maintaining and troubleshoot ISMS, moving out to new building, banking framework, charity program and jamuan hari raya.

3.1.1 Research

The trainee received task to work with the research team. In this activity, the trainee need to make a research about several topics given by the team leader who named Madam Naqliyah bt Zainuddin. First task for this activity was the trainee need to make research about the privacy at 3 sector which is Bank sector, Health Care sector and Telecommunication sector. First of all, the trainee need to compare the definition of privacy from several articles. After that, the trainee need know what the new issues and problems that faced by Bank sector, Health care sector and Telecommunication sector. Moreover, the trainee also need to make a comparative analysis, submit and present it to team leader Madam Naqliyah bt Zainuddin. Besides, the trainee also need to develop the flow chart and framework for Personal Identifier information (PII) for this three sectors in understanding how they manage and receive the data privacy. The several articles, act and standards that used by trainee as references to make research for this activities.

Table 3. 1 List of article, act and standard

No	Article / Act / Standards	Years
1	Health information privacy and security framework: supporting electronic medical records in healthcare system	2017
2	Information flow in time of crisis: The case of the European Banking and Sovereign Sector	2019
3	Open Banking privacy at the epicentre	2018
4	The Impact of Management Information system effectiveness on task productivity case of the Greek banking sector	2016
5	Mobile Payment in India: the privacy factor	2017
6	The Value of Protecting Privacy	2019
7	Personal Data protection Act	2010
8	HIPAA	2019
9	ISO Standard (ISO 27552, ISO 29001)	2019, 2010

After that, the trainee also gets the new task from Mrs Naqliyah to make a research about Industry revolution 4.0, Internet of things and Cyber Threat at Airport. First of all, the trainee needs to understand the industry 4.0 and industry revolution 4.0. For the information industry 4.0 and industry revolution 4.0 is different. Industry 4.0 is more focus to smart factory and industry revolution 4.0 is cover for all sector like smart city, smart healthcare and others. The trainee need identify the risk and problem that faced by industry and this country when using IR 4.0. The trainee also should understand the positive and negative impact towards privacy and security when implementation IR 4.0 in this country. After the trainee understand the IR 4.0, the trainee need make comparative analysis and submit and presentation to team leader Madam Naqliyah bt Zainuddin.

Moreover, the trainee also makes research about the Cyber Threat at airport. For this topic the trainee need make a research about the types of threats, the hardware and software that use by hackers, types of hackers and the most problems and risk that faced by airport at worldwide. All information collects need to make comparative analysis. This is several articles, book and journal that use by trainee as references to make research for IR 4.0 and Cyber Treat at Airport.

Table 3. 2 List of article, book and journal

No	Article/Book/Journal	Years
1	Overcome the silent Threat : Building cyber resilience in airport	2018
2	Aviation insider treat: What We Know, our Finding and What we recommend	2017
3	Securing Smart Airports	2016
4	Smart Airport cybersecurity: Threat mitigation and cyber resilience controls	2019
5	The Internet of things (IoT) and its impact on individual privacy: An Australian perspective	2016
6	Regulation and governance of the Internet of Things in India	2018
7	Enhancing social networking in smart cities: Privacy and security borderlines	2018
8	Security and privacy challenges in smart cities	2018

3.1.2 Auditor checklist ISO/IEC 27552

ISO/IEC 27552 is standard for privacy information management requirements and guidelines. This standard is extension to ISO/IEC 27001 and ISO/IEC 27002. While ISO/IEC DIS 27552 provides guidance for the protection of the privacy which enables the organization management system covered on general and specific requirement for personal identifiable information (PII) protection. Furthermore, this standard also consists of additional requirements and guidance that usable for protection of the PII by all types and size of organizations. After that, this standard focuses on Privacy Information Management System (PIMS). PIMS is information security management system which addresses the protection of privacy as potentially affected by the processing of PII. ISO/IEC 27552 have eight clauses which are clauses 1 scope, clauses 2 normative references, clauses 3 terms, definition and abbreviations, clauses 4 general, clauses 5 PIMS specific requirements related to ISO/IEC 27001, clauses 6 PIMS-specific guidance related to ISO/IEC 27002, clauses 7 additional ISO/IEC 27002 guidance for PII controllers and clauses 8 Additional ISO/IEC 27002 guidance for PII processors. This standard more focus on three actors which are are:

i. **PII PRINCIPLE**

Personal Identifiable Information (PII) Principle is a natural person to whom the personally identifiable information (PII) relates to, which is the owner of the data or information it is.

ii. **PII PROCESSOR**

Personal Identifiable Information (PII) Processor is a privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller. PII processor is the person or organizations that process the user PII on the behalf of the PII Controller with authority given by PII Controller.

iii. PII CONTROLLER

Personal Identifiable Information (PII) Controller is privacy stakeholder that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes. Which mean, the organization that holds and collects the data of the PII principle for the purpose of business and transaction.

The trainee get new task to develop auditor checklist ISO/IEC 27552. First of all, the trainee needs to understand all clauses and objective of ISO/IEC 27552. The objectives auditor checklist is to guide and help the auditor to make the audit for ISO 27552, ensure that the audit scope is being followed, ensure a consistent audit approach and be used as an information base for planning future audits. With this checklist, the auditor can easily to ask a question to their client and auditor also easily get the answer. The trainee develop question for clause 5 and clause 7. The duration for this activity take 5 month start from research phase until develops the question and guideline. Some clause in ISO/IEC 27552 have additional requirement from ISO/IEC 27001 and ISO/IEC 27002.

Table 3. 3 Additional requirement ISO 27001

Clause number in ISO/IEC 27001:2013	Title	Sub-clause number in this document	Remarks
4	Context of the organization	5.2	Additional requirements
5	Leadership	5.3	No PIMS-specific requirements
6	Planning	5.4	Additional requirements
7	Support	5.5	No PIMS-specific requirements
8	Operation	5.6	No PIMS-specific requirements
9	Performance evaluation	5.7	No PIMS-specific requirements
10	Improvement	5.8	No PIMS-specific requirements

Table 3. 4 Additional requirement ISO 27002

Clause number in ISO/IEC 27002	Title	Sub-clause number in this document	Remarks
5	Information security policies	6.2	Additional guidance
6	Organization of information security	6.3	Additional guidance
7	Human resources security	6.4	Additional guidance
8	Asset management	6.5	Additional guidance
9	Access control	6.6	Additional guidance
10	Cryptography	6.7	Additional guidance
11	Physical and environmental security	6.8	Additional guidance
12	Operations security	6.9	Additional guidance
13	Communications Security	6.10	Additional guidance
14	System acquisition	6.11	Additional guidance

This is first time trainee develop the auditor checklist. The trainee learns a lot from senior auditor to develop the auditor checklist. After the first draft is complete, the trainee need to present in front senior analyst, auditor and supervisor. Three times the trainee need to redo the question in checklist to ensure that checklist is easily to understand and have quality. Clauses five has eight sub clause which is 5.2 context of organization, 5.3 leadership and commitment, 5.4 action to address risks and opportunities, 5.5 resources, 5.6 operation,5.7 monitoring, measurement, analysis and evaluation, 5.8 improvement. Next, clause seven has five sub clauses which is 7.2 conditions for collection and processing, 7.3 obligations for PII Principle, 7.4 privacy by design and privacy by default, 7.5 PII sharing, transfer and disclosure. This is example of auditor checklist ISO/IEC 27552 for clause 5 and clause 7.

Clause #	Content	Question	Document Information References	Explanation Comment
5	PIMS-specific requirements related to ISO/IEC 27001			
5.2	Context of organization			
5.2.1	Understanding the organization and its context			
	The organization shall determine its role as a PII controller (including as a joint PII controller) and/or a PII processor.		1. Review of the policy and procedure that related to role of the PII controller and processor.	
5.2.1	The organization shall determine external and internal factors that are relevant to its context and that affect its ability to achieve the intended outcome(s) of its PIMS. For example, these can include: • Applicable privacy legislation; • Applicable regulations; • Applicable judicial decisions; • Applicable organizational context, governance, policies and procedures; • Applicable administrative decisions; • Applicable contractual requirements.		1. Review of the policies and procedure on internal and external factors	
5.2.1	Where the organization acts in both roles (e.g. a PII controller and a PII processor), separate roles shall be determined, each of which is the subject of a separate set of controls.		1. Review of the policies and procedures on PII controller and PII processor	

Figure 3. 1 Clause 5.2

Clause #	Content	Question	Document Information References	Explanation Comment
5.3	Leadership			
5.3.1	Leadership and commitment			
	Top management shall demonstrate leadership and commitment with respect to the information security management system by: a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization; b) ensuring the integration of the information security management system requirements into the organization's processes; c) ensuring that the resources needed for the information security management system are available; d) communicating the importance of effective information security management and of conforming to the information security management system requirements; e) ensuring that the information security management system achieves its intended outcome(s); f) directing and supporting persons to contribute to the effectiveness of the information security management system; g) promoting continual improvement; and h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.	1. How top management demonstrate leadership and commitment with respect to the information security management system?	1. Review the achievement of organization 2. Review the policy and procedures 3. Review the roles of leadership	

Figure 3. 2 Clause 5.3

Clause #	Content	Question	Document Information References	Explanation Comment
5.4	Planning			
5.4.1	Actions to address risks and opportunities			
5.4.1.1	General			
	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement. The organization shall plan: d) actions to address these risks and opportunities; and e) how to: 1) integrate and implement the actions into its information security management system processes; and 2) evaluate the effectiveness of these actions.		1. Review related document or plan on action to address risk and opportunities 2. Review related document or plan on how to integrate and implement the actions into its information security management system processes. 3. Review document on to evaluate the effectiveness of these actions.	

Figure 3. 3 Clause 5.4

Clause #	Content	Question	Document Information References	Explanation Comment
5.5				
5.5.1	Resources:			
	The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	1. How organization determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system?	1. Review the policy and procedure that related with resources	
5.5.2	Competence:			
	The organization shall: a) Determine the necessary competence of person(s) doing work under its control that affects its information security performance; b) Ensure that these persons are competent on the basis of appropriate education, training, or experience; c) Where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d) Retain appropriate documented information as evidence of competence.	1. How organization ensure competence of person(s) doing work under its control that affects its information security performance? 2. How organization ensure that these staff are competent on the basis of appropriate education, training, or experience? 3. What are the action taken by organization to acquire the necessary competence of staff?	1. Review the policy and procedure that related to competence 2. Review the documentation and reporting of competence	

Figure 3. 4 Clause 5.5

Clause #	Content	Question	Document Information References	Explanation Comment
5.6	Operation			
5.6.1	Operational planning and control			
	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2. The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall ensure that outsourced processes are determined and controlled.		1. Review the relevant policy and procedure on operational planning and control 2. Review the reporting and document operational and control	
5.6.2	Information security risk assessment			
	The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a). The organization shall retain documented information of the results of the information security risk assessments.		1. Review of related policy and procedure on information security risk assessment 2. Review of the related document information security risk assessment which is : a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;	

Figure 3. 5 Clause 5.6

Clause #	Content	Question	Document Information References	Explanation Comment
5.7	Performance Evaluation			
5.7.1	Monitoring, measurement, analysis and evaluation			
	The organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall determine: a) what needs to be monitored and measured, including information security processes and controls; b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results; c) when the monitoring and measuring shall be performed; d) who shall monitor and measure; e) when the results from monitoring and measurement shall be analysed and evaluated; and f) who shall analyse and evaluate these results the organization shall retain appropriate documented information as evidence of the monitoring and measurement results.	1. How organization evaluate the information security performance and the effectiveness of the information security management system?	1. Review any document that relate on monitoring, measurement, analysis and evaluation information security management. 2.Review the method that use for	

Figure 3. 6 Clause 5.7

Clause #	Content	Question	Document Information References	Explanation Comment
5.8	Improvement			
5.8.1	Nonconformity and corrective action			
	When a nonconformity occurs, the organization shall: a) react to the nonconformity, and as applicable: 1) take action to control and correct it; and 2) deal with the consequences; b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur; c) implement any action needed; d) review the effectiveness of any corrective action taken; and e) make changes to the information security management systems, if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered.	1. How organization evaluate the nonconfirmity? 2. How organization manage to solve and take action which is to control and correct it? 3. How organization deal with the consequences or recur or occur again? 4. How organization ensure that the issues are not happen again?	1.Review any document that related on nonconformity and corrective action 2. Review the related policy and procedure on nonconformity and corrective action	

Figure 3. 7 Clause 5.8

Clause #	Content	Question	Document Information References	Explanation Comment
7	Additional ISO/IEC 27002 guidance for PII controllers			
7.2	Conditions for collection and processing			
7.2.1	Identify and document purpose			
	Control The organization should identify and document the specific purposes for which the PII will be processed. Implementation guidance The organization should ensure that PII principals understand the purpose for which their PII is processed. It is the responsibility of the organization to clearly document and communicate this to PII principals. Without a clear statement of the purpose for processing, consent and choice cannot be adequately given. Documentation of the purpose(s) for processing PII should be sufficiently clear and detailed to be usable in the required information to be provided to PII principals (see 7.3.2). This includes information necessary to obtain consent (see 7.2.3), as well as records of policies and procedures (see 7.2.8).	1. How organization identify and document the specific purpose for PII will be processed? 2. How organization ensure that PII principals understand the purpose for which their PII is processed?	1. Review the related policies and procedure on identify and document purpose.	

