



**UNIVERSITI TEKNOLOGI MARA
FACULTY OF INFORMATION MANAGEMENT**

**INDUSTRIAL TRAINING REPORT:
CYBERSECURITY MALAYSIA (SELANGOR)
LEVEL 7, TOWER 1, MENARA CYBER AXIS, JALAN IMPACT,
63000 CYBERJAYA, SELANGOR**

**SPECIAL PROJECT: PRIVACY IMPLEMENTATION
GUIDELINES: AUDITOR CHECKLIST ISO/IEC DIS 27552**

**BY
NABILAH AQMAR BINTI RAZALI
2016317511**

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

01 FEBRUARY 2019 – 30 JUNE 2019

**INDUSTRIAL TRAINING REPORT:
CYBERSECURITY MALAYSIA (SELANGOR)
LEVEL 7, TOWER 1, MENARA CYBER AXIS, JALAN IMPACT,
63000 CYBERJAYA, SELANGOR**

**SPECIAL PROJECT: PRIVACY IMPLEMENTATION
GUIDELINES: AUDITOR CHECKLIST ISO/IEC DIS 27552**

**BY
NABILAH AQMAR BINTI RAZALI**

**FACULTY SUPERVISOR
MADAM SALLIZA MD RADZI**

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

01 FEBRUARY 2019 – 30 JUNE 2019

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

Nabilah Aqmar Binti Razali

2016317511

Date of submission: 04 July 2019

ABSTRACT

Internship session is start based on the period from 1ST FEBRUARY 2019 to 30 JUNE 2019 in Information Security Management Assurance (ISMA) Department at CyberSecurity Malaysia (CSM). There are many activities and memories that the trainee experiences during the internship at CyberSecurity Malaysia (CSM). The trainee experiences in both of the CSM building, which in Seri Kembangan and new building in Cyberjaya. During internship, the trainee is exposed with the information security and privacy which is an important knowledge that every person should notice and acknowledge. Other than that, the trainee is involved with the usage and implementation of the ISO standard that related to many guidelines, procedure, policy and regulation. The trainee is acknowledging with three of the ISO that related to the security and privacy, which the trainee is assigned to conduct research regarding the standard, in understanding the requirement needed, implementation guidance and additional of the requirement needed. Thus, the trainee is required to conduct research on Industry Revolution 4.0, Industry 4.0, Internet of Thing, Cloud Computing, Big Data and Smart City. Beside the working experiences, the trainee also experiences in having a good relationship with all other department in socializing between the officemate. Other than that, the trainee also involved with every company events which the trainee is invited in joining with other employee.

Keywords: *Information Security, privacy, guidelines, standard, ISO/IEC*

ACKNOWLEDGEMENT

Praise is upon the Almighty Allah for giving me the strength, health and facility to complete this assignment in time.

Firstly, I would like to express my sincere gratitude to Madam Salliza Md Razi (as Supervisor) for her kindly encouragement and guidance because without her guidance I could not properly do this task. She assists and teach me on how is the correct ways to completed this assignment. After that, towards my internship organization CyberSecurity Malaysia because, lean me a good experience while doing my internship at their company. Without their support, my internship cannot be completed successfully. With the guidance of my Supervisor, Pn Sabariah Ahmad (Head of Department (HOD)) and my team leader, Mrs. Naqliyah, all of the task given are very useful and consist of the continues values towards myself and also the organization.

I would like to thank my parents for their support in completing this assignment. Without their moral and financial support, I would not have been able to do it.

Finally, this task could not be done on time if it wasn't because of my friends motivated. I'd to appreciated their helps in encouraging me and help me to complete this assignment in good ways.

TABLES OF CONTENT

CONTENTS	
DECLARATION	i
ABSTRACT	ii
ACKNOWLEDGEMENT	iii
TABLES OF CONTENT	iv
LIST OF TABLES	vii
LIST OF FIGURES.....	vii
1. CHAPTER 1	1
1.1. Background of the organization	1
1.2. Organization Structure.....	5
2. CHAPTER 2	6
2.1. Departmental Structure	6
2.2. Department Function	7
3. CHAPTER 3	9
3.1. Training Activities	9
3.1.1. Ice Breaking	9
3.1.2. Research	9
3.1.2.1. Industry 4.0.....	9
3.1.2.2. Big Data	10
3.1.2.3. Cloud Computing.....	10
3.1.2.4. Smart City.....	11
3.1.2.5. Artificial Intelligent	11
3.1.2.6. Information Privacy and Information Security	11
3.1.3. Aviation Risk, Threat and Challenges.....	12
3.1.4. Auditor Checklist.....	12
3.1.5. Develop Framework.....	14
3.1.5.1. Healthcare Sector.....	14
3.1.5.2. Financial Sector	15
3.1.5.3. Telecommunication Sector	16
3.1.6. Comparative Analysis	17
3.1.7. Moving to New Building	19

3.1.7.1.	Appraise of The Record/Files.....	19
3.1.7.2.	Destruction and Disposal Of The Record	19
3.1.7.3.	Transferring of The Boxes	20
3.1.7.4.	Labelling The Boxes	20
3.1.8.	Data Transferring	22
3.1.9.	Open New Files	22
3.1.10.	Charity.....	23
3.1.11.	Knowledge Sharing	27
3.1.12.	Gathering	30
3.1.12.1.	Potluck	30
3.1.12.1.1.	Potluck with Level 4 And Level 6	30
3.1.12.1.2.	Potluck with Division	31
3.1.12.2.	Feast of Hari Raya	32
3.1.12.2.1.	Kementerian Komunikasi dan Multimedia	32
3.1.12.2.2.	Menara Cyber Axis.....	34
3.1.13.	Timelines	37
3.2.	Special Project.....	38
3.2.1.	Purpose of Project.....	38
3.2.2.	Overview on ISO/IEC 27552	38
3.2.2.1.	Introduction to Privacy	38
3.2.2.2.	Context of Privacy	40
3.2.2.3.	Importance of Privacy Protection	42
3.2.2.4.	Framework Implementation Guidance	43
3.2.2.4.1.	Healthcare Sector.....	43
3.2.2.4.2.	Banking Sector	46
3.2.2.5.	Implementation Guidance.....	49
3.2.3.	Information Privacy Risk on Organization	52
3.2.3.1.	Challenges.....	52
3.2.3.1.1.	Identity Theft	52
3.2.3.1.2.	Data Breach	53
3.2.3.1.3.	Human Error.....	53
3.2.3.2.	Privacy Risk.....	55
3.2.4.	Information Privacy Standard Based on ISO/IEC 27552	57

3.2.4.1. Implication of the development of Auditor Checklist.....	62
4. CHAPTER 4.....	63
4.1. Application Knowledge.....	63
4.1.1. Research Skill.....	63
4.1.2. Auditor Checklist.....	63
4.1.3. Comparative Analysis.....	64
4.1.4. Privacy and Security Awareness.....	64
4.1.5. Cyber Threat.....	65
4.2. Personal Thought and Opinion.....	66
4.3. Lesson Learnt.....	67
4.4. Limitation and Recommendation.....	69
5. REFERENCES.....	70
6. APPENDICES.....	71

LIST OF TABLES

Table 3. 1: Timeframe for all of the activities and task of the trainee.	37
Table 3. 2: Summary of the ISO/IEC DIS 27552 AND ISO/IEC 29100.	41
Table 3. 3: Actors and Data type applied for Healthcare Sector.	45
Table 3. 4: Actors and Data type applied for Banking Sector.	48
Table 3. 5: PIMS-specific requirements for ISO/IEC 27001	50
Table 3. 6: PIMS-specific requirements for ISO/IEC 27002	51
Table 3. 7: Privacy risk and opportunity identification, and responsible person involved ...	55

LIST OF FIGURES

Figure 1. 1: Timeline of the development of the CyberSecurity Malaysia (CSM).	1
Figure 1. 2: Timeline of the development of the CyberSecurity Malaysia (CSM).	1
Figure 1. 3: The Mines Waterfront building, previous CSM office.	2
Figure 1. 4: CSM also rent SAPURA building that located beside The Mines Waterfront building.....	3
Figure 1. 5: Organization Chart (Board of the Directors)	5
Figure 2. 1: Department Chart	6
Figure 2. 2: Information Security Management Assurances Department.....	8
Figure 3. 1: Industry 4.0 chart	9
Figure 3. 2: Auditor Checklist Sheet in Microsoft Excel	13
Figure 3. 3: Find relevent references to develop framework from National eHealth of Malaysia.	14
Figure 3. 4: Financial Sector relevant references from Banking Policy Requirement to support the framework	15
Figure 3. 5: Find out new issues regarding Telecommunication Sector.....	16
Figure 3. 6: Example of Comparative Analysis for standard of Privacy	17
Figure 3. 7: Comparative Analysis of management of PII in Banking Sector	18
Figure 3. 8: Put record that need to disposed into green container	19
Figure 3. 9: Transferring the record in the box	20
Figure 3. 10: The boxes with the label	21
Figure 3. 11: The trainee while labelling the boxes	21
Figure 3. 12: The orphan house at Kanchong Darat, Selangor	23
Figure 3. 13: Get to know them more closely	24

Figure 3. 14: Project Manager hands over the donation for Hari Raya AidilFitri to the owner of the orphanage.....	24
Figure 3. 15: Photo Session with them before leaving off to next orphanage.	25
Figure 3. 16: Next orphanage located at Semenyih.	25
Figure 3. 17: Photo session with owner of the orphanage.	26
Figure 3. 18: Knowledge Management @ Library at new building at Menara Cyber Axis, here is the place for knowledge sharing every Wednesday.....	27
Figure 3. 19: While sharing with them about experiences to Korea.....	28
Figure 3. 20: Knowledge Management @ Library in The Mines Building	28
Figure 3. 21: The sharer received appreciation souvenir from Knowledge Management Department.....	29
Figure 3. 22: Potluck with level 4 at The Mines, which consist of more than 4 department.	30
Figure 3. 23: Potluck with all of division with Vice President	31
Figure 3. 24: Sir Gobind Singh Deo came to CyberSecurity Malaysia booth	32
Figure 3. 25: Sir Gobind try our desert provided	33
Figure 3. 26: With CSM staff at front of the booth	33
Figure 3. 27: With person in charge of the booth from Outreach Department.....	34
Figure 3. 28: With Vice President Dr Masliana and all members of department	35
Figure 3. 29: With other colleague of CSM, such as good memories for the trainee	35
Figure 3. 30: With close friend at CSM.....	36
Figure 3. 31: Healthcare data framework, by showing the flow of PII.	44
Figure 3. 32: Financial sector data framework, by showing the flow of PII.....	47
Figure 3. 33: The initial document request list for audito checklist.....	50
Figure 3. 34: Auditor Checklist Clause 5	57
Figure 3. 35: Auditor Checklist Clause 5.3	58
Figure 3. 36: Auditor Checklist Clause 6	59
Figure 3. 37: Figure 29: Auditor Checklist Clause 7	60
Figure 3. 38: Auditor Checklist Clause 8	61

LIST OF APPENDICES

Appendix 6. 1: Log Book.....	71
Appendix 6. 2: Timeline (Schedule)	72
Appendix 6. 3: Presentation Slide	72
Appendix 6. 4: Attendances	72
Appendix 6. 5: Research Paper	72
Appendix 6. 6: Other Activities	72

1. CHAPTER 1 INTRODUCTION

1.1. Background of the 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 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 28 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.

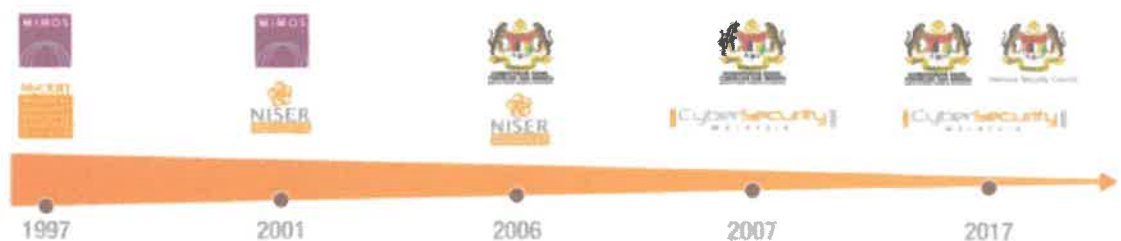


Figure 1. 1: Timeline of the development of the CyberSecurity Malaysia (CSM).

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 ten 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.

CyberSecurity Malaysia (CSM) located at Seri Kembangan at The Mines Waterfront Business Park building and Sapura Group building for over 13 years at these building start from 2007 until 2019. On April, 2019 CSM officially move in to own new building at Cyberjaya, names as Cyber Axis Tower.



Figure 1. 3: The Mines Waterfront building, previous CSM office.



Figure 1. 4: CSM also rent SAPURA building that located beside The Mines Waterfront building.

Vision

Our vision is to be a globally recognized 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 organisational 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. Organization Structure

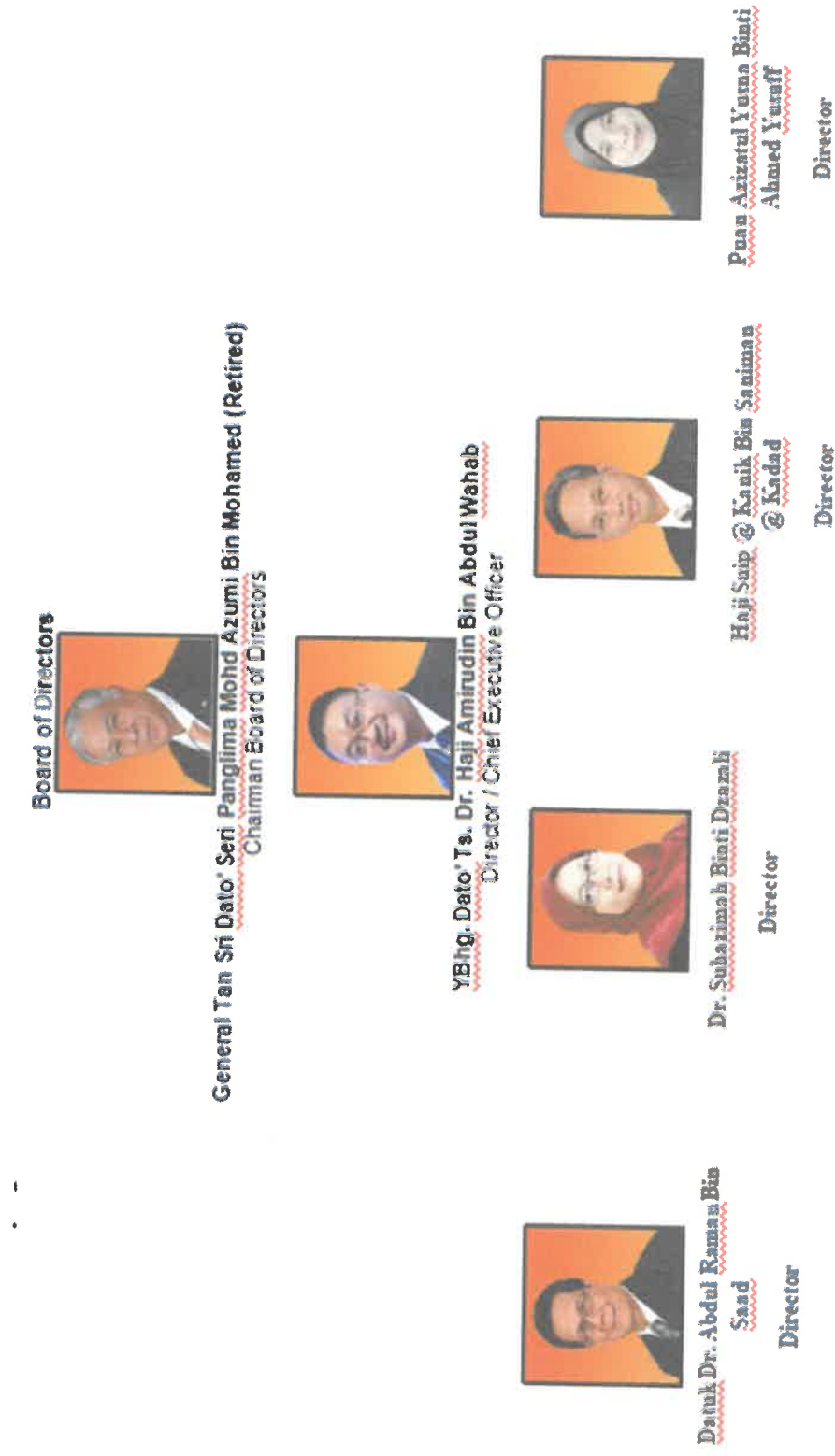


Figure 1. 5: Organization Chart (Board of the Directors)

2. CHAPTER 2 ORGANIZATION INFORMATION

2.1.1. Departmental Structure

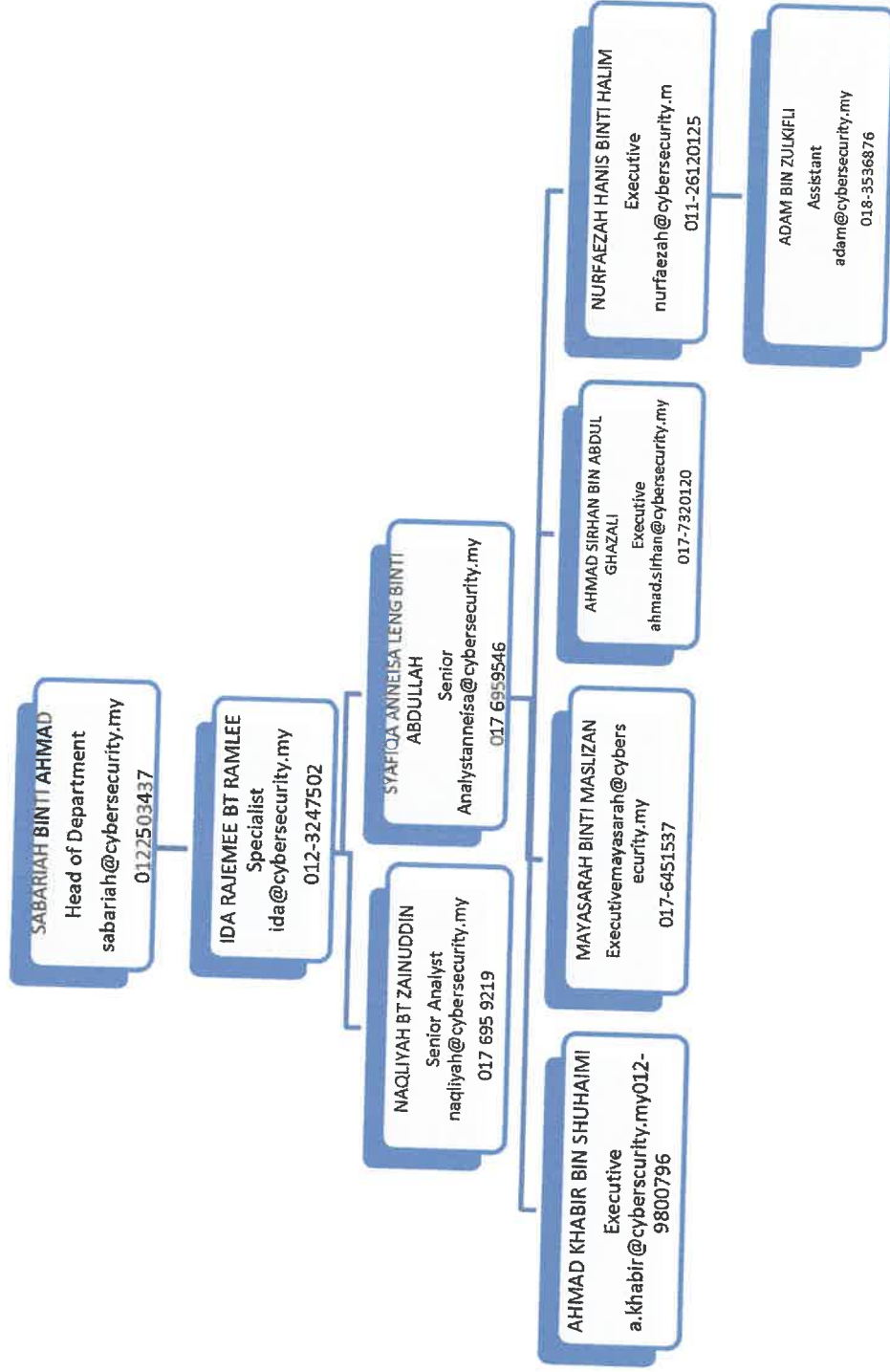


Figure 2. 1 : Department Chart

2.2. Department Function

Security Management & Best Practices

The primary role of Security Management & Best Practices (SMBP) department is to drive information security management based on ISO/IEC 27001:2005 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 programed, information security management review, development of information security policies and procedures and Business Continuity Management (BCM). For BCM team, were in charge in ensuring that CSM business continuity are well planned, and perform well. BCM team also known as BCM coordinator. BCM team also perform as a consultant for big company such as Malaysian Airport Holding Berhad.

In addition, this department also develops information security guidelines and best practices for the public with a view to assist them in securing their information security environment. This department also contribute towards standardization development in areas of information security; both locally and internationally. This department is like to invite everyone to visit their published guidelines and best practices. Other than that, this department were handling the policy for internal of the CSM, which this department were in charge in ensuring that CSM are fully utilized and implement the ISMS policy and procedure. Thus, SMBP will conduct the internal audit for CSM. This team also known as ISMS driver which is Information Security management for an organization security management system (ISMS) standard. Thus, this department also involved in managing Information Security Governance, Risk and Compliance.

While, there are also a team for Applied Research for Security Management & Resilience Services and Joint effort with National Security Council to deliver annual National Cyber Drill Exercise that known as (X-MAYA). Participate in standard development for information security at national and international levels. This department is also entrusted to deliver trainings and awareness talks related to ISMS to external organizations. In the early of the February, this department changes their name from Security Management Best Practice (SMBP) into Information Security Management Assurances (ISMA).



Figure 2. 2: Information Security Management Assurances Department

3. CHAPTER 3 INDUSTRIAL TRAINING ACTIVITIES

3.1. Training Activities

3.1.1. Ice Breaking

3.1.2. Research

The main task and responsibilities of the trainee is research, which the trainee are allocated for research team under Information Security Management Assurances (ISMA). The trainee is required to conduct research which with the topic given by the team leader. The research is conduct by method of review the previous research paper. There are few topics given by the team leader that cover on the security and privacy and the current issues related to the advancement of the technology.

3.1.2.1. Industry 4.0

Industrial Revolution 4th is a total transformation of all industries' sectors from primary, secondary, tertiary, and Quaternary sector. While, from the secondary sector, from German Government's strategic initiative which to transform the secondary industry into modernized cybernetic based manufacturing and production system that are efficient and more cost effective. To establish Germany as a lead market and provider of advanced manufacturing solutions, which known as Smart Manufacturing and Industry Internet of Things.

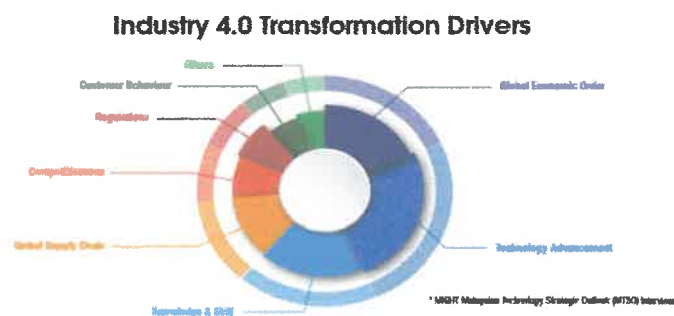


Figure 3. 1: Industry 4.0 chart

Based on the Malaysia Industry 4.0 stated that at the heart of Industry 4.0 is a set of rapidly evolving and converging technologies. These are pushing the boundaries of what can be manufactured through additive manufacturing and advanced materials. These technologies are enabling richer insights through big data analytics. They are enhancing human capacity through artificial intelligence and autonomous robots. These greater efficiencies changing the traditional manufacturing system production relationships between suppliers, producers, and customers as well as between humans and machines.

3.1.2.2. Big Data

Increasingly big data techniques are being applied in manufacturing industries to improve customer experience and product quality, realise energy efficiencies, and conduct predictive maintenance. It is now possible to collect masses of data from several different sources to direct decisions that anticipate product or equipment failure.

3.1.2.3. Cloud Computing

Cloud computing is a computing paradigm, where a large pool of systems is connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of the technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment. There are three services offered for cloud computing which is :

1. Software as a Service (SaaS):
2. Platform as a Service (Paas)
3. Infrastructure as a Service (IaaS)

3.1.2.4. Smart City

Smart City is the technology which implemented towards the needs of the city. Smart City nowadays be applied to the facilities in the city such as Traffic Light, and Streetlight that already applied at the Malaysia.

3.1.2.5. Artificial Intelligent

AI is a concept that is made up of numerous subfields such as machine learning, which focuses on the development of programme that can teach themselves to learn, understand, reason, plan, and act when exposed to new data in the right quantities. AI technology will supplement the smart factory towards networked factory, in which data from supply chains, design teams, production lines and quality control are linked to form a highly integrated and intelligent engine.

3.1.2.6. Information Privacy and Information Security

Information privacy is currently regarded as an element of information security processes, the actual coverage of information privacy in technical security standards of all layers will be now explored. Through this analysis the need for

information privacy guidelines, in reference to the above layers, is highlighted.

Security must consist of CIA, which is Confidential, Integrity and Availability

3.1.3. Aviation Risk, Threat and Challenges

For the cyber security in aviation sector which is airport that the risks are frequently changing due to the new vulnerabilities and threat that may evolve and affect. This happened because it is being parallel with the advancement and changing of the technology implementation. In aviation sector, malicious cyber-threats that may influence and affect the operational efficiency of smart airports in aviation sector, that are equipped with IoT applications, are developed and analysed.

3.1.4. Auditor Checklist

The trainee is given a task which to acknowledged and understood ISO standard that related to Privacy. The type of ISO that related to privacy and security which focusing on the Personal Identifiable Information (PII). The trainees required to review and acknowledge ISO/IEC 27001, ISO/IEC 27002, ISO/IEC DIS 27552, and ISO/IEC 29100. Each of the ISO has related issues and concept which to complement each other. To develop the checklist, the trainee needs to conduct research related to the industry processing data. The checklist is consisting of the clause, sub clause, information document references and also the supportive question which to assist the auditor.

There are five clause allocated for that standard, which this standard defines additional requirements and provides guidance for the protection of privacy as potentially affected by the processing of PII, enabling the organizations' overall Management System to be extended to cover both the general requirements for information security which known as Information Security Management System (ISMS) and the more specific requirements for PII protection, both together establish a Privacy Information Management System (PIMS). These additional requirements and guidance are written in such a way that they are practically usable for PII protection by organizations of all sizes and cultural environments.

All of the checklist is completed by five months of the internship, which started from February until June. The checklist is regularly monitored by the team leader and head of the department. There are few meetings conducted which to fulfil the needs of the checklist, with team leader, assist team leader and head of the department. The trainee is required to present the task performed, which to update to head of the department regarding the checklist assessment.