Figure 3. 8 Clause 7.2

Clause #	Content	Question	Document Information References	Explanation Comment
7	Additional ISO/IEC 27002 guidance for PII controllers			
7.3	Obligations to PII principals			
7.3.1	Determining and fulfilling obligations to PII principals			
	Control The organization should determine, document and comply with their legal, regulatory and business obligations to PII principals related to the processing of their PII and provide the means to meet these obligations. Implementation guidance Obligations to PII principals and the means to support them vary from one jurisdiction to another. The organization should ensure that they provide the appropriate means to meet the obligations to PII principals in an accessible and timely manner. Clear documentation should be provided to the PII principal describing the extent and manner in which the obligations to them are fulfilled, along with an up-to-date contact point where they can address their requests. The contact point should be provided in a manner similar to the one used to collect PII and consent (e.g. if PII are collected by email or a website, the contact point should be by email or the website, not an alternative such as phone or fax).	1. How organization determine, document and comply with their legal, regulatory and business obligations to PII principals? 2. How organization ensure that they provide the appropriate means to meet the obligations to PII principals in an accessible and timely manner?	1. Review any legal and regulatory and business obligations to PII principles. 2. Review any documentation provided to PII principle 3. Review any contact point	

Figure 3. 9 Clause 7.4

Clause #	Content	Question	Document Information References	Explanation Comment
7	**Additional ISO/IEC 27002 guidance for PII controllers**			
7.4	**Privacy by design and privacy by default**			
7.4.1	**Limit collection**			
	Control The organization should limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes. **Implementation guidance** The organization should limit the collection of PII to what is adequate, relevant and necessary in relation to the identified purposes. This includes limiting the amount of PII that the organization collects indirectly (e.g. through web logs, system logs, etc.). Privacy by default implies that, where any optionality in the collection and processing of PII exists, each option should be disabled by default and only enabled by explicit choice of the PII principal	1. How organization limit the collection of PII to the minimum?		
7.4.2	**Limit processing** **Control** The organization should limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes. **Implementation guidance** Limiting the processing of PI needs to be managed through information security and privacy policies (see 7.2) along with documented procedures for their adoption and compliance. Processing of PII, including the period of PII storage and who is able to access the PII, should be limited by default to the minimum necessary relative to the identified purposes.	1. How organization limit the processing of PII?	1. Review any information security and privacy policies 2. Review any of the documented procedures for the adoption and compliance	

Figure 3. 10 Clause 7.4

A Clause #	B Content	C Question	D Document Information References	E Explanation Comment
7	**Additional ISO/IEC 27002 guidance for PII controllers**			
7.5	**PII sharing, transfer, and disclosure**			
7.5.1	**Identify basis for PII transfer between jurisdictions**			
	Control The organization should identify and document the relevant basis for transfers of PII between jurisdictions. **Implementation guidance** PII transfer can be subject to laws or regulations depending on the jurisdiction or international organization to which data is to be transferred (and from where it originates). The organization should document compliance to such requirements as the basis for transfer. Some jurisdictions may require that information transfer agreements be reviewed by a designated supervisory authority. Organizations operating in such jurisdictions should ensure they are aware of any such requirements.	1. How organization identify and document the relevant basis for transfers of PII between jurisdictions?	1. Review any laws or regulations depending on the jurisdiction or international organization 2. Review any of the information transfer agreements 2. Check on the documentation/report of information transfer agreements be reviewed by a designated supervisory authority	
7.5.2	**Countries and international organizations to which PII might be transferred** **Control** The organization should specify and document the countries and international organizations to which PII might possibly be transferred. **Implementation guidance** The identities of the countries and international organizations to which PII might possibly be transferred in normal operations should be made available to customers. The identities of the countries arising from the use of subcontracted PII processing should be included. The countries included should be considered in relation to 7.5.1 and any applicable legal or regulatory requirements. Out of normal operations, there can be cases of transfer made at the request of a law enforcement authority, for which the identity of the countries cannot be specified in advance, or is prohibited by applicable jurisdictions to preserve the confidentiality of a law enforcement investigation (see 7.5.1, 8.5.4 and 8.5.5).	1. How organization ensure, specify and document the countries and international organizations to which PII might possibly be transferred?	1. Review any document related to the countries and international organizations to which PII might possibly be transferred 2. Review any applicable legal or regulatory requirements related to countries and international organizations to which PII might be transferred 3. Review any of the law enforcement authority related to countries and international organizations to which PII might be transferred	

Figure 3. 11 Clause 7.5

Figure 3. 12 Clouse 7.5

3.1.3 Cafe Ilmu

Cafe Ilmu is sharing knowledge activity which any staffs in CyberSecurity Malaysia can share their story and hobby to others people. This activity organizes by Knowledge Management Department. The activity is every Wednesday from 9 am until 12.45 pm at Knowledge Management department. This activity became more interesting because the participant got free food and present. Participant also gained new knowledge. Cafe Ilmu is one of the platforms that can help internship student to be known and improve their confident to speak in front of crowd. Staff need to register their name with the staff at Knowledge department if they want to be the presenter. If the slots from that week are available staff will be email to participant to make sure they prepare the topic and slideshow for presentation.

At 27 March 2019, the trainee registered as presenter for the sharing knowledge activity. Others participants at that time are Shaifudin bin Sulaman from international engagement department (IE), Nabila Aqmar binti Razali who was also an internship student. Shaifudin bin Sulaman share about chrome extension for productivity and Nabila Aqmar binti Razali share about travel tips and tricks to Korea. All information they share will record by staff from Knowledge department and they will share this video to all staff in CyberSecurity Malaysia through email. For this activity, topic chose by the trainee to share with others was "Ainul Hayat". The reasons trainee chooses this topic because the story is rare and most people don't know about this story. This story is about prophet Khidir and King Zulkarnain travel around the world to find the water of life (Ainul Hayat). Moral value from the story are work hard, never give up, working in a team and being patient.

With this program the trainee can improve the communication skills and increase the confident during speaking in front people. Moreover, this program also teach trainee to make a new social connection with others staffs in CyberSecurity Malaysia and build leadership skill.

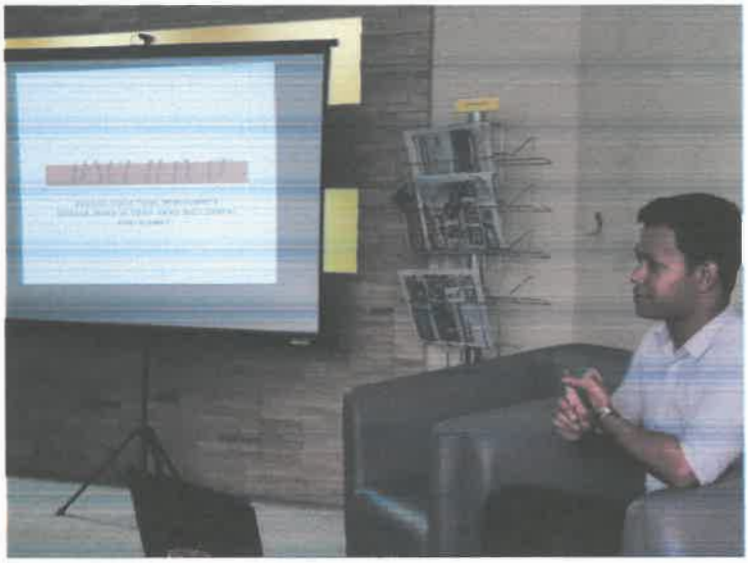


Figure 3. 13 Presentation Ainul Hayat

Figure 3. 14 Knowledge Sharing

3.1.4 Develop Research Paper

The trainee get new task from Madam Naqliyah which was to conduct research and writing the research paper. Duration of collection the information and make analysis is one week. The trainee needs review several articles, books and journals to collect the information, understand the topic and identify the issues from every resource. After collect the information the trainee need to make comparative analysis and need to consult and present to Madam Naqliyah. After get the approval, the trainees proceed to next stage which starts to write the paper. These papers have 6 parts which is abstract, introduction, and literature review, privacy term according to standard ISO/IEC 29100, way forward and conclusion. The title for this paper is "A study of Information Privacy personal identifiable information (PII)".

The aim of this paper is to acknowledge individual, organization, and government about data privacy implementation guidance. Thus, this paper also discussed the ecosystem of two sectors that are used as a representative to understand the reality of the ecosystem from different sector. Other than that, to provide a clear delineation of data privacy and security concern towards the readers. To encourage user understand privacy compliance from standard and legal framework or principles.

In this paper, have mention about the ISO 29001. ISO 29001 is privacy framework, this standards is intended to help organization define their privacy safeguarding requirements related to PII within an ICT environment by specifying a common privacy terminology, define the actors and their roles in processing PII and describing privacy safeguarding. This paper mention about the important of privacy to all organization and organization should make sure that all personal identifiable information (PII) is protected well.

3.1.5 Maintaining and troubleshoot ISMS

ISMS is stand for Information security management system. ISMS is define as that part of the overall management system, based on a business risk approach to establish, implement, operate, monitor, review, maintain and improve information security. The benefit of implementation ISMS improve overall governance structure in managing information security in the organization, improve control environment continuously and comply with legal and regulatory requirements. At 17 April 2019, Mr. Khabir and Mr. Sirhan give trainee new task which is assist them in maintaining and troubleshoot ISMS. The trainee and others two staff went to MAMPU for troubleshoot the ISMS.

First of all, briefing had been given by Mr. Khabir before we got our task. The tasks given to the staff is identifying the bug which manage their database by using remote desktop and make a report for troubleshoot. The task become easier to the trainee because they understand the PHP coding and SQL. After that, Mr. khabir make a troubleshoot at that system and identify the port 139 and port 135 have a problem. Port 139 and 135 is not connecting with their server. The trainee make a report about the problem and the report need submit to client and one copy our organization store. Port 139 is port to transfer the file and printer sharing. Port 139 is one of the dangerous ports on the internet because it is easy target to be hack

Figure 3. 15 MAMPU

3.1.6 Moving out from Seri Kembangan to Cyberjaya

On April 2019, Cyber Security Malaysia was moving out to a new building in Cyberjaya Selangor. The trainee should help the staff in packing all things. These activities started from 9 April until 15 April 2019. Every single person in this department gave their hand. There are several activities during the program which are:

- **Pack all document**

  In this activity the trainee help all staff to pack all current documents in box. The trainee helped the staff in wrapping the box to make sure the item on the box secured. There are two types of box provided by organization which are moving box and confidential box. Moving box provided to all the staff to store their item and records while confidential box is to store all confidential and top secret records

- **Tagging box**

  Mrs. Nurfaezah Hanis binti Halim responsible in managing all activities. One of her task is developing the tagging to all boxes in ISMA. The function of tagging the box is to identify the box easily, avoid from lost and misplacing the box.

- **Appraisal Records**

  Appraising is the process of evaluating the documents whether they have value of not to the organization. In ISMA, the trainee and several staff appraised the records. Hence, they can decide either to dispose or store the records. Mrs. Nurfaezah Hanis give all staff the manual needs to follow by all the staffs in appraising activity.

- **Disposed Records**

  All records that not have value and not regularly use need to dispose. Besides, in context of record management, any records which kept in 5 to 7 years need to dispose if they have no value. In this organization they shred the records with shredder machine to dispose the records.

Figure 3. 16 Tagging Box

Figure 3. 17 Arrange the box

Figure 3. 18 Package all document

Figure 3. 19 Package all document

3.1.7 Banking Framework

The trainee get new task to assist Nabila Aqmar to establish the implementation framework of ISO/IEC 27552. For this task Nabila Aqmar need to develop three frameworks from different sector which is banking sector, telecommunication sector and health care sector. Our supervisor gives trainee to establish the Banking framework to assist Nabila Aqmar. The trainee started with research from several article, act, journal and book about movement of personal data and privacy in banking sector. After that, the trainees make analysis and identify several research from other researcher as a references to develop the Banking sector. This is one of difficult task that get in this internship program it is because the trainee not familiar with the banking sector and not have any knowledge about act and policy that use by banking sector at Malaysia. However, staff at this department always help and guide trainee to improve their work.

Banking sector is an organization or companies that provide services for financial management and financial assets which handle:

- Cash
- Credit
- Saving
- Loan
- Other financial transaction

Bank is an organization that can be trusted which is a safe place to store money and credit without doubtful and hesitate. Other than that, banking also provide loans services which include home mortgages, car loans, business loans, and any other related loans.