14	6.2.2	Protection from malware			
15	6.2.3	Control against malware			
16	6.2.4	Control against malware			
17	6.2.5	Control against malware			
18	6.2.6	Control against malware			
19	6.2.7	Control against malware			
20	6.2.8	Control against malware			
21	6.2.9	Control against malware			
22	6.2.10	Control against malware			
23	6.2.11	Control against malware			
24	6.2.12	Control against malware			
25	6.2.13	Control against malware			
26	6.2.14	Control against malware			
27	6.2.15	Control against malware			
28	6.2.16	Control against malware			
29	6.2.17	Control against malware			
30	6.2.18	Control against malware			
31	6.2.19	Control against malware			
32	6.2.20	Control against malware			
33	6.2.21	Control against malware			
34	6.2.22	Control against malware			
35	6.2.23	Control against malware			
36	6.2.24	Control against malware			
37	6.2.25	Control against malware			
38	6.2.26	Control against malware			
39	6.2.27	Control against malware			
40	6.2.28	Control against malware			
41	6.2.29	Control against malware			
42	6.2.30	Control against malware			
43	6.2.31	Control against malware			
44	6.2.32	Control against malware			
45	6.2.33	Control against malware			
46	6.2.34	Control against malware			
47	6.2.35	Control against malware			
48	6.2.36	Control against malware			
49	6.2.37	Control against malware			
50	6.2.38	Control against malware			
51	6.2.39	Control against malware			
52	6.2.40	Control against malware			
53	6.2.41	Control against malware			
54	6.2.42	Control against malware			
55	6.2.43	Control against malware			
56	6.2.44	Control against malware			
57	6.2.45	Control against malware			
58	6.2.46	Control against malware			
59	6.2.47	Control against malware			
60	6.2.48	Control against malware			
61	6.2.49	Control against malware			
62	6.2.50	Control against malware			
63	6.2.51	Control against malware			
64	6.2.52	Control against malware			
65	6.2.53	Control against malware			
66	6.2.54	Control against malware			
67	6.2.55	Control against malware			
68	6.2.56	Control against malware			
69	6.2.57	Control against malware			
70	6.2.58	Control against malware			
71	6.2.59	Control against malware			
72	6.2.60	Control against malware			
73	6.2.61	Control against malware			
74	6.2.62	Control against malware			
75	6.2.63	Control against malware			
76	6.2.64	Control against malware			
77	6.2.65	Control against malware			
78	6.2.66	Control against malware			
79	6.2.67	Control against malware			
80	6.2.68	Control against malware			
81	6.2.69	Control against malware			
82	6.2.70	Control against malware			
83	6.2.71	Control against malware			
84	6.2.72	Control against malware			
85	6.2.73	Control against malware			
86	6.2.74	Control against malware			
87	6.2.75	Control against malware			
88	6.2.76	Control against malware			
89	6.2.77	Control against malware			
90	6.2.78	Control against malware			
91	6.2.79	Control against malware			
92	6.2.80	Control against malware			
93	6.2.81	Control against malware			
94	6.2.82	Control against malware			
95	6.2.83	Control against malware			
96	6.2.84	Control against malware			
97	6.2.85	Control against malware			
98	6.2.86	Control against malware			
99	6.2.87	Control against malware			
100	6.2.88	Control against malware			

Figure 3. 2: Auditor Checklist Sheet in Microsoft Excel

3.1.5. Develop Framework

The trainee is assigned to develop framework for three sector that focus on Healthcare Sector, Financial Sector, and Telecommunication Sector. For every sector, deep research must be conduct which to find out the flow of the Personal Identifiable Information (PII) of every process acquired. The trainee needs to conduct research on these three sectors that focus PII of the principles and how the data are distributed and whose are responsible person that can accessed the PII. To develop the framework, there are many changes occur which to produce a good framework that are used as a solid industry processes.

3.1.5.1. Healthcare Sector

There are many parties involved the managing and using the data or PII of the principles. The purposed of using the PII instead for the medical purposed is for the research purposed conduct by the Ministry of Health of Malaysia.

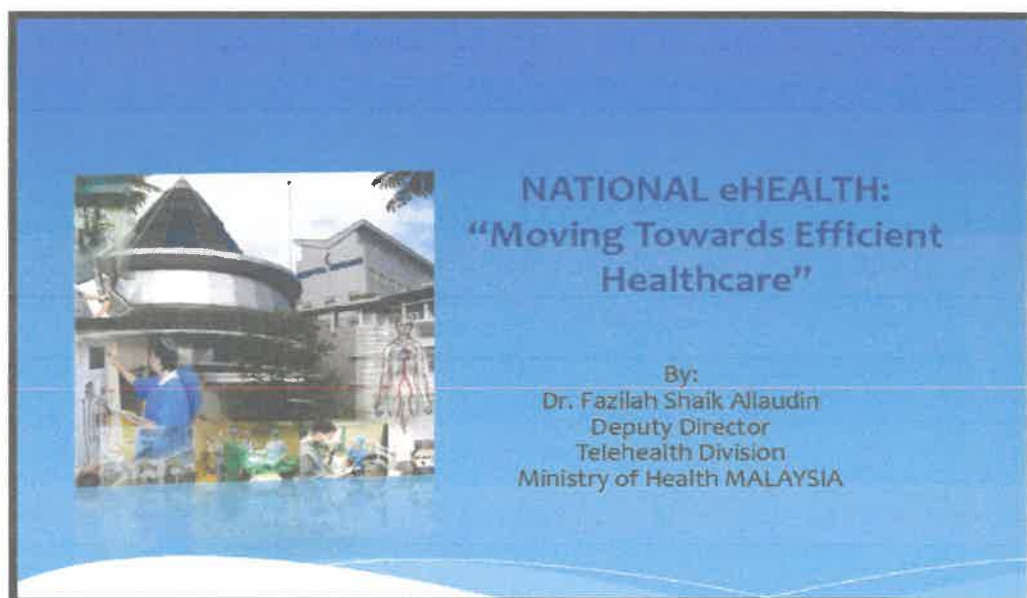


Figure 3. 3: Find relevant references to develop framework from National eHealth of Malaysia.

3.1.5.2. Financial Sector

For financial sector, the PII of the principle must securely protected by the PII controller which known as bank organization. The PII of the principle in the financial sector are frequently breach due to the unresponsive action taken by the unauthorised person, which for the purpose of marketing, selling data and many more. Other than that, financial sector is the sector that highly risk, and threaten for the scenario of breaching and exposing of the PII and sensitive data.

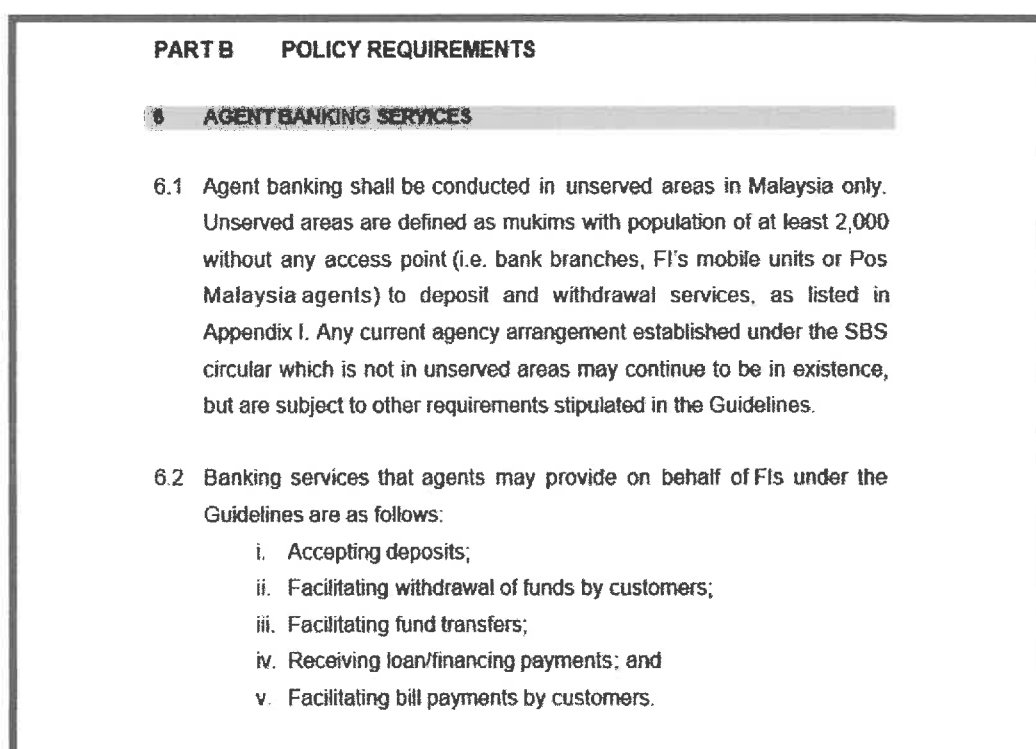


Figure 3. 4: Financial Sector relevant references from Banking Policy Requirement to support the framework

3.1.5.3. Telecommunication Sector

For the Telco Sector, that more focusing on the communication line such as Maxis, Celcom and Digi. This sector are also as part of the highly risk and threaten of the data, PII and sensitive data breaches and exposing. Which this sector dealing with many third parties and agent.

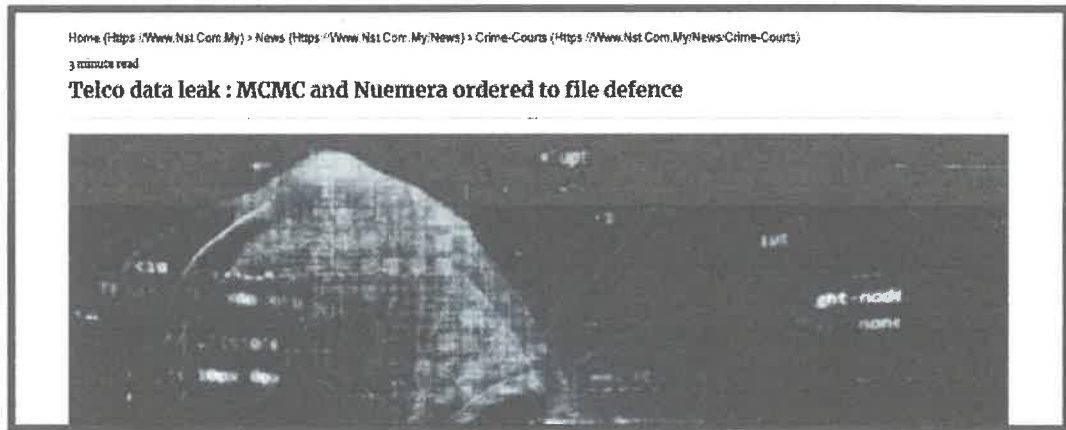


Figure 3. 5: Find out new issues regarding Telecommunication Sector.

3.1.6. Comparative Analysis

Each of the research conduct on every of the topic assigned, the trainee are required to developed comparative analysis which by comparing each of the result of the research paper, by comparing every paper result. The comparative analysis must be performed in the Microsoft Excel, which is easier for the trainee to presenting to the head of the department, team leader and assist team leader. Every research conducted must be shared with the team, which is the the trainee and the colleague exchanging opinion, information and knowledge based on the finding of the research.

Standard/ Framework	Principles	Industry Environment	Responsible
APEC Privacy Framework 2005	<ul style="list-style-type: none"> ➤ Preventing Harm ➤ Notice ➤ Collection Limitation ➤ Uses of Personal Information ➤ Choice ➤ Integrity of Personal Information ➤ Security Safeguard ➤ Access and Correction ➤ Accountability 	9 Focus on common privacy issues and the impact of privacy issues upon the way legitimate businesses are conducted. It does so by highlighting the reasonable expectations of the modern consumer that businesses will recognize their privacy interests in a way that is consistent with the Principles outlined in this Framework.	➤ Personal information controller means a person or organization who controls the collection, holding, processing or use of personal information. It includes a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf, but excludes a person or organization who performs such functions as instructed by another person or organization.
The Software Alliance BSA Privacy Framework	<ul style="list-style-type: none"> ➤ Transparency ➤ Purpose Specification ➤ Informed Choice ➤ Data Quality ➤ Consumer Control ➤ Security ➤ Facilitating Data use for legitimate Business Interest ➤ Accountability ➤ Legal Compliance & Enforcement ➤ International Interoperability 	10 Transparency of personal data collection and use; enable and respect informed choices by providing governance over that collection and use; provide consumers with control over their personal data; provide robust security; and promote the use of data for legitimate business purposes.	

Figure 3. 6: Example of Comparative Analysis for standard of Privacy

	Personal Data	Collection of Personal Data	Purposes for the collection	Disclosure of personal Data
Bank Of Singapore	Name, NRIC, passport or other identification number, telephone number[s], mailing address, email address, transactional data and any other information relating to any individuals which you have provided us in any forms you may have submitted	<ol style="list-style-type: none"> When you submit any form, including but not limited to application forms or other forms relating to any of our products or services or any investments which you purchase through the Companies When you enter into any agreement or provide other documentation or information in respect of your interactions with us, or when you use our services When you interact with our staff, including relationship managers and their assistants, example via telephone calls (which may be recorded), letters, fax, face-to-face 	<ol style="list-style-type: none"> Responding to, processing and handling your complaints, queries, requests, feedback and suggestions Verifying your identity and customer due diligence Managing the administrative and business operations of the Companies and complying with internal policies and procedures (including but not limited to facilitating business continuity planning) 	<ol style="list-style-type: none"> Companies providing services relating to insurance and/or reinsurance Trustees, attorneys and asset managers appointed by you to manage your account Agents, contractors, vendors, installers, or third party service providers who provide administrative or operational services Credit reporting agencies Debt collection agencies Corporate service providers or lawyers, who are appointed by you
Indefinite	Personal Data	Collection of Personal Data	Purposes for the collection	Disclosure of personal Data
	Personal Information" means information that can personally identify an individual, such as name, address, email address, phone number, social security number, date	Collect Personal Information and Non-Personal Information through the Website, including information you provide voluntarily, such as:	<ol style="list-style-type: none"> Respond to your inquiries and process your request for services, products, or information Develop, improve, or approve new products or services 	<ol style="list-style-type: none"> To another business entity in the event of a merger, restructuring, acquisition, any other sale or transfer of our assets or liabilities, or any change in ownership control

Figure 3. 7: Comparative Analysis of management of PII in Banking Sector

3.1.7. Moving to New Building

The trainee is required to help department to prepare for the moving out to new building until 17 April. Through the process of moving, the trainee also learn about the record management and filing on how to manage record for moving out. Thus, to classify the record according to the boxes allocated. Other than that, the trainee also learns new experience in appraisal the record, destruction, and disposal.

3.1.7.1. Appraise of The Record/Files

The trainee is required to appraised the record based on the date of the publication by referring to the ISMS driver which known as Ms Hanes. She is in changes for the moving out for our department.

3.1.7.2. Destruction and Disposal Of The Record

The trainee helps the ISMS driver in destructing the record by using the shredding machines. Before shredding the record, the record must be put into the green container before shredding the records.



Figure 3. 8: Put record that need to disposed into green container

3.1.7.3. Transferring of The Boxes

The trainee also helped in transferring the records from the selves to the boxes given by the third party that supplying the boxes, wrapping and deliver the boxes to new building. There are three different boxes given by the SABALI holding, which is organization that handling the delivering the boxes. One boxes is for confidential box, personal box and moving record box, which the size is more bigger than other two boxes.

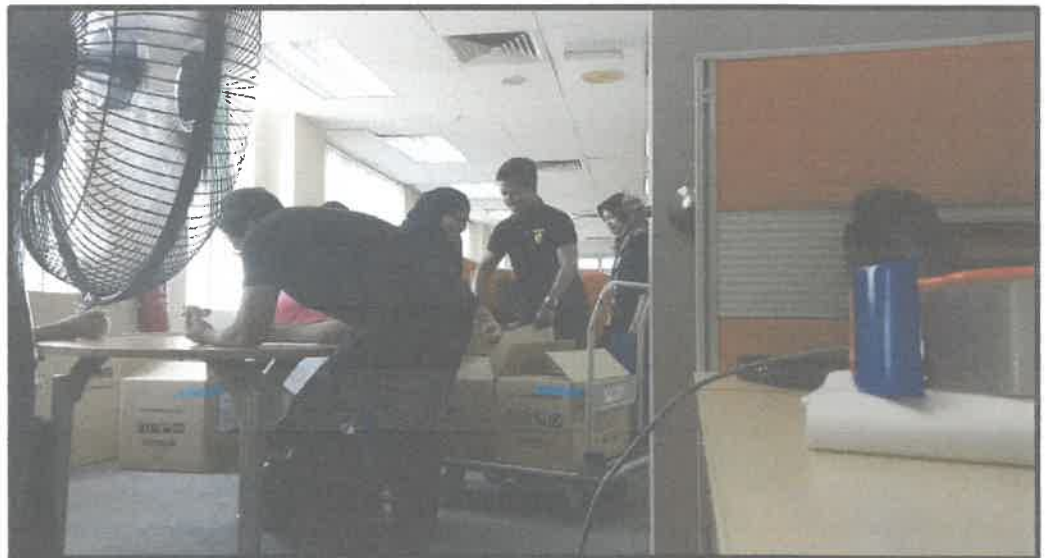


Figure 3. 9: Transferring the record in the box

3.1.7.4. Labelling The Boxes

The trainee also in change in labelling the boxes which is to easier for the SABALI Holding in sorting the boxes for each of the department because to avoid from misplace of the boxes. Other than that, for easier for the ISMS driver in noticing which boxes are department owned.



Figure 3. 10: The boxes with the label

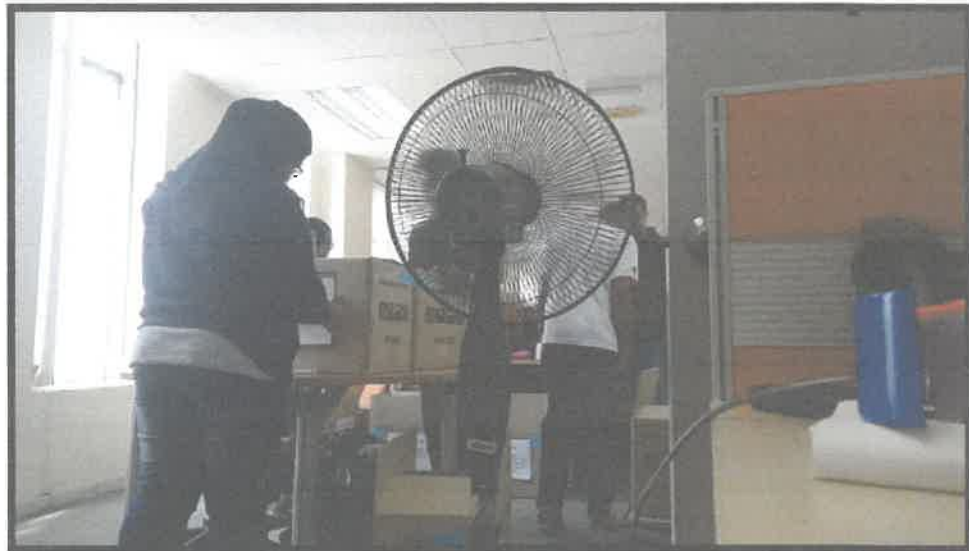


Figure 3. 11: The trainee while labeling the boxes

3.1.8. Data Transferring

The trainee help other team in converting data from the questionnaire conducted by the ISMS driver towards third agency. The trainee also need to converting the data into the excel format, which is easy for the ISMS to calculate the risk and other related processes. Other than that, the trainee also help in calculating the respondent based on the position of the respondent.

3.1.9. Open New Files

The trainee also help ISMS driver in opening new files regarding the ISMS assessment which is the file that related to the ISMS policy, procedure and requirement followed by the internal of the organization. The trainee is assigned which to labeling the files, by using CSM formatting of files, and write up the description of the files into files paper document.

3.1.10. Charity

The program to do charity which to donate to orphanage was planned over 2 weeks before the event. This charity collected the donation from the employees which by donating cloth, money, beg, shoes, and many more. The entire items are packed neatly and clean. The donation given and selected in a good condition.

The trainee helps packing the item and managed the collection regarding the classification number of each box. Over 40 boxes are managed to be collect for this charity, which completed with all of item. Two day before the event held, the trainee helps the project manager in handling the item. During the event held, the trainee help other employees with carrying the boxes, served the “Orphan” family and shared on giving “Duit Raya” to them.



Figure 3. 12: The orphan house at Kanchong Darat, Selangor



Figure 3. 13: Get to know them more closely



Figure 3. 14: Project Manager hands over the donation for Hari Raya Aidilfitri to the owner of the orphanage.



Figure 3. 15: Photo Session with them before leaving off to next orphanage.



Figure 3. 16: Next orphanage located at Semenyih.



Figure 3. 17: Photo session with owner of the orphanage.

3.1.11. Knowledge Sharing

On 27th March the trainee is performed a knowledge sharing which is the activities that are conducted every Wednesday, anyone from the company can share any experience, knowledge and information during this session. There are two to three people are allowed to share during in one week. While, during the trainee sharing session, the trainee shared about the experienced while going to Korea on November 2018. Other than that, the trainee also shared about the tips and tricks when going to Korea, which may help others if planning going to that country. Every Wednesday, the trainee is attending the knowledge sharing session which is to get to know new information, and knowledge.



Figure 3. 18: Knowledge Management @ Library at new building at Menara Cyber Axis, here is the place for knowledge sharing every Wednesday

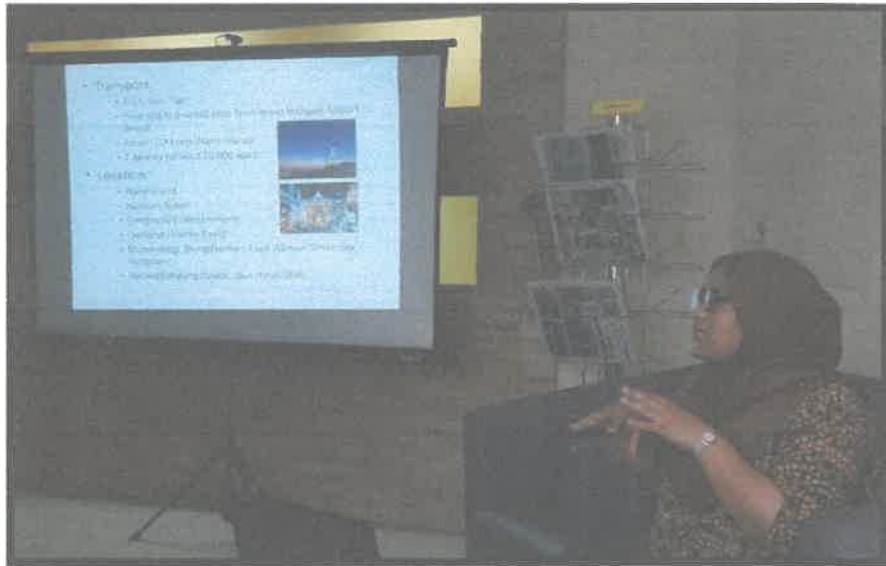


Figure 3. 19: While sharing with them about experiences to Korea



Figure 3. 20: Knowledge Management @ Library in The Mines Building



Figure 3. 21: The sharer received appreciation souvenir from Knowledge Management Department

3.1.12. Gathering

3.1.12.1. Potluck

3.1.12.1.1. Potluck with Level 4 And Level 6

At end of the months, every department located at Level 4 is making Potluck session which to strengthen relationship and friendship between the colleagues. After moving to new building the tradition are still continuing until now. Which by transferring to new building the Potluck with start with reciting Surah Yassin together with other department.



Figure 3. 22: Potluck with level 4 at The Mines, which consist of more than 4 department.

3.1.12.1.2. Potluck with Division

Before moving to new building, division of the trainee department which known as Cyber Security Proactive Services Division conducting Potluck which to celebrate new building and celebrate previous memories at previous building.



Figure 3. 23: Potluck with all of division with Vice President

3.1.12.2. Feast of Hari Raya

3.1.12.2.1. Kementerian Komunikasi dan Multimedia

Attended to the banquet of Hari Raya which conducted by Kementerian Komunikasi dan Multimedia (KKM) at PICC Putrajaya. CyberSecurity Malaysia is an agency under this ministry was invited to this ceremony. There are many activities during the event. Each of the agency must contributed a dishes, which CyberSecurity Malaysia provided a desert such as Pisang Cheese and Keledek Cheese.



Figure 3. 24: Sir Gobind Singh Deo came to CyberSecurity Malaysia booth



Figure 3. 25: Sir Gobind try our desert provided



Figure 3. 26: With CSM staff at front of the booth



Figure 3. 27: With person in charge of the booth from Outreach Department

3.1.12.2.2. Menara Cyber Axis

On the last day of the internship, Menara Cyber Axis is conducting banquet of Hari Raya which with all the department, and also with other organization that allocated in a same building, such as Nacsa, Jabatan Standard Malaysia and MyNIC Malaysia. There are many attractions that facilitating for the employee in Menara Cyber Axis.



Figure 3. 28: With Vice President Dr Masliana and all members of department



Figure 3. 29: With other colleague of CSM, such as good memories for the trainee



Figure 3. 30: With close friend at CSM

3.1.13. Timelines

Table 3. 1: Timeframe for all of the activities and task of the trainee.

TASK & ACTIVITIES	MONTH															
	FEBRUARY			MARCH			APRIL			MAY			JUNE			
1 Research and Review Concept of Security & Privacy • Review ISO/IEC 29100 • Review ISO/IEC 27552 • Review ISO/IEC 27001 • Review ISO/IEC 27002	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	8	2	1	1	1	2	8	2	2	1	2	2	3	1	1	2
	5	5	1	8	5	1	5	2	2	3	7	7	0	1	7	4
	100/100%															
	50/100%															
2 Develop Framework • Research (Financial sector, Telecommunication Sector, and Healthcare Sector) • Design (Microsoft Office Visio)	50/100%															
	50/100%															
3 Research Conduct • Industry Revolution 4.0 • Industry Revolution • Cloud Computing • Big Data • Artificial Intelligence , ETC	70/100%															
	80/100%															
4 Research Paper • Conduct Research (previous research paper) • Collect Data • Develop paper (IEEE format)	80/100%															
	80/100%															
5 Auditor Checklist Implementation Guidance ISO/IEC DIS 27552 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines	80/100%															

3.2. Special Project

3.2.1. Purpose of Project

The purpose of this document is to provide an implementation framework for ISO/IEC 27552. ISO/IEC 27552 is a newly released standard and an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management that focus on requirement and guidelines. This framework will assist organizations from various sectors to proficiently implement the ISO/IEC 27552 at their organizations.

3.2.2. Overview on ISO/IEC 27552

3.2.2.1. Introduction to Privacy

Based on the ISO/IEC 29100, this standard is published which to enhance the existing of the security standard by adding a focus that relevant to the processing of privacy. Thus, in this standard, there are privacy framework generated which to serve as a basis for privacy standardization initiatives which used for controlling the privacy for outsourced data processes and acknowledge about the privacy risk assessment.