Banking sector is one of the popular sectors that handle privacy of personal data. Banks and other financial institutions managed a large volume of sensitive information such as account number, pin number and massive amount of transaction. Customer information is growing from day to day and banking sector need to handle that information properly. In addition, they also need to ensure that information is not being misuse by unauthorized person or lost. This sector has three actors along with their roles of PII which is PII principal, PII processor and PII controller. PII principal for this sector is customers that register to use the bank services.

All information provided by PII principal is important and need to be stored carefully. Examples of information provided by PII principal are name, Identification Card (IC) number, address, phone number etc. However, PII principal also provide the sensitive data such as pin number and account bank. As we know, all banks and financial institutions have their own privacy policy to ensure that the personal data shall not be shared without getting the permission from the data owner. Therefore, the customer must read and clearly understand the policy properly before sign any of the documents given to them. Below are the flow of PII in banking sector which show on how the flow of PII are distributed and managed with who is responsible on used it.

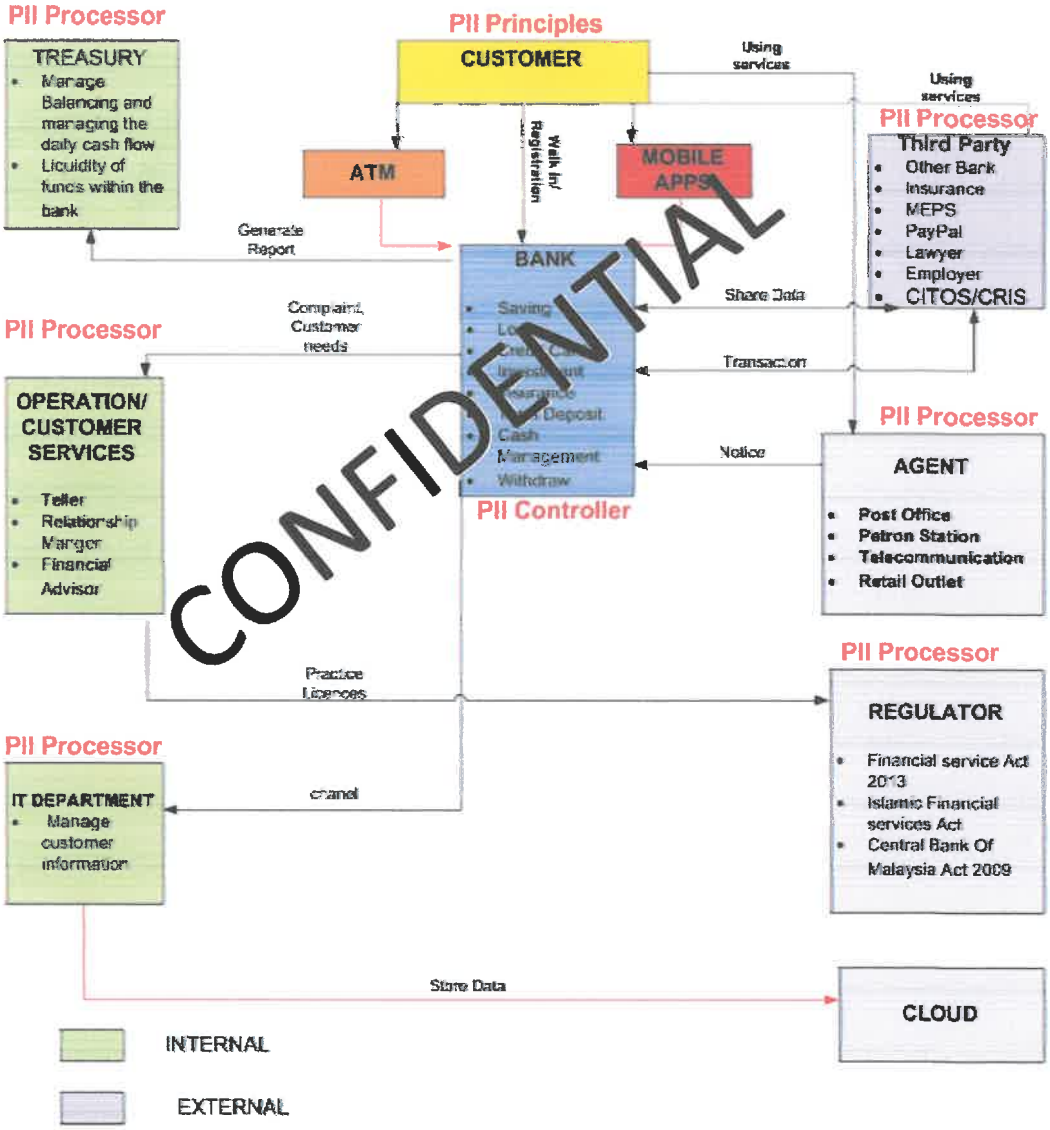


Figure 3. 20 Banking Framework

Table 3. 5 Banking Framework

PII Principle	Customer
PII Controller	Bank
PII Processor	Third Party/Agent/ Regulator/ Cloud/ It Department/ Operation/Customer Services/ Treasury
Sensitive Data	The flow of sensitive data is through the red line which to represent sensitive data used in banking sector. 1. Sensitive data that used, shared and consist in banking sector is the data that related to any transaction such as : • Pin number • Account bank number. • Amount of money, • Agreement of loan • Any data that related to the account bank of principles. • Data of the transaction performed by the principles 2. While, from mobile application sensitive data consist of: • Password of the log in account • Username of the principles used while log in into the application, • Updates from the transaction performed. • 3. After that, sensitive data that can be access by PII processor which is internal department in organization itself known as Information Technology Department. Sensitive data stored at IT department which is all of the history of transaction through technology are managed by IT department and the sensitive data will be recorded and stored in Cloud (cloud also is one of the Third Party Services Provider) which for the purposed of storage, and backup.
PII	PII Processor: External party that can access PII : • **Third Party** Third Party that provides services related to the banking sector such as Interbank, MEPS, PAYPAL, CTOS, CCRIS and as stated above. This is because the third party hold user PII while the PII principles used their services and keep it as history for the purpose of evidences. • **Agent** Access PII of principle that also provide financial services on its behalf such as through telecommunication, Retail Outlet and Petrol Station. For example, using Post Office services to withdraw money from ASB Bank, or to deposit money to Tabung Haji account. The agents must at a minimum or basic services only which to provide the services of accepting deposits and conducting withdrawals. Thus, cannot provide main services that bank are serving.

3.1.8 Charity Program

CyberSecurity Malaysia advocate charity program during Ramadhan. The location choosed by Cybersecurity Malaysia at Rumah Anak Yatim dan Asnaf As-Solihin Banting Selangor and Pertubuhan Kebajikan dan Sosial Redhamu Tuhan Semenyih Selangor. The project manager for this project is Sharifuddin bin sulaman. This project was planned over two weeks. There are eleven staff who involve for this project. During this charity program, CyberSecurity Malaysia collected over 40 boxes that consist of clothes, shoes, shirts, Baju Melayu, Songkok, handbag and Sampin.

Two days before the program, the trainee and others staff work together to select and choose the item. Before start the program project manager brief some information to all staff and make last check before heading to Rumah anak yatim. The trainee need to make sure all boxes are enough and classified each of the boxes based on their content.

Tentatif Program

Masa	Butiran
7.50 pagi	Pindah barang ke Van
8.30 pagi	Bertolak ke Rumah Anak Yatim Dan Asnaf As-Solihin, Banting
9.30 pagi	Penyerahan Sumbangan di Rumah Anak Yatim Dan Asnaf As-Solihin, Banting
10.00 pagi	Bertolak ke Pertubuhan Kebajikan dan Sosial Redhamu Tuhan, Semenyih
11.15 pagi	Penyerahan Sumbangan di Pertubuhan Kebajikan dan Sosial Redhamu Tuhan
11.45 pagi	Kembali ke CyberSecurity Malaysia

Figure 3. 21Tentative

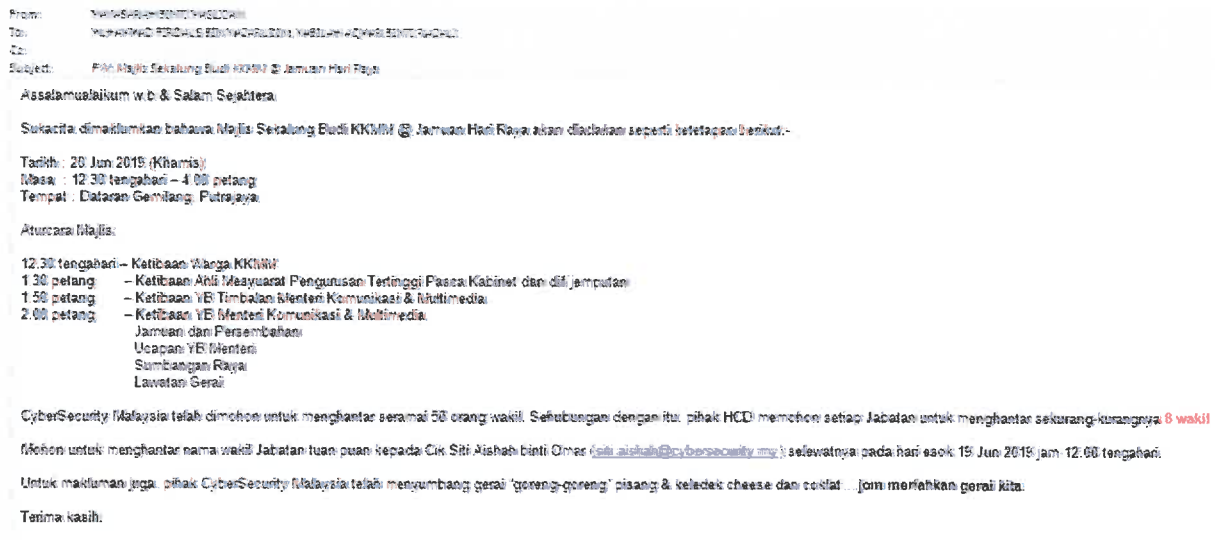
Tentative that gives by project manager the program start at 7.50 am until 11.45am. The trainee start heading to Rumah Anak Yatim dan Asnaf as-Solihin, Banting Selangor. The journey to the location took one and half hour. The trainee spent only thirty minutes at the orphanage house. Then, all of them started their journey to the other location at Semenyih Selangor. They took one and half hour to reach Pertubuhan Kebajikan dan Sosial Redhamu Tuhan.

Figure 3. 22 Rumah Anak Yatim dan Asnaf As-Solihin

Figure 3. 23 Figure 25 Pertubuhan Kebajikan dan Sosial Redhamu Tuhan

3.1.9 Jamuan Hari Raya

The trainee gets two invitations to attend "Jamuan Hari Raya" that organize by Ministry of communication and Multimedia Malaysia and CyberSecurity Malaysia. Jamuan Hari Raya that organizes by Ministry of Communications and Multimedia Malaysia held on 20 June 2019 at Dataran Gemilang, Putrajaya. In this programs that provide the variety of food like Satay, Nasi Beriani, Laksa Peneng and others. This program also attended by Ministry of Communication and Multimedia Malaysia YB Tuan Gobind Singh Deo and Chairman of the National Film Development Corporation Malaysia Hans Isaac.



From:
To:
Cc:
Subject: [redacted]

Assalamualaikum w.b & Salam Sejahtera.

Sukacita dimaklumkan bahawa Majlis Sekalung Budi KKMM @ Jamuan Hari Raya akan diadakan seperti ketetapan berikut:-

Tarikh : 20 Jun 2019 (Khamis)
Masa : 12.30 tengahari – 4.00 petang
Tempat : Dataran Gemilang, Putrajaya

Aturcara Majlis:

12.30 tengahari – Ketibaan Warga KKMM
1.30 petang – Ketibaan Ahli Mesyuarat Pengurusan Tertinggi Pasca Kabinet dan diiringi
1.50 petang – Ketibaan YB Timbalan Menteri Komunikasi & Multimedia
2.00 petang – Ketibaan YB Menteri Komunikasi & Multimedia
Jamuan dan Persembahan
Ucapan YB Menteri
Sumbangan Raya
Lawatan Gerai

CyberSecurity Malaysia telah dimohon untuk menghantar seramai 50 orang wakil. Sehubungan dengan itu, pihak HCD memohon setiap Jabatan untuk menghantar sekurang-kurangnya 8 wakil

Mohon untuk menghantar nama wakil Jabatan tuan puan kepada Cik Siti Aishah binti Omar (siti.aishah@cybersecurity.my) selewatnya pada hari esok 19 Jun 2019 jam 12.00 tengahari.

Untuk makluman juga, pihak CyberSecurity Malaysia telah menyumbang gerai 'goreng-goreng' pisang & keledek cheese dan coklat ... jom meriahkan gerai kita.

Terima kasih.