Other than that, this standard which can be used as technical references for organization and auditor in evaluating the architecture of privacy in the organization. Privacy safeguarding requirement help organization in specify the privacy terminology which help organization to familiar with the concept of privacy. Other than that, this requirement also defines the actor and roles of privacy in processing the personal identifiable information. Thus, primary is describing the privacy safeguarding requirement which can assist the organization in effective implementation of privacy by referring to the privacy principles.

While ISO/IEC DIS 27552, this standard provides guidance for the protection of the privacy which enables the organization management system that cover on general and specific requirement for personal identifiable information (PII) protection. After that, 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.

Information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data [1]. According to [2], stated that privacy 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. There are few standards that cover on a privacy implementation which is ISO/IEC 27552, and ISO/IEC 29100.

To conclude, privacy is personal information related to the owner of the data which can be exposed with the consent of the owner for the specific purpose. Privacy data is data that own by the owner which describe, identifiable and define the criteria and concept of the ownership. Privacy must be protected from getting access, expose and breach to public. The valuable data must be secure by individual and organization either for personal data privacy or others data privacy according to privacy policy of an organization.

3.2.2.2. Context of Privacy

There are three actors used in privacy concept which is to refer to the person involvement in the process.

1. 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.

2. PII Control

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.

3. 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.

Table 2 below shows the summary of the context, content, element, which covered in the standard of the privacy used to develop the implementation.

Table 3. 2: Summary of the ISO/IEC DIS 27552 AND ISO/IEC 29100.

ISO/IEC DIS 27552 *This standard is Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management that focus on requirements and guidelines	ISO/IEC 29100 * This standard focus on Information technology for Security techniques by providing Privacy framework.
<p>Focus : Specifies requirements and provides guidance for establishing, implementing, maintaining and 261 improving a Privacy Information Management System (PIMS) in the form of an extension to 264 ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.</p>	<p>Focus: Control privacy technology, define the actors and their roles in assessing PII describing privacy safeguarding requirements, and referencing known privacy principles.</p>
<p>Extension</p> <ul style="list-style-type: none"> o ISO/IEC 27001 	<p>Extension</p> <ul style="list-style-type: none"> o ISO/IEC 27002
<p>Requirement</p> <ul style="list-style-type: none"> ➤ Context of the organization ➤ Leadership ➤ Planning ➤ Support ➤ Operation ➤ Performance evaluation ➤ Improvement 	<p>Actors and Roles</p> <ul style="list-style-type: none"> ➤ PII – Personal identifiable information ➤ PI Principles ➤ PI Controller ➤ PI Processor <p>Possible flows of PII among the PI principal, PI controller, PI processor and a third party and their roles</p>
<p>Guidelines</p> <ul style="list-style-type: none"> ➤ Information Security Policies ➤ Organization Info. Security ➤ Human Resource Security ➤ Asset management ➤ Access control ➤ Physical and environment security ➤ Operation security ➤ Communication security ➤ System acquisition, development, and Maintenance ➤ Supplier relationship ➤ Information Security Incident Management ➤ Info. Security aspects of business continuity management ➤ Compliance 	<p>Interaction</p>
<p>Addition Guidance</p> <ul style="list-style-type: none"> o PII Controller 	<p>Recognizing PII</p> <ul style="list-style-type: none"> ➤ Identifier ➤ Pseudonymous data ➤ Unsolicited PII ➤ info. Linked to PII Principles Metadata Sensitive PII
<p>Conditions for collection and processing</p> <ul style="list-style-type: none"> ➤ Obligations to PII ➤ Principles ➤ Privacy by design and by privacy default ➤ PII sharing, transfer and disclosure 	<p>Privacy Safeguarding requirement</p> <ul style="list-style-type: none"> ➤ Legal and regulatory factors ➤ Contractual factors ➤ Business factors ➤ Other factor :
<p>Conditions for collection and processing</p> <ul style="list-style-type: none"> ➤ Obligations to PII ➤ Principles ➤ Privacy by design and by privacy default ➤ PII sharing, transfer and disclosure 	<p>Privacy Policies</p> <ul style="list-style-type: none"> ➤ The term "privacy policy" is often used to refer to both internal and external privacy policies.
<p>Privacy Control</p>	<p>Privacy Control</p> <ul style="list-style-type: none"> ➤ Organizations should identify and implement privacy controls to meet the privacy safeguarding requirements identified by the privacy risk assessment and treatment process.

3.2.2.3. Importance of Privacy Protection

Based on the previous research paper [3] stated that the main motive to protect personal information or to selectively disclose that information is to avoid conflict. Which mean that, personal data that related to the person must be protected from unauthorized user because to prevent from getting access by irresponsible person that could misuse the data for other purpose that led to be more conflict and critical problem. Other than that, privacy is important for many different reasons which is for the purpose of solitude, autonomy, emotional release, self-evaluation, limited and protected communication (Westin, 1970), the reduction of personal distress (Newell, 1994), and the need for intimacy and psychological respite and the desire for protection from social influence and control (Margulis, 2003).

Furthermore, data privacy must be protected from any unauthorized user, because with the data receive irresponsible person could misuse the data and exposed the data to other people by selling the personal data for the purpose of business marketing or criminal matters. Other than that, privacy must be securely protected by the organization from getting distributed and breach. Privacy data is personal data that cannot be displayed to the public and sharing are based on the consent of the personally identifiable information (PII) principles.

In conclusion, privacy is very important to all organization to make sure that all personally identifiable information (PII) is protected well. Nowadays, everyone should concern and acknowledge the importance of privacy which to ensure that they can manage their information properly and to avoid from share their personal information to an unauthorized person.

3.2.2.4. Framework Implementation Guidance

3.2.2.4.1. Healthcare Sector

Healthcare sector is organization or company that facilitates provision of healthcare to patients. Healthcare sector provide goods and services to patients relating to the health care and medical insurance. Other than that, healthcare also provides medical device manufacturers and medical equipment or drugs. In healthcare sector, in processing and facilitate patients, information privacy of the patients are needed and used.

According [4] to stated that informational privacy is an important principle in health care. It supports patients' dignity, self-determination, and patient safety. Informational privacy concerns information related to patient's health, how it should be protected, and who has the right to access it. Informational privacy is defined as the patient's right to decide how, when, and how much information they are willing to share with another person¹⁴ or in the health care organization.

For the Healthcare sector, the organizations possess two types of data to be kept by them such as PII data and sensitive data. PII is Personal Identifiable Information which relates to the owner of the data or information that is own by the PII principal. While, sensitive data in the context of healthcare is the medical information, medical result and other most intimate sphere, or that might have a significant impact on the PII principal. Both data should be protected from being exposed or breached.

This is due to the personal data that could not be shared with others or unauthorized users which possibly may use the data for the criminal purposes and sabotages. For example, sensitive data of the well-known person such as Minister, Chairman, and other important person should be protected and secured

from unauthorized person because these kind of person may have a various competitor or enemy that have a bad intention towards them. Below is the flow of PII in healthcare sector which show on how the flow of PII are distributed and managed with who is responsible person involved in the used on PII.

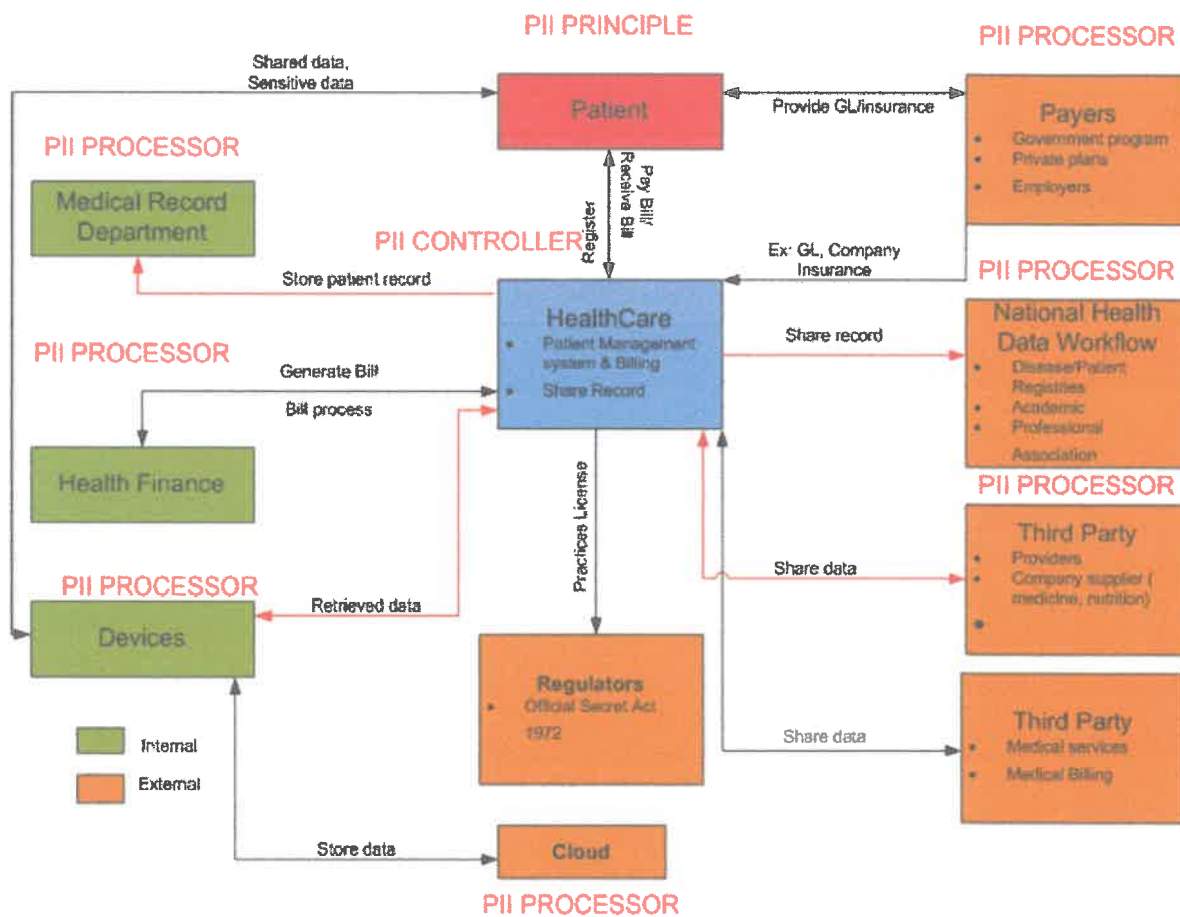


Figure 3. 31: Healthcare data framework, by showing the flow of PII.

Table 3. 3: Actors and Data type applied for Healthcare Sector.

PII Principle	Patient
PII Controller	Hospital/Clinic
PII Processor	Third Party/Agent/ National Health Data/ Devices/ Payer
Sensitive Data	<p>The flow of sensitive data can be seen on the arrow in red color which to represent sensitive data that deliver from one actor to another actor.</p> <ol style="list-style-type: none"> 1. Sensitive data that consist in healthcare sector is report of the health of the principles or known basically as patients. Sensitive data consist of data that represent the condition of the patient currently. 2. Sensitive data that are used, kept and stored by internal actor which as PII Processor : <ul style="list-style-type: none"> • Medical record department <p>Authority given by the PII controller to processes and store the data from getting access by unauthorized person. Medical record department stored and managed record efficiently. Besides that, medical record department also managed electronic medical record. Thus, ensuring that the records of data are complete, accurate and available to authorized personnel only.</p> <ul style="list-style-type: none"> • Devices <p>Nowadays with the advancement of the technology on healthcare sector, health data can be access using technology, so devices is one of the sources used. Devices store sensitive data through the data recorded.</p> 3. Sensitive data also can be shared with National Health Dataflow which for the overall statistic of the national healthcare report. Thus, for the purpose research and experience towards new diseases. 4. Other than that, PII processor also used PII data of the principles with the consent of the PII principles and PII controller for the purpose based on the processes applied. For example, through PII processor called as third party involved with healthcare company such as medicine supplier and provider. Use data PII for the purpose of research on improvement of the quality
PII	<ol style="list-style-type: none"> 1. PII are collected by the PII controller which is to identify and notify the PII principles existences. 2. Third party that supply medical services and medical billing are required PII of the patient which to provide service for payment, facilities, and equipment.

3.2.2.4.2. Banking Sector

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

1. Cash
2. Credit
3. Saving
4. Loan
5. 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 and 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.

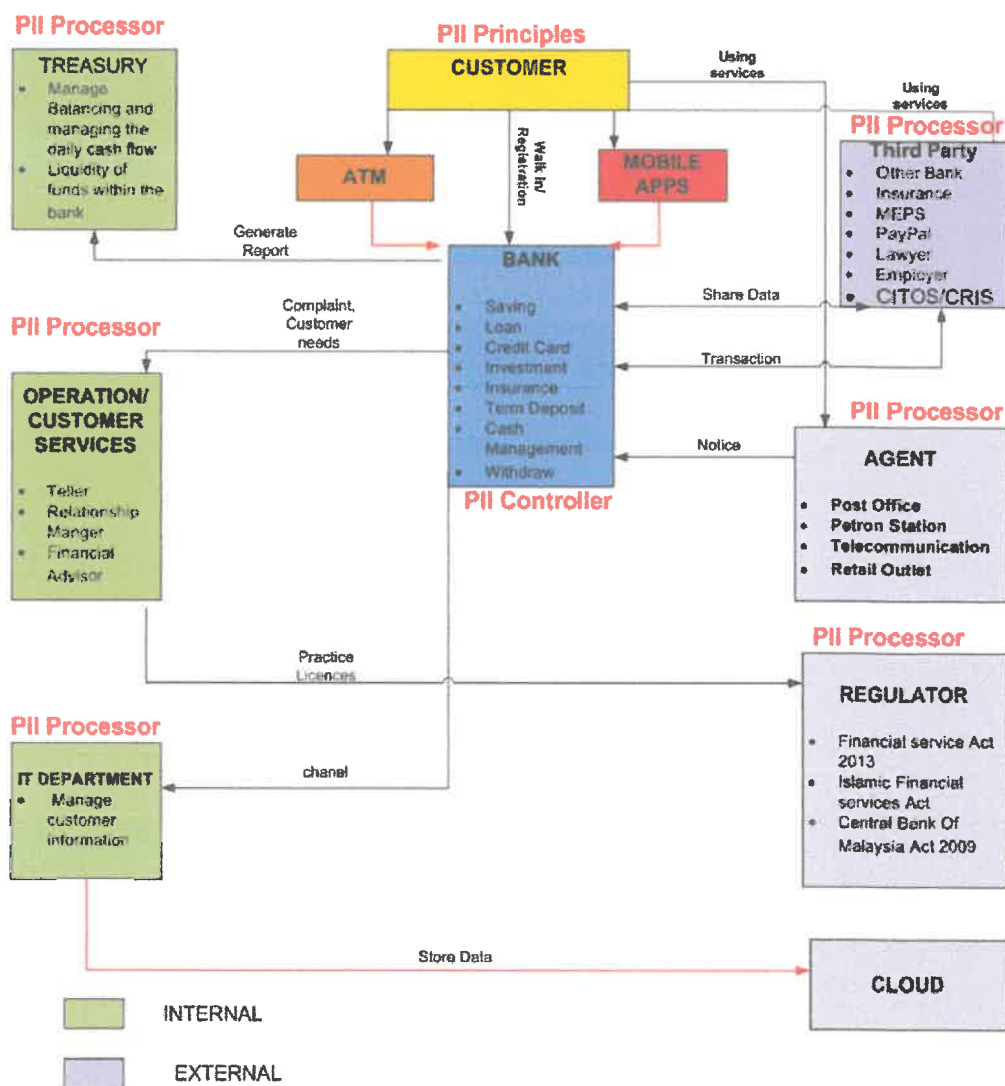


Figure 3. 32: Financial sector data framework, by showing the flow of PII.

Table 3. 4: Actors and Data type applied for Banking Sector.

PII Principle	Customer
PII Controller	Bank
PII Processor	Third Party/Agent/ Regulator/ Cloud/ It Department/ Operation/ Customer Services/ Treasury
Sensitive Data	<p>The flow of sensitive data is through the red line which to represent sensitive data used in banking sector.</p> <ol style="list-style-type: none"> 1. Sensitive data that used, shared and consist in banking sector is the data that related to any transaction such as : <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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	<p>PII Processor: External party that can access PII :</p> <ul style="list-style-type: none"> • 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. These is the services that agent may provide on behalf of Financial Institutions under the Guidelines [5] are as follows: <ol style="list-style-type: none"> ii. Facilitating withdrawal of funds by customers; iii. Facilitating fund transfers; iv. Receiving loan/financing payments; and v. Facilitating bill payments by customers.

3.2.2.5. Implementation Guidance

Privacy Guidelines: Auditor Checklist ISO/IEC DIS 27552 which extensions of ISO/IEC 27001 and ISO/IEC 27002 that focus on privacy and Personal Identifiable Information (PII). The purpose of this project which to assist auditor during auditing process in guiding them on planning, and implementing of the standard during the internal auditing that can ensure a consistent audit approach. Furthermore, which to assist the auditing process becoming more systematic and in a comprehensive manner which ensures that audit scopes are being followed and perform better during the auditing process. Other than that, which to assist in providing impartial opinions and assessments of company records, procedures and processes. Thus, with this auditor checklist the result could be in an adequate proper evidence and documentation.

Other than that, to help the auditor acknowledged the relationship between interested parties, third party, supplier and shareholder. This is because it is important to ensure that the checklist is implemented and adapted to the process of the organization, and that it is not a generic process. Furthermore, the question provided which to guide and help the auditor to ask during the reviewing records and interviewing personnel that involve towards the process. Other than that, auditor can use this checklist which to ensure that all the requirement are followed and fulfill. This is because the goal of auditing is to find evidence that the process is meeting its own requirements. Here is the mapping of the ISO/IEC 27552 standard clause allocated, which the extension of both 27001/27002 with privacy guidance.

Review documentation: INITIAL DOCUMENT REQUEST LIST

1. All policies, procedure documents, and organization charts
2. Key reports used to manage the effectiveness, efficiency, and process success
3. Access to key applications used in the process
4. Description and inventory of process master data, including all data fields and attributes

Figure 3. 33: The initial document request list for audit checklist

Table 3. 5: PIMS-specific requirements for ISO/IEC 27001

Location of PIMS-specific requirements and other information for implementing controls in ISO/IEC 27001:2013

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. 6: PIMS-specific requirements for ISO/IEC 27002

Clause number in ISO/IEC 27002:2013	Title	Clause number in this document	Remarks
5	Information security policies	5.2	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, development and maintenance	6.11	Additional guidance
15	Supplier relationships	6.12	Additional guidance
16	Information security incident management	6.13	Additional guidance
17	Information security aspects of business continuity management	6.14	No PIMS-specific guidance
18	Compliance	6.15	Additional guidance

3.2.3. Information Privacy Risk on Organization

3.2.3.1. Challenges

Nowadays, privacy issues through the usage of the internet becoming more threatening. There are various challenges and risk that need to be faced by the users such as identity theft, data breach and human error. As privacy risks exist wherever agencies collect, use, share and manage personal information relating to their employees, customers and clients and others. Opportunities will also exist to improve how agencies collect, use, share and manage personal information. Risk management takes into account both risks and opportunities, and is vital for the appropriate management of personal information.

3.2.3.1.1. Identity Theft

One of the popular challenges nowadays is identity theft. This will occur when someone used other identity for the purpose of sabotage, marketing purpose, scam and other related issues by using personal information. Personal information will be sold to third parties and other personal information will be captured and used for marketing or other purposes without permission. Besides, personal information can be collected through the scanning and stealing from the mail box, phone, dumpster diving (looking through garbage for document), involve into attacks database and phishing e-mails.

3.2.3.1.2. Data Breach

Data is growing faster from time to time every day. Data has grown exponentially over the last decade with poor security practice, organization will face risk of a data breach. Personal Identifiable Information (PII) is one of the biggest concerns in data privacy. Based on the Breach level index data records lost or stolen, the statistic of data breach since 2013 until now is 6,401,748. The numbers of statistic are increase every second. According to Verizon 2016 Data Breach Investigate Reports in 2015, there were 64,199 security incidents and 2,260 confirmed data breaches [3].

3.2.3.1.3. Human Error

According to [3] stated that human error is another serious incident that commonly occurred. There is a time when the employee sent the sensitive information to the wrong person. In some of the worst cases, the employee decides to hit the reply all button to an email with hundreds of people contain beneath the chain. Due to this serious carelessness, a lot of people may gain all access to view the sensitive and confidential information with such a small mistake and they do not even have to hack or log in to other people's account to foresee the information itself.

Next is a password weakness. Weak passwords are still the most common reason for data breaches, so organizations should pay very close attention to password security policies and password management. Although this may seem like a simple matter but it contributes to a very serious issues when it comes to data leakage. Even within this modern era, people are not considering to choose a secure password for their accounts instead they only embedded a simple kind of password chosen which can be easily assumed by the hackers.

This happened because they think that the password chosen does not give a huge impact to them and nothing will happen by just choosing a simple password for their account. So, the best practices in choosing a password are ensuring complex passwords composed of numeric, alphabetic (uppercase and lowercase) characters in addition to special symbols and similar characters, forcing users to change passwords regularly and requiring new passwords not previously used by the user.

3.2.3.2. Privacy Risk

Based on [6] which discussed about privacy risk and opportunity identification has stated examples of common privacy risks and responsible person who should be involved with privacy matters.

Table 3. 7: Privacy risk and opportunity identification, and responsible person involved

Examples of common privacy risks	Responsible person who should be involved
Staffs do not understand their responsibilities and the actions they need to take to mitigate privacy risks.	<ul style="list-style-type: none"> ➤ Risk team ➤ Managers of staff who deal with personal information ➤ Learning & Development ➤ Front-line staff (those dealing with customers) ➤ HR
Management does not fully understand where personal information is stored and processed.	<ul style="list-style-type: none"> ➤ Information management team ➤ Front-line/operational staff (those dealing with customers and processes/systems for management of personal information) ➤ Managers of staff who deal with personal information ➤ Information Technology ➤ Records Management
Privacy risks associated with changes to the organization, including process or system changes, are not adequately considered.	<ul style="list-style-type: none"> ➤ Risk team ➤ Project / programme office ➤ Information Technology ➤ HR, in respect of changes in people resources
Personal information is retained longer than is necessary for the business purpose.	<ul style="list-style-type: none"> ➤ Risk team ➤ Records management ➤ Information management
Employees and third parties are unaware of how they can appropriately collect, use, retain, share and dispose of personal information.	<ul style="list-style-type: none"> ➤ Risk team ➤ Records management ➤ Information management ➤ Procurement, ➤ Contract managers ➤ Internal audit ➤ HR
Personal information is disclosed to other parties, or used/processed for purposes to which the individual has not consented.	<ul style="list-style-type: none"> ➤ Risk team ➤ Front-line staff ➤ Managers of staff who deal with personal information

	<ul style="list-style-type: none"> ➤ Internal audit ➤ Legal team
Privacy-related enquiries are not responded to thoroughly, in an accurate and timely manner.	<ul style="list-style-type: none"> ➤ Risk team ➤ Front-line staff ➤ Managers of staff who deal with personal information ➤ Team/individuals who deal with privacy-related queries ➤ Legal team
Personal information is not adequately secured from accidental errors or loss, or from malicious acts such as hacking or deliberate theft, disclosure or loss.	<ul style="list-style-type: none"> ➤ Risk team ➤ Information technology ➤ Security team ➤ Project / programme management ➤ Front-line staff
The agency's personal information is handled inappropriately by third parties.	<ul style="list-style-type: none"> ➤ Risk team ➤ Third parties ➤ Procurement ➤ Contract managers ➤ Assurance, if assurance is undertaken over third parties' practices ➤ Contract "owners" ➤ Legal team
Privacy processes and controls do not operate as intended.	<ul style="list-style-type: none"> ➤ Risk team ➤ Internal audit ➤ Front-line staff ➤ Managers of staff who deal with personal information
Privacy-related incidents are not responded to appropriately.	<ul style="list-style-type: none"> ➤ Risk team ➤ Front-line staff ➤ Managers of staff who deal with personal information ➤ Security team ➤ HR, in respect of possible breaches of the code of conduct ➤ Legal team
The agency does not learn from patterns of privacy-related incidents.	<ul style="list-style-type: none"> ➤ Risk team ➤ Business improvement ➤ Managers of staff who deal with personal information ➤ HR ➤ Senior leadership

3.2.4.1. Implication of the development of Auditor Checklist

There are are positive implication for the development of auditor checklist for ISO/IEC DIS 27552. The primary impact by having this checklist which can assist the auditor in conducting the auditing process. The auditor can use this checklist which to know what is the possible question to ask during the auditing process. Other than that, the auditor can know what document that they refer which to ensure the evidences.

The impact towards the Cybersecurity Malaysia is the employees can improve their performance by implementation the requirement needed through the the existence of the checklist. Which is, to increase the level of vulnerabilities and credibility of CSM performances,

4. CHAPTER 4

4.1. Application Knowledge

4.1.1. Research Skill

The trainees required to perform many research during the internship. There are many techniques that the trainee can observed from the senior analyst on how to perform a right method and procedure. After that, the trainee is assigned on conducting research to develop framework which to use in report, then the trainee is really familiar with the research skill. Other than that, the trainee also performs research for cyber threat that could bring beneficial to the trainee.

Based on the subject that have been learn on research methodology in subject of Evaluation of Information Services could help me in fulfil the task given by the supervisor and team leader of my department. Which this subject, acknowledge students on how to conduct research more effectively and efficiency.

4.1.2. Auditor Checklist

The trainee is assigned to do checklist for auditor based on the ISO/IEC 27552 which is the extensions of ISO/IEC 27001 and 27002. So, the trainees need to study about the pattern of the auditor usually used. Thus, the trainees have to understand the concept and study on how the audit is actually conducted, because to provide the checklist it is must be rational with the technique apply by the auditor. So, the trainee is exposed with the auditor technique, concept and method used.

Based on the subject teach by Madam Salliza Md Razi regarding the subject of Legal and Ethical Aspects of Information System (IMS657), which subject give exposure to the student about the existing standard that very important during

working in the industry. Which, student are acknowledge about ISO/IEC 27001. Easier for the student to understand the standard and applied during working in the industry.

4.1.3. Comparative Analysis

Based on the research conducted, the trainee also exposed with the skill on comparative analysis because each of the research must be attached with the comparative analysis which to easier for trainee to discuss and present to the team leader and head of the department. Other than that, the trainee knows on how to categories the data based on the category. Comparative analysis help employee to summarize the outcome from multiple article.

Based on the subject of Management of Information System Department, which Madam Izzatil Husna Arshad gave a task regarding research on the career opportunities in Information System Management, and the result should in a comparative analysts, which to compare the result of the research in suitable criteria.