Figure 3. 24 Invitation Jamua Hari Raya

Figure 3. 25 YB Tuan Gobind Singh Deo

Figure 3. 26 ISMA Team

Figure 3. 27 CyberSecurity staff

Next, Jamuan Hari Raya that organizes by CyberSecurity Malaysia held on 28 June 2019 at Menara Cyber Axis. Variety of food that provide in this programs which is Lemang, Rendang, Kambing Golek, Roti Jala and others. In this program the trainee can know staffs from another department and agency. Have three agency joint this programs which is Standards Malaysia, Mynic and

Figure 3. 28 Invitation Jamuan Hari Raya

Figure 3. 29 CyberSecurity staff

Figure 3. 30 ISMA Department

3.2 Special Project

3.2.1 Introduction

Special project is a compulsory task need to fulfil by the trainee in an Industrial Training. This task requires the trainee to contribute their skills and knowledge in a project that can give benefits to the organization. Besides, the trainee also need to ensure the project develops will relate to Information System.

As a consequences, trainee developed a website that can give exposure to the public about their privacy data. The idea to develop the privacy website come after the trainee involve in the develop privacy framework and guide line project in this organization. Privacy is concerns the protection of individuals' personal information from the illegal disclosure and use by third malicious parties and it is directly related to the individual's online behavior and privacy (Moustaka, 2018). After the trainee makes some research, the trainee identifies people in Malaysia do not concern or take care about their information privacy. They easily share their data to other person or organization. The purpose of this website is to share some important information about privacy to society in Malaysia and give some awareness importance of privacy. In this website, the trainee also provides tips and trick to protect our Personal Identifiable information (PII). The trainee provides all research paper that suitable to privacy topic in this website. All users can download the article and use as references to make research or to add the knowledge. The target user for this website comes from three categories which is student, lecture and research. To develop this website the trainee takes 4 month to fully complete the technical part and documentation part.

3.2.2 Problem

That is several problems that identify:

I. Lack of awareness and knowledge to understand the importance of privacy

II. Easy to share our privacy information to unauthorized person and organization

III. Lack of exposure to children, staff and others society about data privacy management

3.2.3 Objective

The objectives of Privacy Awareness Websites:

I. To exposure the importance of privacy to the society

II. To provide tips and tricks in managing and protecting the privacy of personal information

III. To understand and implementation ISO 27552 as the privacy of Malaysia

3.2.4 User Target

Privacy Awareness Website (PAW) also involved within a lot of great requirements and multiple functions suit for specific purposes. This system served two categories of users which are the user (students, lecture, and researcher) and administrator (Privacy team CyberSecurity Malaysia). The scopes of the system that will be provided for each of the categories are as follows:

Table 3. 6 User Target

No	User	scope
1	User (students, lecture, and researcher)	The user can see all information that provide in this website. Beside the user also can download several research paper that provider about related topic in this websites.
2	Administrator (Privacy team CyberSecurity Malaysia)	Admin for this website can edit, delete and update all information that provide at user interface. Admin also.

3.2.5 Tools for Development

Table 3.7 shows the items, the descriptions of the items of the tools that used for the development of this website. CyberSecurity Malaysia provide all tools that use by the trainee. The trainee need get the permission with supervisor and Security Technology System department to install all software that need use in this project. After the trainee get the permission the trainee proceed to continue develop this project

Table 3. 7 Tools of Development

NO	ITEMS	DESCRIPTION
1	Laptop	**HP Pavilion 14-AL102TX GOLD** • Specifications ▪ Intel® Core™ i5-7200U (2.5 GHz, up to 3.1 GHz, 3 MB cache, 2 cores) ▪ 4 GB DDR4-2133 SDRAM (1 x 4 GB) ▪ NVIDIA® GeForce® 940MX (2 GB DDR3 dedicated) ▪ 1 TB 5400 rpm SATA ▪ 65 W AC power adapter
2	Adobe Dreamweaver	Adobe Dreamweaver CS6 This software program used in designing web pages, more fully featured HTML web to create and edit web pages in a user-friendly environment.
3	Adobe Photoshop	Adobe Photoshop CS6 This software majorly used for the task that involved with the design and, photo editing. For instance, the creation of the logo design. By using Photoshop, the image can be created in high quality.
4	Operating System	**Windows 7 Professional** Windows 7 Professional is an operating system that is installed in the PC and laptop to develop the system.
5	Bootstrap	Bootstrap its template that use by trainee to develop this privacy awareness website. This is requirement that mention by Cybersecurity to use for development this website
6	Notepad++	Notepad++ Version 7.5.6 Notepad++ used to write the coding languages in order to develop the system. Using Notepad++ is more attractive as it includes many interesting colors.
7	Web Browser	Google Chrome & Internet Explorer This application used to run the system to see if it can be run smoothly by using the certain web browser.

3.2.6 Methodology

The methodology that trainee propose to use is the system development life cycle which is System Development Life Cycle that stands for planning, analysis, design, implementation, and maintenance. The following sentences are some details for the methodology.

3.2.6.1 Planning

For the planning, the trainee had done a proper planning regarding web development. So, within this planning, the trainee will do a research in order to seek what is the problem that emerges which makes this kind of websites need to be developed. Then after the trainee had identified some of the potential problems, the trainee will specifically create the solutions for all of the problems that found. The solutions will be main priority when developing this websites. Not only that, the trainee also calculate the amount of time, resources that require in order to successfully develop this website. All of the suitable items for this web development will be carefully considered within this planning

3.2.6.2 Analysis

For the analysis phase, the trainee had conducted some research in order to gain all relevant information that need to develop this website. So for this reason, trainee had organized some interview session with the staff at the Cybersecurity Malaysia to collect all the required information. Furthermore, the trainee also look into some journals or article to find out if this kind of website will basically bring a lot of benefits to user.

3.2.6.3 Design

So for the design phase of this web development, the trainee scratches the storyboard and site map. After that, trainee consults the storyboard to supervisor to get the permission to procced that design. This websites have two interface which is user interface and admin interface. For user interface user can see all information that provide and also can download the article. Next, admin interface can update, delete and add the information.

3.2.6.4 Implementation

Then for the implementation phase, the trainee get free from Cybersecurity Malaysia all of the required hardware and also the software upon the system execution. So for the software, the software such as the notepade ++ will be installed in order to execute all the codes of the programming. Then the laptop will be used and other devices such as a mouse, monitor, and the motherboard also get from Cybersecurity Malaysia to serve as the back-up in case something bad happens to the laptop itself.

3.2.6.5 Maintenance

In this very last stage, the trainee gave the permission to the Cybersecurity Malaysia to test this system. So if there is any weakness being found within the testing period, the trainee immediately fix that problem and may add some more features after the testing of the system in order for the system to be well-functioned.

3.2.7 Project Planning

Assessing schedule feasibility is about time constraint or schedule that has been assigned for the period of time in order to make sure that the project will be fully completed according to that time. This also can be information to the development team or notify them the deadlines of the project either the date given is reasonable to perform all tasks that has been assigned. The trainee makes brainstorming session to know the period of time to complete our project. To make sure project run in accordance to the date that has been assigned, the trainee developed project timeline or Gantt chart to ensure can follow the deadlines.

Project timeframe must be planned properly in order to overcome overdue of the project planning. Profit of the organization is important to ensure the company will always effective and efficient with financial management so to ensure that is by making the schedule properly. Project planning is referring to assessing schedule feasibility in which it is related to project duration. Project planning helps trainee in determining all potential time frames and completion date schedules can be met and that meeting these dates will be sufficient for dealing with the needs of the organization. The trainee use Gantt chart in order to estimate the time frame of Privacy awareness website.

For this project the trainee estimate five month to fully finish this project. This project will be starting from 1st February 2019 until 28 July 2019. There are several phase that need to follow which is planning, analysis, design, implementation and design.

Table 3. 8 Duration Develop website

No	Phase	Start Date	Finish Date	Total days exclude weeekends
1	Planning	1/2/2019	28/2/2019	20 days
2	Analysis	4/3/2019	26/3/2019	17 Days
3	Design	1/4/2019	3/4/2019	17 Days
4	Implementation	2/5/2019	14/6/2019	32 Days
5	Maintenance	17/6/2019	28/6/2019	10 Days

Figure 3. 31 Planning

Figure 3. 32 Analysis

Figure 3. 33 Design

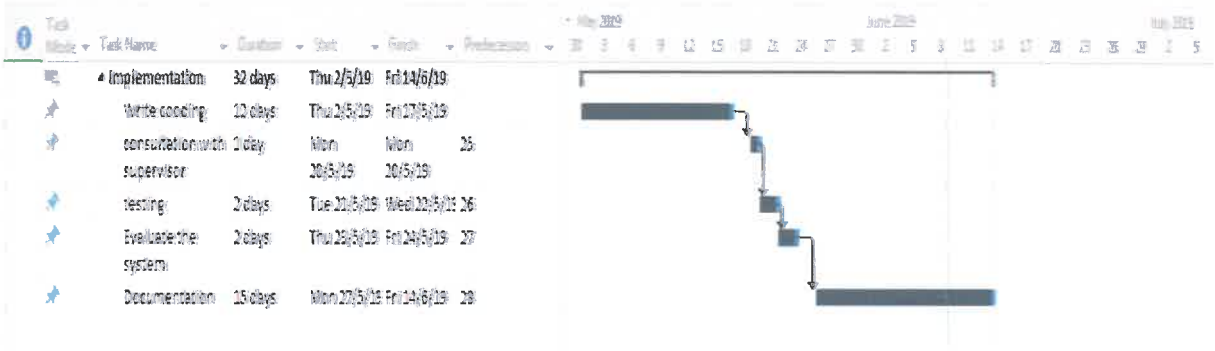


Figure 3. 34 Implementation

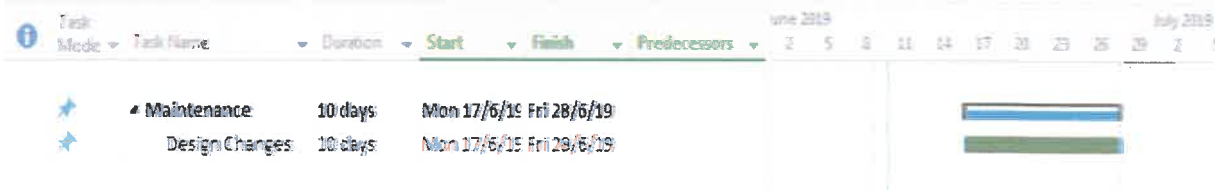


Figure 3. 35 Maintenance

3.2.8 Analysis

In this phase, the trainee takes one month to complete this phase and conduct three times meeting with privacy team and Head of Department. After the process of collecting requirements through some research, interview and observation has been made, the trainee decided to propose Privacy Awareness Website. The reasons then website was being developed is to give knowledge and awareness to society at Malaysia to store their information data carefully and not share to unauthorized person. The others reasons are to ensure user understand what types of information Personal identifiable identity (PII).

First of all, in this phases the trainee conduct the research to gather all information about important of privacy, privacy in IR 4.0, awareness of privacy and policy and procedure to preserve and maintain information privacy in organization or personal. All information that collects need to analysis and present to supervisor and Head of department. The trainee also need analyze which information is suitable to share and expose in website. The trainee also need ensure information that share in website need using simple words to make sure target user easily to understand that information.

Next, the trainee conducts the interview with privacy team leader. The purpose of this interview is to understand more detail about the privacy and ISO 29001 and ISO 27552. In this interview the trainee gets more knowledge about the privacy based on experience that share by privacy team leader. In this interview also, privacy team leader share some tips and idea about the structure and flow of the privacy websites. The trainee also discusses the flow chart and sitemap of this website to team leader and head of department.

Moreover, the trainee also analyses some privacy awareness website from other organization and country to identify what information they share to their user. For example privacy awareness week (Australian), stay safe online (National Cyber Security Alliance), privacy awareness week (Philippines).