4.1.4. Privacy and Security Awareness

The trainee is exposed with the concept of the privacy and security of data of individual and organization. How the organization should handle data of the client, customer, vendor, supplier and also data own by the organization from being exposed and breach to unauthorized user. Thus, the trainee aware that leadership plays an importance role for information security being supported, both visibly and materially which is by senior management. Privacy and security is important because to assist in achieving organization business objectives and

processes. Thus organization conformity towards every requirement of information security which protect in term of Continuity, Integrity, Authority (CIA) of information in asset of organization such as people, technology and processes. Example of process is the activities perform such as email.

Legal and Ethical Aspect of Information System (IMS657) subject help the trainee in implementing a good performance in term of privacy and security, because the trainee is acknowledging about the issues and aware about the privacy and security concept which have been exposure during this subject.

4.1.5. Cyber Threat

Other than that, the trainee also helps other team which to find out about the cyber threat and issues on aviation sector. The trainee need to conduct a research on cyber threat and issues which to find out about the cases, challenges and also outcomes of the issues and challenges from the research paper. So, the trainee is exposing with the issues in aviation sector and knew the current issues and news on this sector.

With the exposure of Legal and Ethical Aspects of Information System (IMS657) subject assist the trainee during conducting research about cyber threat, which the trainee did not have to spent a lot of time in understanding about the concept of cyber and seeking for the possible threat. With the exposure from this subject that acquired student to find out about the cybercrime, computer crime and personal data, help the trainee to familiar and aware before joining the industry. Which the trainee is aware about the current issues and threat regarding the cyber and technology.

4.2. Personal Thought and Opinion

For the personal thoughts and opinion, this well-established company provides great opportunities towards intern, which they help and assist the trainees on how to completing the task. This company really impressed the trainees which they concern on the learning period and time given to acknowledge and expert on certain topic given by them. After that, in my opinion that this company can be the best platform for the trainees to build experiences, new skill and the development of the trainee' career, because the trainee can learn a lot from here by socialize with all employee of the company even from a different department, division and unit. Other than that, this company foster good relationship within and between department and build a good relation with colleagues, and in my opinion it is a good etiquette implemented by this company to be and show as good example for the trainee and outsider of the company. Thus, with this positive behavioral produce a good performance and outcome for the company to become more successful and well known.

4.3. Lesson Learnt

There are many lessons that could be learnt in this company which they treat the trainees as permanent employee so that we could learn any skills and way of producing and processing the services. Other than that, the important lesson that the trainee could learnt is teamwork. In our department all of the employees doing their task with a strong and passionate teamwork that positively produce a good result and effectively.

Even, they are from different team but they can help each other on giving idea, opinion that could contribute to the work task. Furthermore, the lesson that the trainee could learn is to do your work sincere and solve the problem but not avoid the problem, so the result can be more effective and even the task can be completed on time.

Other than that, the relationship between employees in this company is so close which even from different department and division. So, there are many experience can be shared together between different background, department and division. On the other hand, through this internship, the trainee can learn on how to work multi task, which not focusing one job only.

Through this attitude, the employees and the trainee itself could receive and share many experiences that could enhance their skill, and qualification. And exposed and developed with latest trend and current issues. In term of technique and knowledge, that the trainee can have a lesson about the importance of the securing privacy from breach to irresponsible person.

The information privacy not even must be kept safe by the owner but also to whom the data are given with consent. The trainee can implement this lesson during work and the trainee can share and arise awareness to future employer and colleague about the importance of information privacy. This is because, privacy is usually being not take seriously.

4.4. Limitation and Recommendation

During my internship, there is no limitation while training here, but there is few can consider one as limitation which as a trainee we could not use their wireless network connection because there is a policy allocated stated that only permanent employee is allowed in accessing the wireless network connection, this is because to avoid unnecessary harm, action happened that can cause a negative impact to the company daily process and routines. For example, to avoid infected of virus, and other parasite that may harm the company reputation and breach of data.

As concern, this company is cyber security company that align with the standard, policy, procedure and guideline which to control their brand, and reputation to be as a strong and trusted company. Then, this is one of the implementation guidance that this company complies. The control is become a limitation to the trainees because it hard for the trainees to do work if working outside from the working station. However, the company provides the trainees with cable network which only can be use in working station. If the trainees have any invitation to the meeting outside of the working station, then the trainees cannot connect to the network and searching for the information.

Not enough staff in ISMA department. There are only few of the staff allocated for this department which contributed to three units. Few staff are needed which to help the department complete the task, this is because this department play an important role, for the organization by handling whole internal ISMS, and Business Continuity.

5. REFERENCES

- Agent. (2012). Retrieved from http://www.bnm.gov.my/files/publication/fsps/en/2012/cp02_002_box.pdf
- Arlington healthcare. (2014). Retrieved from <https://www.arlingtonhealthcaregroup.com/healthcare-ecosystem/>
- Banking Department. (2019). Retrieved from <https://www.investopedia.com/terms/b/banking-department.asp>
- B. Martínez-Pérez, I. de la Torre-Díez, and M. López-Coronado. (2015). "Privacy and Security in Mobile Health Apps: A Review and Recommendations". *J. Med. Syst.*, vol. 39, no. 1
- "BNM/RH/GL 008-16 Development Finance and Enterprise Department Guidelines on Agent Banking."
- Department. (2015). Retrieved from <https://www.quora.com/What-are-the-various-departments-of-a-bank-and-what-are-their-functions>
- H. Koivula-Tynnilä, A. Axelin, and H. Leino-Kilpi.(2018)."Informational Privacy in the Recovery Room—Patients' Perspective." *J. Perianesthesia Nurs.*, vol. 33, no. 4, pp. 479–489
- L. Alkire, J. Pohlmann, and W. Barnett. (2019)."Triggers and motivators of privacy protection behavior on Facebook". *J. Serv. Mark.*, p. JSM-10-2018-0287
- National eHealth, Ministry of Health Malaysia
- New Zealand Government. "Privacy Risk and Opportunity Identification." *Guid. Priv. Manag.*, pp. 1–15
- Pekeliling Ketua Pengarah Kesihatan Bil 17/2010
- Privacy Statement. (2019). Retrieved from http://www.bnm.gov.my/index.php?ch=en_misc&pg=en_misc_privacy&ac=273
- Privacy Statement. (2019). Retrieved from <http://www.bankislam.com.my/en/Documents/PrivacyStatement-PDPA-en.pdf>
- Responsibilities. (2016). Retrieved from <http://www.myhealth.gov.my/en/confidentiality-of-medical-records-information-whos-responsibility/>
- Third Party. (2016). Retrieved from <https://www.finextra.com/blogposting/13407/banking-data-for-third-parties>
- Third party. (2019). Retrieved from <http://www.xchanging.com/industries/healthcare>
- V. Moustaka, Et al. (2019). "Enhancing social networking in smart cities: Privacy and security borderline." *Technol. Forecast. Soc. Change*, vol. 142, no. September, pp. 285–300

Timeline (Schedule)

Job Scope

No.	Komponen	Rujukan
1	<p>Pemahaman Privasi</p> <ul style="list-style-type: none"> a) Tadbir Urus Privasi b) Dasar dan Procedur Privasi c) Pengurusan Privasi <ul style="list-style-type: none"> i) Perancangan ii) Penasihat iii) Pemantauan dan Melaporkan iv) Audit dan Ulas d) Operasi Privasi <ul style="list-style-type: none"> i) Pengurusan persetujuan ii) Hak sokongan privasi pelanggan iii) Ulasan iv) Pengurusan pencerobohan 	<ul style="list-style-type: none"> i. ISO/IEC 29100: Privacy framework ii. APEC Privacy Framework 2005 iii. The Software Alliance BSA Privacy Framework iv. The OECD Privacy Framework 2013 v. Privacy Governance Framework 2016 (Information and Privacy Commission, New South Wales) vi. ISO/IEC TS 19608:2018 - Guidance for developing security and privacy functional requirements based on ISO/IEC 15408 vii. Privacy Management Reference Framework
2	<p>Mengasaskan perancangan data terbuka</p> <ul style="list-style-type: none"> a) Penerbitan maklumat: "<i>Open by default</i>" / "<i>Open by design</i>" b) Had data terbuka c) Kategori data terbuka 	<ul style="list-style-type: none"> i. ISO/IEC 27001:2013 ii. Akta Perlindungan Data Peribadi 2010 (Akta 709) iii. Akta Perlindungan Pengguna 1999 (Akta 599) iv. Guidelines on The Implementation of the Public Sector Open Data Initiative by MAMPU (2015)

No.	Komponen	Rujukan
3	<p>Penyediaan dan pelaksanaan teknikal</p> <p>Melakukan penaksiran risiko terhadap privasi data terbuka</p> <ul style="list-style-type: none"> i) Menilai kandungan maklumat data terbuka ii) Menilai kelebihan data terbuka iii) Menilai risiko data terbuka iv) Imbang duga kelebihan dan risiko data terbuka v) Menilai keseluruhan impak data terbuka 	<ul style="list-style-type: none"> i. ISO/IEC 29134:2017 - Security techniques - Guidelines for privacy impact assessment ii. ISO/IEC 27005: Information security risk management iii. City of Seattle Open Data Risk Assessment (2018)
	<p>Panduan terhadap Perlindungan Privasi Keterbukaan Data</p>	<ul style="list-style-type: none"> i. ISO/IEC 27002: Code of practice for information security controls; ii. ITU-T X.1058 ISO/IEC 29151: Code of practice for personally identifiable information protection
4	<p>Penglibatan privasi di dalam teknologi terkini</p>	<p>a) Internet of Things (IoT)</p> <ul style="list-style-type: none"> i. IoT Security & Privacy Trust Framework v2.5 2017 ii. Internet of Things Security Guideline V1.2 by IoT Alliance Australia (IoTAA) iii. Internet of Things (IoT) Cybersecurity Improvement Act of 2017 iv. Internet of Things Consumer Tips to Improve Personal Security Act of 2017 ("IOT Consumer TIPS Act of 2017") v. State of Modern Application, Research, and Trends of IoT Act ("SMART IoT Act"). <p>b) Cloud</p>

No.	Komponen	Rujukan
		<ul style="list-style-type: none"> i. ISO/IEC FDIS 27017:2015 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services ii. ISO/IEC 27018:2019 - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors <p>c) Smart City</p> <ul style="list-style-type: none"> i. State of Modern Application, Research, and Trends of IoT Act ("SMART IoT Act"). ii. Kertas kajian oleh ahli akademik <p>d) Blockchain and IR 4.0</p> <p>Kertas kajian oleh ahli akademik</p>

Presentation Slide



CyberSecurity MALAYSIA

CYBERSECURITY MALAYSIA (SELANGOR)
LEVI 7, TOWER 1, MEDARA CYBER AXIS, JALAN IMPACT,
69000 CYBERJAYA, SELANGOR

INDUSTRIAL TRAINING
FEBRUARY – JUNE 2019
BY: NABILAH ADIPAR BELLI KAZALI
201631751

Table of contents

Are you ready to explore this organization?

Did you aware about the existences of this company?

Did you know what is cyber security?

1. ORGANIZATION
2. DEPARTMENT
3. TRAINING ACTIVITIES
4. SPECIAL PROJECT
5. CONCLUSION

1. INTRODUCTION

Background



CHAPTER 1:

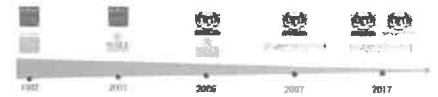
HISTORY

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 the same time strengthen Malaysia self-reliance in cyberspace.

National ICT Security & Emergency Response Centre (NISERC) was created in 2001 as a department in MIMOS Berhad, and the Malaysia Computer Emergency Response Team (MyCERT) was placed under NISERC. On 28 September 2005, the Cabinet decided for NISERC to be spun-off from MIMOS Berhad as a separate entity under MOSTI.

MYCERT

Cybersecurity Malaysia journey started with the creation of the Malaysia Computer Emergency Response Team or MyCERT on the 15th of January 1997 as a unit under MIMOS Berhad. On the 24th of January 1999, the National Information Technology Council or NITC proposed for the establishment of an agency to address emerging ICT security issues in Malaysia.



- MyCERT & Cyber999
- Digital Forensics (CyberICS)
- Malaysian Security Evaluation Facility (MySEF)
- Malaysian Vulnerability Assessment Centre (MyVAC)
- Information Security Certification Body
- Security Management & Audit Practice
- Industry Development
- Government & International Engagement
- Research
- Cyber Security Professional Development
- Outreach

ISMA

INFORMATION SECURITY
MANAGEMENT ASSURANCE
ALSO KNOWN AS SECURITY
MANAGEMENT BEST
PRACTICE (SMBP)



FUNCTION OF ISMA DEPT

The primary role of Security Management & Best Practices (SM&BP) department is to drive information security management based on ISO/IEC 27001:2005 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 program, information security management review, development of information security policies and procedures and Business Continuity Management.



TRAINING ACTIVITIES

RESEARCH - FRAMEWORK - COMPARATIVE ANALYSIS - MOVING TO NEW BUILDING - KNOWLEDGE SHARING - GATHERING - RESEARCH PAPER

7

CONDUCT RESEARCH



Industry 4.0 vs I4.0

Industrial Revolution 4th is a total transformation of all industrial sectors from primary, secondary, tertiary, and Quaternary sector. While Industry 4.0 is adoption from the secondary sector and focus on the smart manufacturing.

Artificial Intelligence

AI is a concept that is made up of numerous subfields such as machine learning, which focuses on the development of programs that can teach themselves to learn, understand, reason, plan, and act when exposed to new data in the right quantities.

Standard

- 1. Review, acknowledge and used
- ISO/IEC 27001 -ISO/IEC 27002
- ISO/IEC DIS 27552 -ISO/IEC 28100

Cloud Computing

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage.