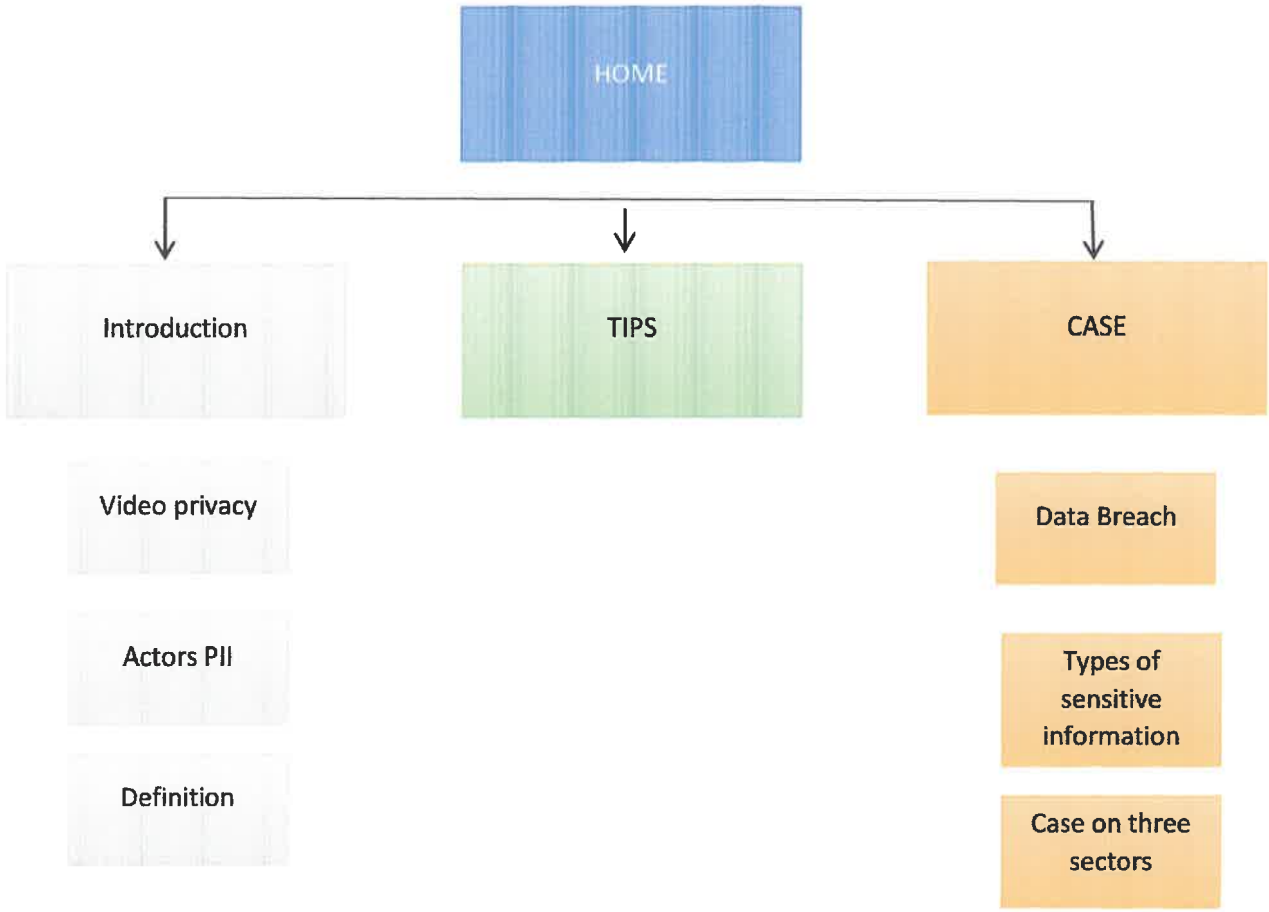
3.2.9 Design

In develop website, this phase are very important to ensure the layout are interactive, easy to understand and beautiful can attract user read the information that provides in this websites. In this phase, the activity that make by trainee are sketch storyboard, design the user interface, meeting and discussion with supervisor and design site map. The duration that take for this phase are 20 days. The trainee changes the design for three times in ensuring the website is more effective and can attract user time to time.

Sketch storyboard is very important to get the idea and design the layout to ensure the website interactive and effective. With storyboard the trainee can easily present to supervisor and show how the website process. The process of evaluation the information need to allocate in the websites is very important. The reason is because to ensure the user can understand the information easily.

After the trainee done sketch the storyboard, the trainee need consult and presentation to supervisor to get the approval. During the meeting and consultation the trainee and others staff sharing the idea to improve the website. After get the approval from supervisor, the trainee starts design the sitemap. Sitemap are very important way for a website to communication with search engines. Sitemap make navigation the website easily and gives better visibility to search engine

3.2.9.1 Sitemap



3.2.9.2 Story Board (Home Interface)

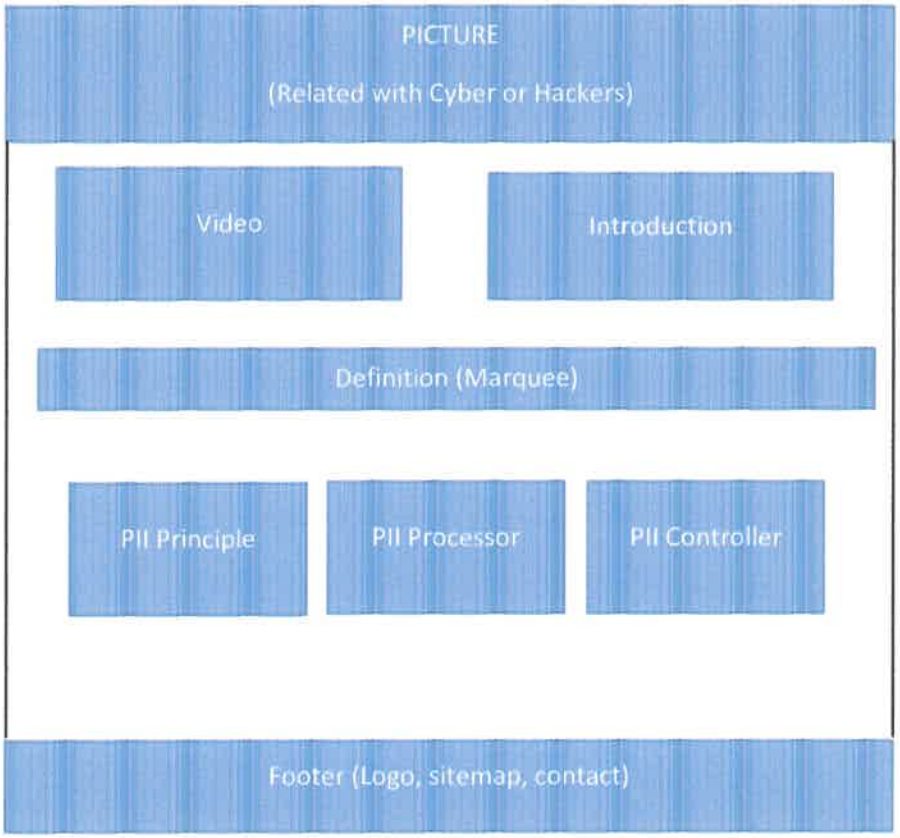


Figure 3. 36 Home Storyboard

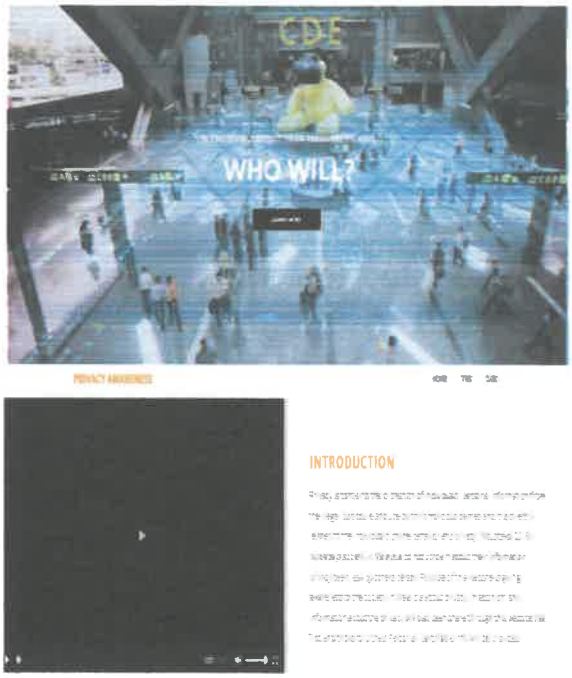


Figure 3. 37 Home Interface

3.2.9.3 Story Board (Tips Interface)

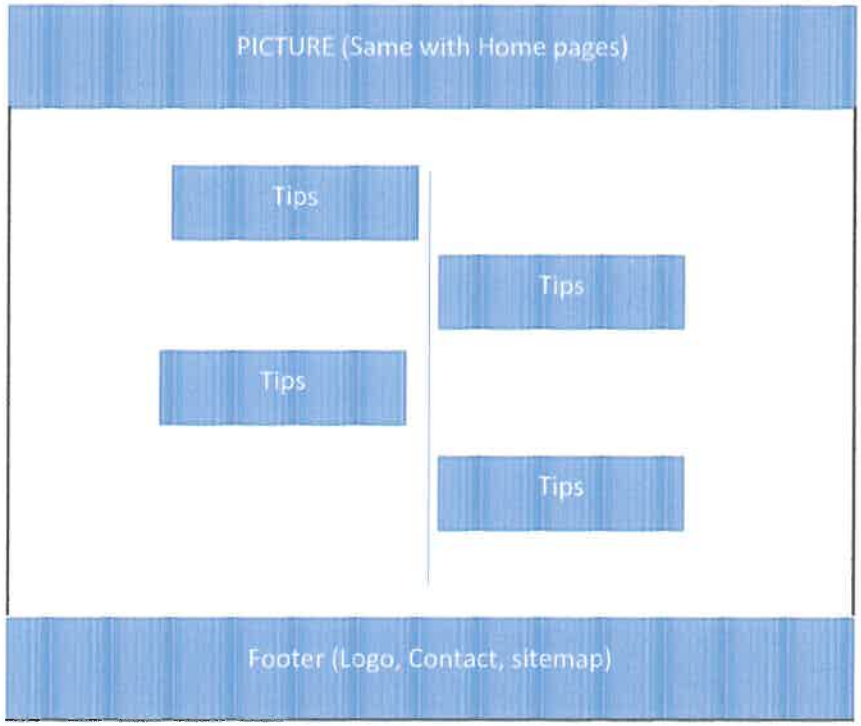


Figure 3. 38 Storyboard Tips

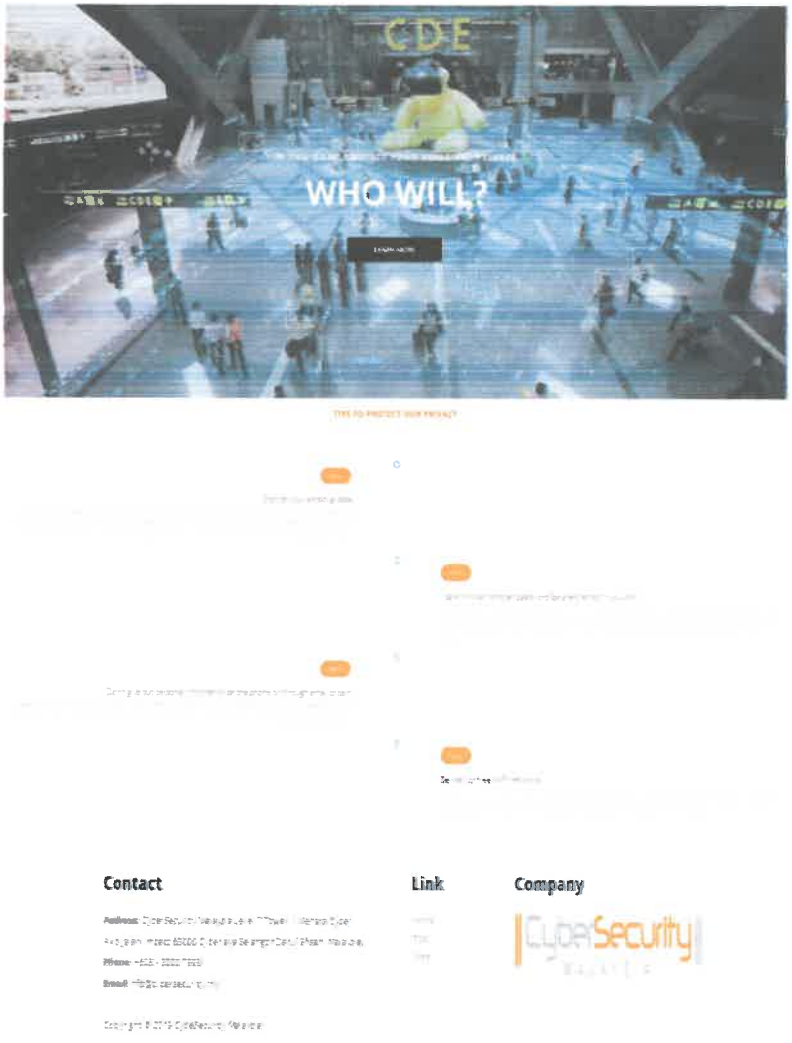


Figure 3. 39Tips Interface

3.2.9.4 Story Board (Case Interface)

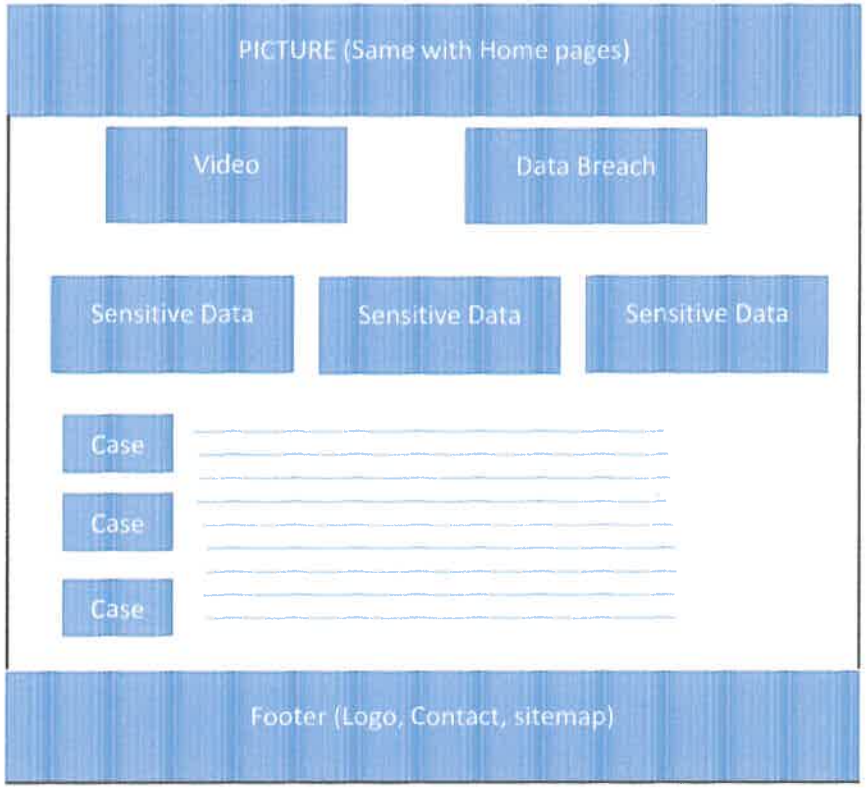


Figure 3. 40 Storyboard Case

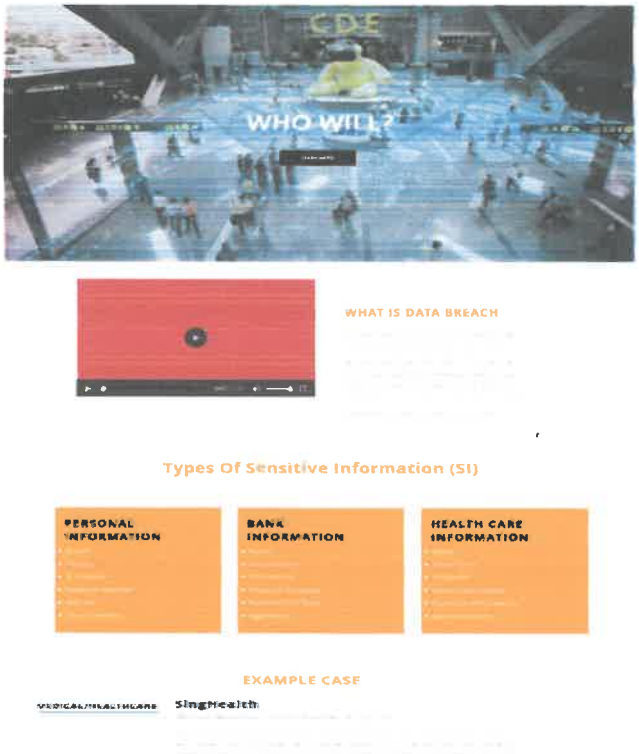


Figure 3. 41 Case Interface

3.2.10 Implementation

In this phase the task that was conducted the trainee like implementation of coding, installation, testing and training. In this phase the trainee conduct four times meeting which privacy team and Head of department. The trainee start with develop front end interface for privacy awareness websites. This activity takes two weeks to fully complete for interface. After that, the trainee inserts all information and infographic information into the website to ensure all information suitable in this websites. Besides, the trainee starts implementation some design to ensure suitable with websites. The trainee also ensure all design follow the storyboard that create in design phase.

So, upon the completion of Privacy awareness website, the process of the testing or user acceptance had been significantly conducted within the Cybersecurity Malaysia. For user acceptance test (UAT), the trainee chooses four people from department information security management and assurance (ISMA) to involve in this activity. The trainee provides user guideline and checklist for (UAT). The purpose of user acceptance test (UAT) is to identify any bug in this website and to ensure all button function and all information can update, delete, edit and upload.

The trainee also conducts the internal training for privacy team. This training is to ensure all privacy team member know how to handle and manage this website. In this training the trainees teach how to edit, delete, update and upload the information in this websites. The trainee had also instructed all of the participants on how to effectively and efficiently utilize the whole system. If there is anything that the user does not understand about the system, the trainee immediately giving the response to all of their inquiry or problems during this training phase.

3.2.11 Maintenance

For the maintenance phase, the trainee had fixed all of the flaws that may be identified within this website. The trainee executes the improvisation based on the minimum bugs and errors from the implementation phase. So during the maintenance phase, the trainee executes the debugging and fix and kinds of errors. The trainer ensures all button are function and connect with other page.

The other problem that land on project is that the interface manages to be displayed but some of the pictures just could not be displayed on some pages. So to solve this kind of problem, the trainee had searched if there is any error that the trainee may not expect at all within the coding implementation.

Indeed, there are some errors within the coding itself. Then, the trainee had managed to fix the errors and the pictures can be displayed on the page as it should be. During the testing phase, some of the user fails to update the picture into the website since that the file size is way too big. So, the trainee alters the coding so that user can upload files with larger size.

4. Chapter 4: Conclusion

In the industrial placement, trainee learned lot of new things and gained many experiences. Trainee also get the chances in applying the theories learned in class.

4.1 Application of knowledge, skills and experience in undertaking the task (Knowledge gained)

The trainee had applied the knowledge and skills learnt in ISM657 legal and ethical aspect. During the study in faculty the trainee as well had explored further on ISO 27001 and Business continuity plan. The trainee can implement the skill and knowledge during internship program. During this internship program the trainee easily to understand and can assist other staff during implement ISO 27001 and Business Continuity plan. The trainee also can share knowledge ISO 27001 and Business Continuity plan that learnt in faculty with other staff to get new opinion and idea.

Next, the trainee also had applied the knowledge and skill learnt in IMC 651 evaluation of information services. During study in faculty the trainee as well had explored in research skill, develop research question, develop research framework, use and understand research methodology, write the research paper and critical paper .The trainee uses all skill in research that learns during studies in Faculty of Information Management. The trainee can easily conduct the research and write the research paper during the internship. All skill and technique that learn in Faculty implemented by trainee.

The experience gathered from handling events and programs including user training and public speaking during studies in Faculty of Information Management, UiTM Kelantan also had benefit the trainee in order to communicate with the staff and joint sharing knowledge activity that organize by Knowledge Management. During study IMS 556 Information System Interaction and Consultation in faculty the trainee learn how to use the proper language, body language, conflict management, and emotional reaction and actions to use in internship program. This knowledge is very important to implement in our self because during the internship program the trainee always have a meeting with head of department and other staff.

Besides, the trainee also had applied the knowledge and skill learnt in IMS607 Advanced Web Design and Content Management and IMS606 and IMS655 System Analyst in Information Management. During study in faculty the trainee learn how to conduct the user acceptance test (UAT) and final acceptance test (FAT). The trainee also learn how to identify the bug or error in system and how to solve that problems. With this knowledge and skill the trainee can easily help other staff to maintaining and troubleshoot the ISM system at MAMPU.

The trainee can use all knowledge and skill that get in faculty to implement in internship program. All subject that provides by the faculty is very important to understand and ensure can implement in our life.

4.2 Personal thoughts and opinion

During the internship program, the trainee feels that the organization provide a lot of opportunities and supportive environment. The supervisor, the staff, and even the top management are friendly and easy to communicate. The work environment in this organization is a fun, conducive and productive atmosphere. The organization also provides the best facility to all staff and also to all internship students. The organization provides laptop, parking space and free drink to all staff. The trainee also thinks that knowledge and skills provided by faculty is necessary and useful and can be implementing.

Next, from the experience all the colleague in CyberSecurity are helpful and supportive in helping all the intern to finish their task assigned. During the internship program many enquiries may come from time to time. The trainee always seek for industry supervisor support regarding the issues in daily task. The industry supervisor will never reject any enquiries and will patiently show the solution. Others than, teamwork between Information Security Management and Assurance department (ISMA) is unquestionably good. All of team member will keep updated the tasks with each teammates in finishing the tasks. There are many different group in this department such as research team, Business continuity management and Information security management system.

4.3 Lesson learnt

During the industry program, the trainee can learn many lessons and get new knowledge. The trainee has learnt to be more discipline, punctual, and has improved in communication skills. Other than, the trainee also learnt how to conduct the meeting with the top management and conduct the research more effective and efficient. Besides, the trainee also learnt new knowledge which is about ISO 27552, ISO 29001, ISO 27002 and Privacy framework. All knowledge that gives during Industry training is useful for the future. Being in working surrounding, the trainee has learnt how to commit with time, multiple tasks, problem solving and responsibility. The most important things that can learn are teamwork. How to work in one group together and achieves the goals together. A lot of teamwork goes behind achieving big goals. To have a meaningful and lifelong career, need to work well with others which are why teamwork is so important in the professional world.

Next, time management is extremely important in a project environment. A good time management will ensure the project run accordingly and helps to achieve objective effectively. During this internship placement, the trainee learned a lot about managing the time in finishing all the task given. Time management is very crucial in a project as trainee need to achieve the dateline and target given by the supervisor.

Self-learning or self-exploration is important in all the task given. Not all problem or issue will be solved by the senior staff. During the first two months, the trainee will be helped through all the issue arise. But after that, the trainee will have to depend on themselves. This self-learning is good for the trainee as this will help them in gaining more knowledge and skills in software development industry. In times when everybody is pressed for time, and formal education comes with its own time constraints, self-learning ensures that one is not under any pressure whatsoever to push oneself.

4.4 Lesson learnt

During this internship program the limitations that faced by trainee is difficult to find the related topic in online database that provide by CyberSecurity Malaysia. The trainee needs using online database that provide by UiTM. In online database Cybersecurity Malaysia they just have 3 publishers and not have many choices. The trainee would also like to recommend this organization to subscribe more publisher in their online database to ensure staff in their organization can easily to find the related topic based on their field. Next, the trainee would also like to recommend that faculty improve the courses by providing more hands-on courses so that the future students who will undergo practical training will be well-equipped with hands-on skills rather than only theories learnt in classes.

Besides, during the internship program the limitations that identify in Information Security Management and Assurance department is they not have enough staff to handle many project. This department need to hired new staff to help them manage the project and get new idea from the new staff. Moreover, in CyberSecurity Malaysia they not allowed internship student use their Wi-Fi because that are policy and procedure that use in Cybersecurity Malaysia. With this policy, the trainee facing difficulty to make the task out site form office.

5. References

Official Portal CyberSecurity Malaysia. *(2019)*. Retrieved 26 June 2019 from https://www.cybersecurity.my

OVIC. (2019). Privacy Awareness Week. Retrieved 26 June 2019 from https://ovic.vic.gov.au

Privacy Commissioner for Personal Data Hong Kong. (2019). Privacy Awareness Week 2019. Retrieved 26 June 2019 from https://www.pcpd.org.hk

Official Australia Information Commissioner. (2019). Privacy Awareness Week. Retrieved 26 June 2019 from https://www.oaic.gov.au

Asia Pacific Privacy Authorities. (2019). Privacy Awareness week. Retrieved 26 June 2019 from http://www.appaforum.org/paw/

Privacy Awareness Week. (2019). Don't be in the dark. Retrieved 27 June 2019 from https://www.oaic.gov.au/paw2019/

Engel, K. (2018). The simple privacy and policy guide for website owners. Retrieved 27 June 2019 from https://www.webhostingsecretrevealed.com

It Governance. (2019). ISO 27001 The international Information Security Standard. Retrieved 27 June 2019 from https://www.itgovernance.co.uk/iso27001

Bsigroup. (2019). ISO/IEC 27552 Privacy Information Management. Retrieved 27 June 2019 from https://www.bsigroup.com

Moustaka, V., & Anthopoulos, L. G. (2019). Enhancing social networking in smart cities: Privacy and security borderlines. *Technological Forecasting and Social Change*, 142, 285-300. doi:10.1016/j.techfore.2018.10.026

Cui, L., & Yang, Y. (2018). Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access, 6*, 46134-46145. doi:10.1109/access.2018.2853985

Sinha, M., Majra, H., Hutchins, J., & Saxena, R. (2019). Mobile payments in India: The privacy factor. *International Journal of Bank Marketing,37*(1), 192-209. doi:10.1108/ijbm-05-2017-0099

Leszczyna, R. (2018). Cybersecurity and privacy in standards for smart grids – A comprehensive survey. *Computer Standards & Interfaces,56*, 62-73. doi:10.1016/j.csi.2017.09.005

Dangur, J., & Jaybhaye, S. M. (2016). Framework for secure data sharing in dynamic group using public cloud. *2016 International Conference on Computing, Analytics and SecurityTrends (CAST)*. doi:10.1109/cast.2016.7914966

Lim, H. E. & Muszafarshah M.M. (2013). Effectiveness of industrial training in improving students' generic skills. International Journal of Business and Society, 14(3), 368 – 375.