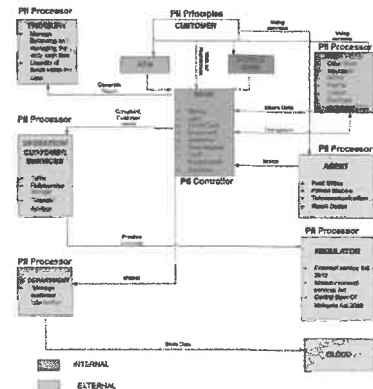
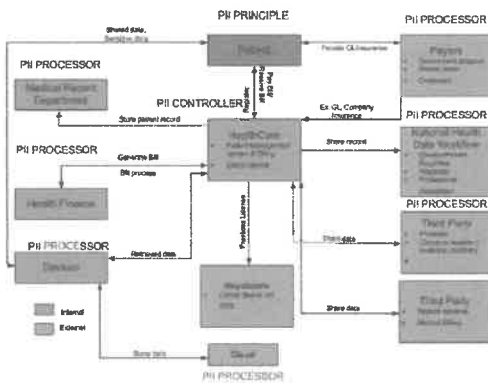
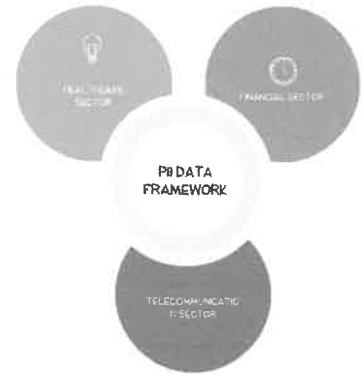
SMART CITY

Smart City is the technology which implemented towards the needs of the city. Smart City nowadays be applied to the facilities in the city such as Traffic Light, and Streetlight that already applied at the Malaysia.

Information Privacy & Security

Information privacy is currently regarded as an element of information security processes, the actual coverage of information privacy in technical security standards of all layers will be now explored.

DEVELOPED FRAMEWORK



April 17, 2019

Moving to new building at Cyberjaya

Moving to new building from Seri Kembangan to Cyberjaya



Appraisal

The trainee is required to appraise the record based on the date of the publication by referring to the ISMS driver which known as Ma Hana. She is in charge for the moving out for our department.



Disposal

The trainee helps the ISMS driver in destructing the record by using the shredding machines. Before shredding the record, the record must be put into the green container before shredding the records.



Transferring Record

The trainee also helped in transferring the records from the server to the boxes given by the third party that supplying the boxes, wrapping and deliver the boxes to new building.



Labelling

The trainee also in charge in labelling the boxes which is to easier for the S&MJJ Holding in sorting the boxes for each of the department because to avoid from mixup of the boxes.



Open new file

Open new new file, for the department record regarding ISMS report. Together with labelling, and classify.



Data Converting

Help ISMS team in transferring the result of a questionnaire into excel sheet.

Knowledge Sharing

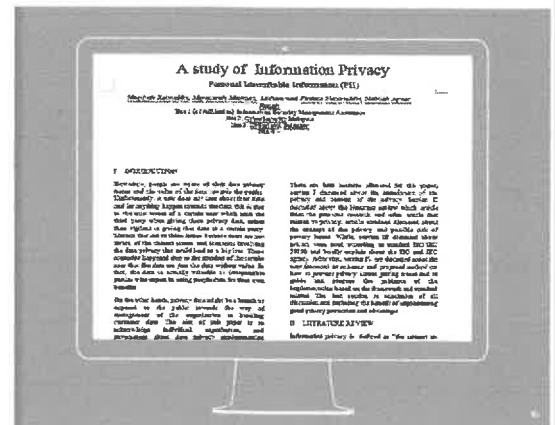
Every Wednesday knowledge Management @ Library of the CSM conducting knowledge sharing session which everyone from the company can share anything and any topic to other. Sometimes, Knowledge Management may invite sharer from outside such as writer, reporter.

The trainee shared the experiences about travelling to Korea, share on life and trick during in Korea. The trainee will come to Knowledge Management @ Library every Wednesday.



Develop Research Paper

The trainee are required which to develop a research paper regarding Information Privacy



GATHERING & PROGRAM

POTLUCK



HARI RAYA FEAST

With Kementerian Komunikasi & Multimedia And tet Merjans Cyberjaya on last day



CHARITY

With Ciphanje Home around Selangor



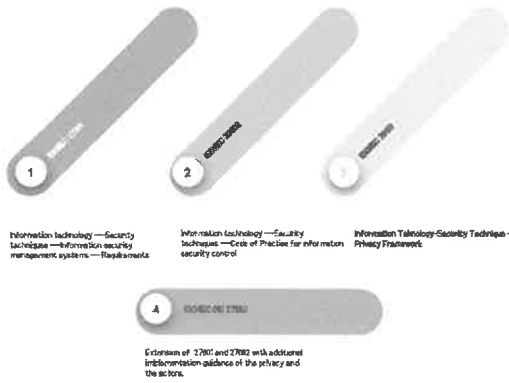
SPECIAL PROJECT



Auditor Checklist Implementation Guidance for ISO/IEC DIS 27552 EXTENSION OF ISO/IEC 27001/27002

There is no checklist made for this standard, which will be implement start with internal of the CSM.

STANDARD USED



AUDITOR CHECKLIST

Auditor checklist for ISO/IEC DIS 27552, which is the extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.

Review documentation: INITIAL DOCUMENT REQUEST LIST

1. All policies, procedure documents, and organization charts
2. Key reports used to manage the effectiveness, efficiency, and process success
3. Access to key applications used in the process
4. Description and inventory of process master data, including all data fields and attributes

AUDITOR CHECKLIST IMPLEMENTATION GUIDANCE: Help and assist auditor on what document are needed by on each of the clause and sub-clause. There are five clause which consist many sub-clause and with the additional implementation guidance.

ISO/IEC 27001: 2013

Application of ISO/IEC 27001:2013 requirements
Location of PIMS specific requirements and other information for implementing controls in ISO/IEC 27001:2013

Clause number in ISO/IEC 27001:2013	Title	Sub-clause number in the document	Remarks
5.1	Context of the organization	5.1	Additional requirements
5.2	Leadership	5.2	ISO/IEC specific requirements
5.3	Planning	5.3	Additional requirements
5.4	Support	5.4	ISO/IEC specific requirements
5.5	Operation	5.5	ISO/IEC specific requirements
5.6	Performance evaluation	5.6	ISO/IEC specific requirements
5.7	Improvement	5.7	ISO/IEC specific requirements

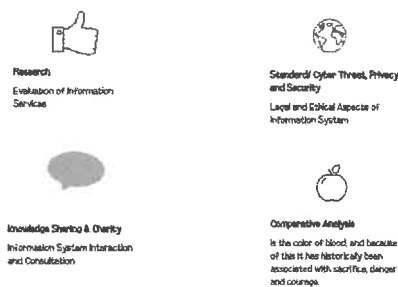
Clause

The list of the clause allocated for ISO/IEC DIS 27552, under ISO/IEC 27002

Scope number in clause, 27001:2013	Title	Clause number in the document	Remarks
4.1	Information security policy	4.1	Additional guidance
4.2	Information security objectives and processes	4.2	Additional guidance
4.3	Information security risk assessment	4.3	Additional guidance
4.4	Information security risk treatment	4.4	Additional guidance
4.5	Information security incident response	4.5	Additional guidance
4.6	Information security business continuity management	4.6	Additional guidance
4.7	Information security compliance	4.7	Additional guidance
4.8	Information security awareness	4.8	Additional guidance
4.9	Information security competence, training and awareness	4.9	Additional guidance
4.10	Information security communication	4.10	Additional guidance
4.11	Information security documentation	4.11	Additional guidance
4.12	Information security records	4.12	Additional guidance
4.13	Information security monitoring, measurement, analysis and evaluation	4.13	Additional guidance
4.14	Information security internal audits	4.14	Additional guidance
4.15	Information security management review	4.15	Additional guidance

CHAPTER 4: CONCLUSION

Application Knowledge



CHAPTER 4: CONCLUSION

Personal Thought: GOOD PLATFORM, GOOD RELATIONSHIP, POSITIVE BEHAVIOR, NO DISCRIMINATION

BUILD CONFIDENT, TIME MANAGEMENT, ALWAYS SHARING KNOWLEDGE, NEW CURRENT ISSUES, UPDATED NEW

Limitation and Recommendation

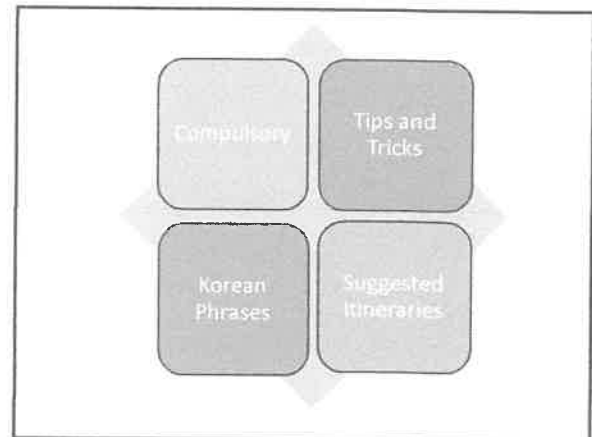
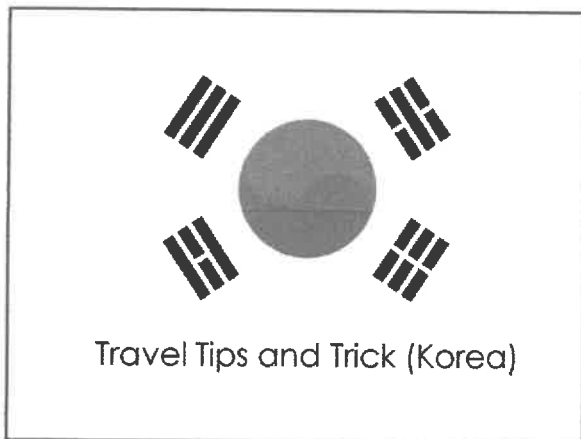
NOT ENOUGH STAFF
NOT ENOUGH TIME
LIMITED ONLINE DATABASE
INTERNET CONNECTION

Lesson Learnt



THANK YOU

Activities



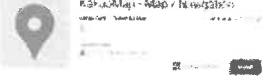

Compulsory

Register:
<https://www.visitkorea.com.my/malaysian-travel-story/>

- T-money Card = { 5 days = 20,000 won}
- Discount Coupon

Download Kakao Map App:

- Subway line and details (time, Location)






Bring lip balm, moisturizer, empty bottle

Tips and Tricks

- Roll don't fold
- Cover your footwear with shoe bags or shower caps
- Pack the heaviest items closest to the wheels
- Put your toiletries in a transparent bag
- Put loose wires in a sunglasses case
- Put breakables in socks
- Capitalize on empty space
- Avoid heels, and wear sport shoes or sneakers

- Bring medicine description
- Fold a shirt and put it in the inside of a hat to keep your hat from getting squished.

Korean Phrases

- Nak tanya *how much* – Ahjussi / ahjumma, **olmayeyo**
- Kalau nak minta diskaun – Ahjussi/ahjumma, **kaka juseyo**
- Jika mereka tak bagi diskaun, puji sikit cakap dia handsome / cantik. Contoh – Ahjussi, **neomu motjida?** Ahjumma, **neomu yeppoyo?**

Suggested Itineraries

- **Prayer**
 - Everland , Itaewon, Nami Island
- **Food**
 - Itaewon (Muslim community)
 - » Makan Restaurant
 - » Eid (Malaysia Branch, Bangi)
 - » Many more, include Turkish restaurant
 - Seoul
 - » Yang Good BBQ (yeoksam)
 - » Kampung
 - Nami Island
 - » Dongmun(Asian Cuisine)



- **Transport**
 - Train, Bus, Taxi
 - Train AREX, and ALL Stop Train (from Incheon Airport to Seoul)
 - Korail , ITX train (Nami Island)
 - T-Money (at least 10,000 won)
- **Location**
 - Nami Island
 - Namsan Tower
 - Gangnam(Entertainment)
 - Everland (Theme Park)
 - Myeondong, Dongdaemun, Ewha Women University, Hongdae
 - Gyeongbokgung Palace, Blue House(PM)



Staff Assembly

From: NORLELA BINTI MOHAMED YUNAN <norlela@cybersecurity.my>

Sent: Tuesday, 26 February, 2019 2:42 PM

To: CyberSecurity Malaysia Staff <staff@cybersecurity.my>

Cc: Human Capital Development <hcd@cybersecurity.my>

Subject: HCD ANNOUNCEMENT : STAFF ASSEMBLY @ 5 MARCH 2019

Assalamualaikum wbt & Salam Sejahtera

Kindly be informed that we will be having Staff Assembly, as follows:

Date

5 March 2019 (Tuesday)

Time

10.15 a.m. – 12.00 noon

Venue

Dewan Musytari, RHR Hotel@UNITEN, Kampus Putrajaya, Universiti Tenaga Nasional, KM7, Jalan Ikram – UNITEN, Kajang, Selangor.

Agenda

10.15 a.m. : Staff Arrival and Registration

10.30 a.m. : Welcome Note by Emcee

10.35 a.m. : Singing of "NegaraKu"

Doa Recital

10.40 a.m. : Updates by Chief Executive Officer

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

11.30 a.m. : Reward & Recognition

11.50 a.m. : Introduction of New Hires in 2018 & 2019

12.00 noon : End of Assembly & Refreshment

Attendance is compulsory.

Thank you & Best Regards,

Human Capital Development Department