Ministry of Higher Education. (2006). Hala Tuju 2, Reassessment Report on Accounting Programme at Public Universities of Malaysia 2006. Pusat Penerbitan Universiti Teknologi MARA: Malaysia.

Megat Mohd Nor, P.N.S. & Ismail, S. (2015). Effect of industrial training on academic performance: evidence from Malaysia. Journal of Technical Education and Training, 7(2), 44-53.

APPENDICES

UNIVERSITI TEKNOLOGI MARA

FAKULTI PENGURUSAN MAKLUMAT
Universiti Teknologi MARA Cawangan Kelantan
Bukit Ilmu, 18500 Machang,
Kelantan Darul Naim
Tel: 09-9762000
Fax: 09-9762156 (HEA)

REKOD KEDATANGAN LATIHAN INDUSTRI

Nama Pelatih : MUHAMMAD FIRDAUS B NAZARUDIN

No. I/C _____

Nama / Alamat Organisasi : CyberSecurity Malaysia

Nama Penyelia : PUAN SABARIAH BTE AHMAD

Bulan /Tahun : FEBRUARY 2019

Tarikh	Waktu Masuk	Waktu Keluar	Tandatangan Penyelia
1/2/2019	9.00 am	6.00 pm	A
4/2/2019	8.40 am	6.00 Pm	
7/2/2019	8.40 am	6.00 Pm	
8/2/2019	8.40 am	6.00 Pm	
11/2/2019	8.40 am	6.00 Pm	
12/2/2019	8.45 am	6.00 Pm	
13/2/2019	8.40 am	6.00 Pm	
14/2/2019	8.45 am	6.00 Pm	
15/2/2019	9.00 am	6.00 Pm	
18/2/2019	8.40 am	6.00 Pm	
19/2/2019	8.40 am	6.00 Pm	
20/2/2019	8.40 am	6.00 Pm	
21/2/2019	8.35 am	6.00 Pm	
22/2/2019	8.40 am	6.00 Pm	
25/2/2019	8.45 am	6.00 Pm	
26/2/2019	8.45 am	6.00 pm	
27/2/2019	8.40 am	6.00 Pm	
28/2/2019	8.40 am	6.00 pm	

Dengan ini saya mengesahkan bahawa maklu at di atas adalah benar.

Tandatangan Pelajar _____ Tarikh : _____

Tandatangan Penyelia _____ Tarikh : _____

UNIVERSITI TEKNOLOGI MARA

FAKULTI PENGURUSAN MAKLUMAT
Universiti Teknologi MARA Cawangan Kelantan
Bukit Ilmu, 18500 Machang,
Kelantan Darul Naim
Tel: 09-9762000
Fax: 09-9762156 (HEA)

REKOD KEDATANGAN LATIHAN INDUSTRI

Nama Pelatih : MUHAMMAD FIRDAUS BIN NAZARUDIN No. Matrik :

No. I/C

Nama / Alamat Organisasi : CyberSecurity Malaysia

Nama Penyelia : PUAN SABARIAH BTE AHMAD

Bulan /Tahun : MARCH 2019

Tarikh	Waktu Masuk	Waktu Keluar	Tandatangan Penyelia
1/3/2019	8.40 am	6.00 pm	
4/3/2019	8.40 am	6.00 pm	
5/3/2019	8.30 am	5.40 pm	
6/3/2019	8.20 am	5.40 pm	
7/3/2019	8.40 am	6.00 pm	
8/3/2019	8.45 am	6.00 pm	
11/3/2019	8.30 am	5.40 pm	
12/3/2019	8.50 am	6.00 pm	
13/3/2019	8.45 am	6.00 pm	
14/3/2019	8.43 am	6.00 pm	
15/3/2019	8.40 am	6.00 pm	
18/3/2019	8.42 am	6.00 pm	
19/3/2019	8.40 am	6.00 pm	
20/3/2019	8.28 am	5.40 pm	
21/3/2019	8.35 am	5.40 pm	
22/3/2019	8.30 am	5.40 pm	
25/3/2019	8.20 am	5.40 pm	
26/3/2019	8.40 am	6.00 pm	
27/3/2019	8.40 am	6.00 pm	
28/3/2019	8.30 am	5.50 pm	
29/3/2019	8.40 am	6.00 pm	

Dengan ini saya mengesahkan bahawa maklumat di atas adalah benar.

Tandatangan Pelajar Tarikh : 1/4/2019

Tandatangan Penyelia Tarikh : 15/4/2019

UNIVERSITI TEKNOLOGI MARA

FAKULTI PENGURUSAN MAKLUMAT
Universiti Teknologi MARA Cawangan Kelantan
Bukit Ilmu, 18500 Machang,
Kelantan Darul Naim
Tel: 09-9762000
Fax: 09-9762156 (HEA)

REKOD KEDATANGAN LATIHAN INDUSTRI

Nama Pelatih : MUHAMMAD FIRDAUS BIN NAZARUDIN

No. I/C

Nama / Alamat Organisasi : CyberSecurity Malaysia

Nama Penyelia : PUAN SABARIAH BTE AHMAD

Bulan /Tahun : APRIL 2019

Tarikh	Waktu Masuk	Waktu Keluar	Tandatangan Penyelia
1/4/2019	8.40 am	6.00 pm	
2/4/2019	8.30 am	5.40 pm	
3/4/2019	8.40 am	6.00 pm	
4/4/2019	8.20 am	5.45 pm	
5/4/2019	8.35 am	6.00 pm	
8/4/2019	8.40 am	6.00 pm	
9/4/2019	8.30 am	6.00 pm	
10/4/2019	8.35 am	6.00 pm	
11/4/2019	8.35 am	6.00 pm	
12/4/2019	8.30 am	5.30 pm	
15/4/2019	8.20 am	5.30 pm	
16/4/2019	8.30 am	5.40 pm	
17/4/2019	8.50 am	6.00 pm	
18/4/2019	8.30 am	5.40 pm	
19/4/2019	8.30 am	5.40 pm	
22/4/2019	8.30 am	5.30 pm	
23/4/2019	8.35 am	5.40 pm	
24/4/2019	8.35 am	5.40 pm	
25/4/2019	8.40 am	6.00 pm	
26/4/2019	8.50 am	6.00 pm	
29/4/2019	8.05 am	5.15 pm	
30/4/2019	8.30 am	5.30 pm	

Dengan ini saya mengesahkan bahawa maklumat di atas adalah benar.

Tandatangan Pelajar Tarikh : 30/4/2019

Tandatangan Penyelia Tarikh : 30 2019

UNIVERSITI TEKNOLOGI MARA

FAKULTI PENGURUSAN MAKLUMAT
Universiti Teknologi MARA Cawangan Kelantan
Bukit Ilmu, 18500 Machang,
Kelantan Darul Naim
Tel: 09-9762000
Fax: 09-9762156 (HEA)

REKOD KEDATANGAN LATIHAN INDUSTRI

Nama Pelatih : MUHAMMAD FIRDAUS BIN NIZARUDIN

No. I/C :

Nama / Alamat Organisasi : Cyber Security Malaysia

Nama Penyelia : PUAN SABARIAH BTE AHMAD

Bulan /Tahun : MAY 2019

Tarikh	Waktu Masuk	Waktu Keluar	Tandatangan Penyelia
1/5/2019	Hari Buruh		
2/5/2019	8.30 am	6.00pm	
3/5/2019	8.30 am	6.00 pm	
6/5/2019	7.30 am	4.00 pm	
7/5/2019	7.50 am	4.30 pm	
8/5/2019	8.30 am	5.00 pm	
9/5/2019	8.30 am	5.00pm	
10/5/2019	8.30 am	5.00pm	
13/5/2019	8.30 am	5.00pm	
14/5/2019	8.30 am	5.00 pm	
15/5/2019	8.30 am	5.00 pm	
16/5/2019	8.00 am	4.30pm	
17/5/2019	8.00 am	4.30 pm	
20/5/2019	WESAK DAY	4.30 pm	
21/5/2019	8.00 am	4.30 pm	
22/5/2019	NUZUL QURAN		
23/5/2019	8.30 am	5.00 pm	
24/5/2019	8.30 am	5.00 pm	
27/5/2019	9.00 am	5.30 pm	
28/5/2019	8.25 am	5.00 pm	
29/5/2019	8.10 am	5.00 pm	
30/5/2019	9.00 am	5.30 pm	
31/5/2019	8.00 am	5.00pm	

Dengan ini saya mengesahkan bahawa maklumat di atas adalah benar.

Tandatangan Pelajar

Tarikh : 31/5/2019

Tandatangan Penyelia

Tarikh : 31/5/2019

UNIVERSITI TEKNOLOGI MARA

FAKULTI PENGURUSAN MAKLUMAT
Universiti Teknologi MARA Cawangan Kelantan
Bukit Ilmu, 18500 Machang,
Kelantan Darul Naim
Tel: 09-9762000
Fax: 09-9762156 (HEA)

REKOD KEDATANGAN LATIHAN INDUSTRI

Nama Pelatih: MUHAMMAD FIRDAUS BIN WAZARUDIN No. Matrik: 2016316991

No. I/C:

Nama / Alamat Organisasi: Cyber Security Malaysia

Nama Penyelia: PUAN SABARIAH BTE AHMAD

Bulan /Tahun: JUNE 2019

Tarikh	Waktu Masuk	Waktu Keluar	Tandatangan Penyelia
3/6/2019	HARI RAYA AIDILFITR		
4/6/2019			
5/6/2019			
6/6/2019			
7/6/2019			
10/6/2019	8.30 am	6.00 pm	
11/6/2019	8.30 am	5.30 pm	
12/6/2019	8.30 am	5.30 pm	
13/6/2019	8.45 am	5.50 pm	
14/6/2019	9.00 am	6.00 pm	
17/6/2019	9.00 am	6.00 pm	
18/6/2019	8.30 am	5.30 pm	
19/6/2019	8.30 am	5.45 pm	
20/6/2019	8.00 am	5.15 pm	
21/6/2019	8.25 am	5.30 pm	
24/6/2019	8.30 am	5.30 m	
25/6/2019	8.30 am	6.00 pm	
26/6/2019	8.30 am	6.00 pm	
27/6/2019	8.30 am	6.00 pm	
28/6/2019	8.30 am	6.00 pm	

Dengan ini saya mengesahkan bahawa m di atas adalah benar.

Tandatangan Pelajar: _____ Tarikh : 28/6/2019

Tandatangan Penyelia: _____ Tarikh : 28/6/2019

FACULTY OF INFORMATION MANAGEMENT
UNIVERSITI TEKNOLOGI MARA (UiTM)
KELANTAN BRANCH

REPORT DUTY DECLARATION FORM

(Semester 7)

To : Puan Nurulannisa Binti Abdullah
Industrial Training Coordinator IM245 – UiTM Kelantan

Name : MUHAMMAD FIRDAUS BIN NAZARUDIN

UiTM ID : 2016316991

Program Code : IM245

H/P No :

I hereby, confirmed and report my duty to CyberSecurity Malaysia (organization).

Date: 1st February 2019 Student Signature _____

Verified by,

Signature _____

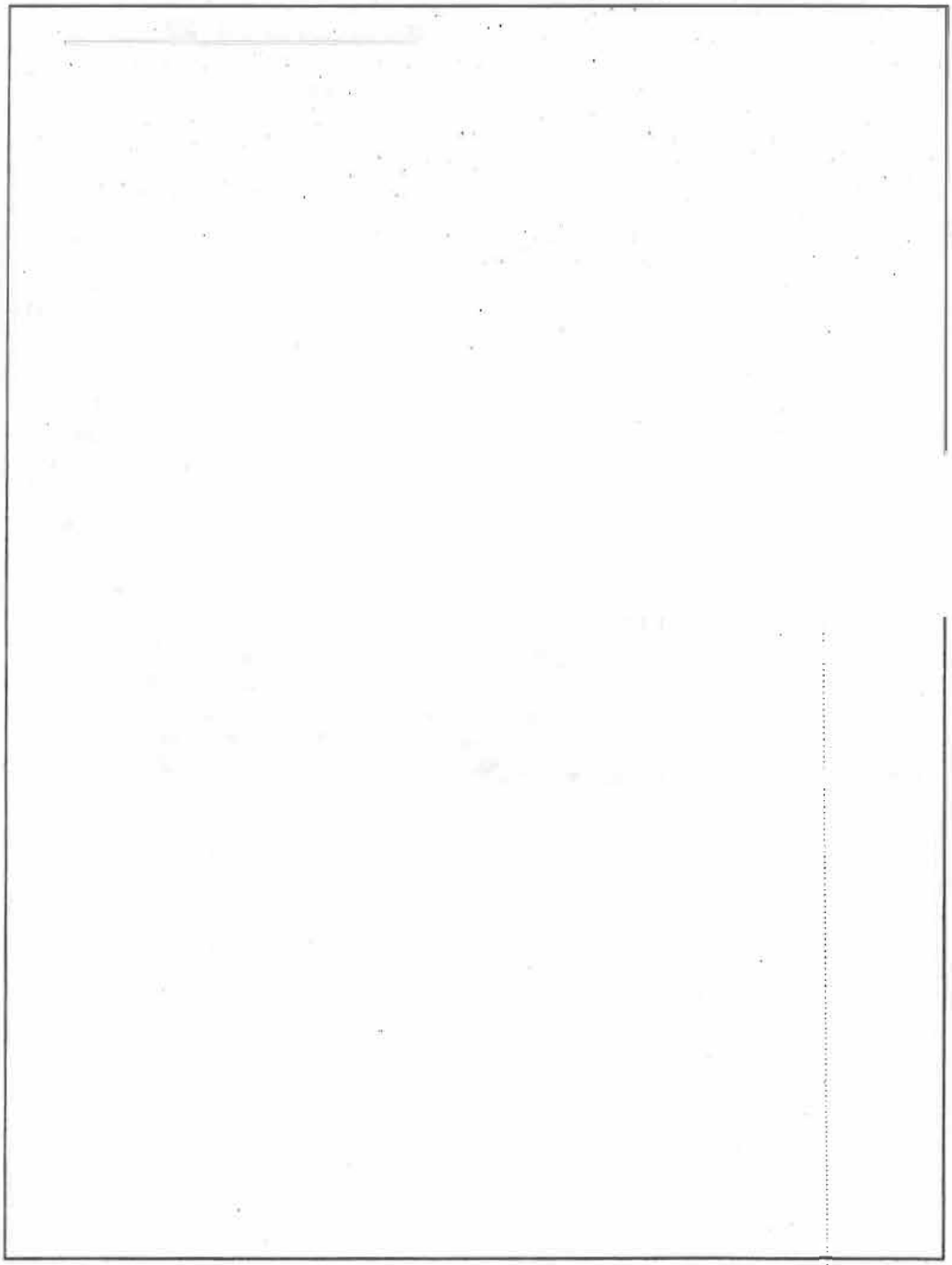
Name _____

Designation _____

Official Stamp _____

** Email to : nurul1217@kelantan.uitm.edu.my or fax to 09-9762156 (HEA)

TEMPLATE MAKLUMAT PENYELIA



SLIDE PRESENTATION

LOG BOOK

3 JULY 2019

Industrial Training: CyberSecurity Malaysia

Presented by Muhammad Firdaus Nazarudin
Matric No : 2016316991

OUR DISCUSSION TODAY

TOPICS AND HIGHLIGHTS

- CyberSecurity Background
- Department Function
- Industry training Activity
  - Research
  - Auditor Checklist ISO 27552
  - Charity Program
  - Troubleshoot ISMS
  - Cafe Ilmu
  - Banking Framework
- Special project
- Conclusion

About CyberSecurity Malaysia

A BRIEF BACKGROUND

- Cybersecurity Malaysia journey started with the creation of the Malaysia Computer Emergency Response Team or MyCERT on the 13th of January 1997
- The National ICT Security & Emergency Response Centre (NISER) was created in 2001 as a department in MIMOS Berhad, and the Malaysia Computer Emergency Response Team (MyCERT) was placed under NISER.
- . On the 20th of August 2007, the Prime Minister of Malaysia officiated the rebranding of NISER into CyberSecurity Malaysia, and launched the new CyberSecurity Malaysia brand name and logo.

CyberSecurity MALAYSIA

INFORMATION SECURITY MANAGEMENT AND ASSURANCE (ISMA)

- Security Management and Best Practice change their name to Information Security Management and Assurance start early February
- In this department have 3 team which is :
  - Information Security Management System
  - Research
  - Business Continuity

Department Function

- RESEARCH
- PRIVACY
- BUSINESS CONTINUITY
- INFORMATION SECURITY MANAGEMENT SYSTEM

Industrial Training Activities

- RESEARCH
- AUDITOR CHECKLIST ISO/IEC 27552
- DEVELOP BANKING FRAMEWORKS
- CAFE ILMU
- CHARITY PROGRAM
- MAINTAINING AND TROUBLESHOOT ISMS
- JAMUAN HARI RAYA
- MOVING OUT

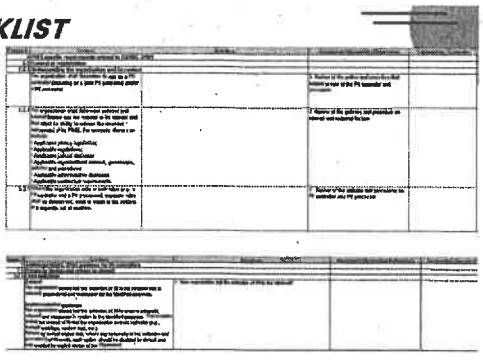
RESEARCH

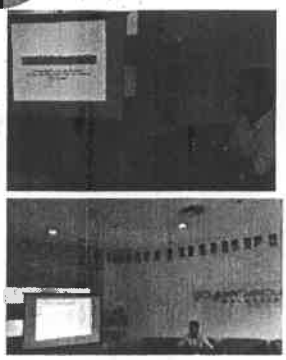
No	Article/Book/Journal	Years
1	Overcome the silent Threat : Building cyber resilience in airport	2018
2	Aviation insider treat: What We Know, our Finding and What we recommend	2017
3	Securing Smart Airports	2016
4	Smart Airport Cybersecurity: Threat mitigation and cyber resilience controls	2019
5	The Internet of things (IoT) and its impact on individual privacy: An Australian perspective	2016
6	Regulation and governance of the Internet of Things in India	2018
7	Enhancing social networking in smart cities: Privacy and security borderlines	2018
8	Security and privacy challenges in smart cities	2018

- **Privacy**
- **IR 4.0**
- **Cyber Threat at Airports**
- **ISO 27552 and PDPA**

AUDITOR CHECKLIST ISO/IEC 27552

- Understand about 3 actors
  - PII CONTROLLER
  - PII PROCESSOR
  - PII PRINCIPLE.
- **The objectives** auditor checklist is to guide and help the auditor to make the audit for ISO 27552, ensure that the audit scope is being followed, ensure a consistent audit approach and be used as an information base for planning future audits.





CAFE ILMU

- This event organize by knowledge Management Department
- Title that choose is "Ainul Hayat"
- Cafe Ilmu is one of the platforms that can help internship student to be known and improve their confident to speak in front crowd

MAINTAINING AND TROUBLESHOOTISMS

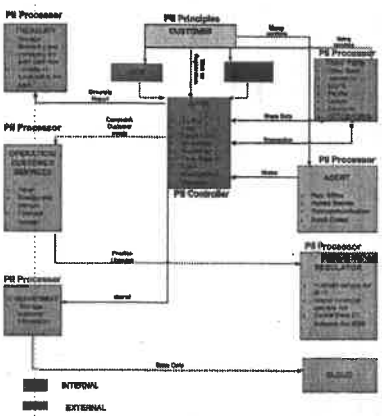
- *Identify bugs and error*
- *Using PHP language*
- *Port 139 and 135 is not connecting with their server*
- *Make report*

MOVING OUT

- On April 2019, CyberSecurity Malaysia it was moving out to a new building in Cyberjaya Selangor
- Activity
  - Pack all document
  - Tagging box
  - Appraisal Records
  - Disposed Records

DEVELOP BANKING FRAMEWORKS

- Identify the function
  - PII PRINCIPLE
  - PII PROCESSOR
  - PII CONTROLLER
- Identify sensitive data
- Identify services that provide by banking sector



RUMAH ANAK YATIM DAN ASNAF AS-SOLIHIN

Location: Banting Selangor
Number of orphans: Boys 33
Girls 20
Charity goods: Baju Kurung, Baju Melayu and Duit Raya

PERTUBUHAN KEBAJIKAN DAN SOSIAL REDHAMU TUHAN

Location: Semenyih, Selangor
Number of orphan: Boys 12
Girls 16
Charity goods: Baju Kurung, Baju Melayu and Duit Raya

OPEN HOUSE MINISTRY OF COMMUNICATION AND MULTIMEDIA MALAYSIA

- Organizes by Ministry of Communications and Multimedia Malaysia helds on 20 June 2019 at Dataran Gombang, Putrajaya

CYBERSECURITY MALAYSIA

- Organizes by CyberSecurity Malaysia held on 28 June 2019 at Menara Cyber Axis.

Privacy Awareness Website

IDEA

The idea to develop the privacy website come after the trainee involve in the develop privacy framework and guide line present in this organization.

PROBLEM

- Lack of awareness and knowledge to understand the importance of privacy
- Easy to share our privacy information to unauthorized person and organization
- Lack of exposure to children, staff and others society about data privacy management

OBJECTIVES

- To exposure the importance of privacy to the society
- To provide tips and tricks in managing and protecting the privacy of personal information
- To understand and implementation ISO 27002 as the privacy of Malaysia

Methodology

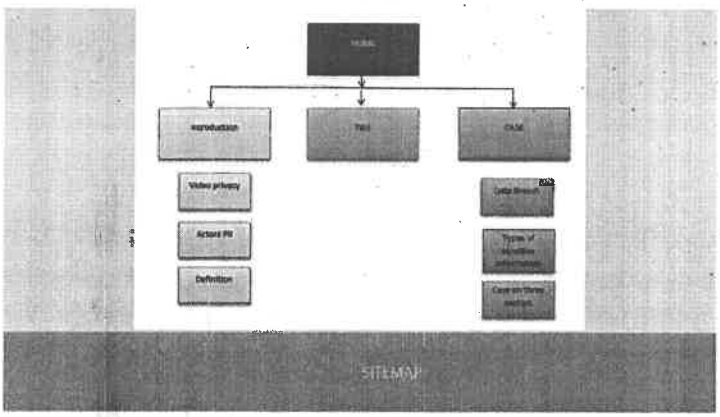
PLANNING

ANALYSIS

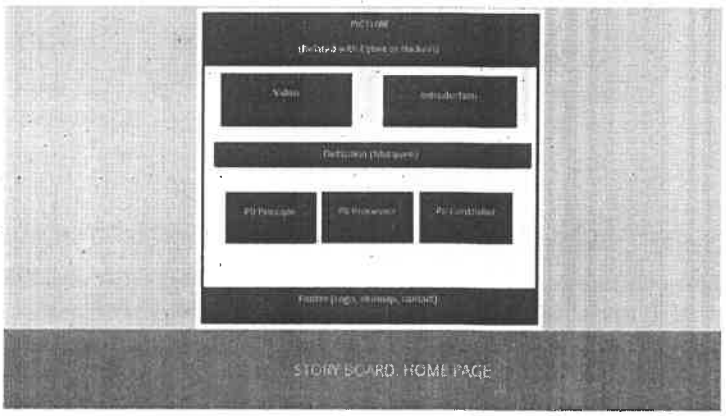
DESIGN

IMPLEMENTATION

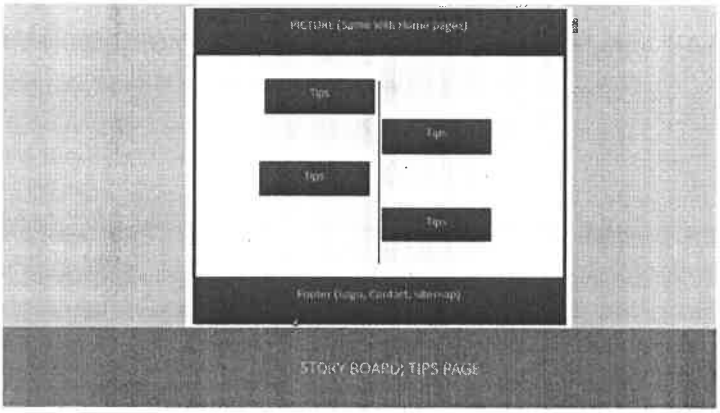
MAINTENANCE



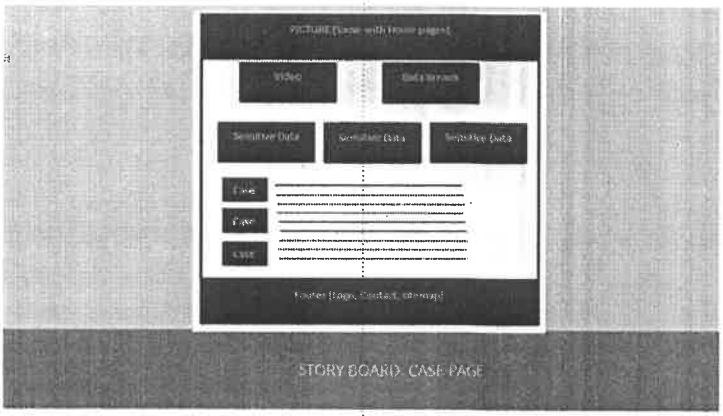
SITEMAP



STORY BOARD: HOME PAGE



STORY BOARD: TIPS PAGE



STORY BOARD: CASE PAGE

CONCLUSION