

**FINAL REPORT**  
**ON**  
**PROJECT ON CAPACITY BUILDING**  
**FOR CYBER SECURITY IN VIETNAM**  
**(CYBER SECURITY TECHNOLOGY /**  
**MARKETING / AWARENESS RAISING)**

**FEBRUARY 2022**

**JAPAN INTERNATIONAL COOPERATION AGENCY (JICA)**  
**JAPAN DEVELOPMENT SERVICE CO., LTD. (JDS)**

<b>GP</b>
<b>JR</b>
<b>22-016</b>

# CONTENTS

1.	Executive Summary .....	1
2.	Contents of Implemented Activities.....	1
2.1	Overall Workflow and Schedule of Activities.....	1
2.2	Content of Implemented Activities .....	3
3.	Special Efforts and Lessons Learned in the Survey Implementation.....	12
4.	Special Efforts and Lessons Learned in the Training Implementation .....	13
4.1	Special Efforts and Lessons Learned in the Awareness Raising Training.....	13
4.2	Special Efforts and Lessons Learned in the Cyber Exercise Training .....	13
5.	Capacity Change of Counterpart Institution.....	14
6.	Recommendations to Awareness Raising Activities in the Project .....	15
6.1	Recommendations to Awareness Raising Activities in the Project .....	15
6.2	Recommendations in Cyber Exercise Training .....	16
	Appendix A: Result of Post-event Survey for Cyber Exercise Training.....	17

## LIST OF FIGURES AND TABLES

### (Figures)

Figure-1	Overall Flowchart of this Work.....	1
Figure-2	Actual Schedule of the Implemented Activities .....	2
Figure-3	System Diagram for Cyber Exercise Environment.....	10

### (Tables)

Table-1	Meeting on Explanation of Work Plan and Interview to AIS.....	3
Table-2	Surveyed Information on Awareness Raising Activities in Japan.....	4
Table-3	Schedule of the Implemented Awareness Raising Training.....	6
Table-4	Online Discussion with AIS on Recommendations and Additional Activities .....	7
Table-5	Regular Meeting with AIS on Awareness Raising Activities #1.....	8
Table-6	Regular Meeting with AIS on Awareness Raising Activities #2.....	8
Table-7	Regular Meeting with AIS on Awareness Raising Activities #3.....	8
Table-8	Regular Meeting with AIS on Awareness Raising Activities#4.....	9
Table-9	Cyber exercise training materials .....	10

## TABLE OF ABBREVIATED WORDS

Abbreviation	Definition	Japanese
AIS	Authority of Information Security	情報セキュリティ局
CERO	Computer Entertainment Rating Organization	コンピュータエンターテインメントレーティング機構
COP	Child Online Protection	児童のオンライン保護
CSIRT	Computer Security Incident Response Team	シーサート
CSH	Cybersecurity Strategy Headquarters	サーバーセキュリティ戦略本部
GSOC	Government Security Operation Coordination team	政府関係機関情報セキュリティ横断監視・即応調整チーム
IPA	Information-technology Promotion Agency, Japan	情報処理推進機構
ITU	International Telecommunication Union	国際電気通信連合
JFY	Japanese Fiscal Year	年度
JASA	Japan Information Security Audit Association	日本セキュリティ監査協会
JCIC	Japan Cybersecurity Innovation Committee	日本サイバーセキュリティ・イノベーション委員会
JNSA	Japan Network Security Association	日本ネットワークセキュリティ協会
KGI	Key Goal Indicator	重要目標達成指標
KPI	Key Performance Indicator	重要業績評価指標
METI	Ministry of Economy, Trade and Industry	経済産業省
MEXT	Ministry of Education, Culture, Sports, Science and Technology	文部科学省
MIC	Ministry of Information and Communication	情報通信省（ベトナム）
MIC	Ministry of Internal Affairs and Communications	総務省（日本）
MOJ	Ministry of Justice	法務省
NISC	National Center of Incident Readiness and Strategy for Cybersecurity	内閣サイバーセキュリティセンター
NPA	National Police Agency	警察庁
PTA	Parent-Teacher Association	PTA
Public-Private Board	Public-private joint committee for opinion aggregation on unauthorized access prevention measures	不正アクセス防止対策に関する官民意見集約委員会（官民ボード）
SME	Small to Medium sized Enterprises	中小企業
STP	Segmentation, Targeting, Positioning	
VPN	Virtual Private Network	仮想プライベートネットワーク

## 1. Executive Summary

In this work, awareness raising activities on cybersecurity in Japan as well as necessary marketing methods for promoting the activities were thoroughly researched. The results of this research were summarized into the report of survey results and converted into training materials for the training implemented for the counterpart (C/P) organization (AIS: Authority of Information Security) staffs. Based on the results of the training, the expert team implemented the follow-up for additional survey as well as the recommendation to awareness raising materials created by AIS. Training on cyber exercises was also implemented as an addition to the follow-up activities. All these activities are described in Chapter 2. special efforts in and lessons learned from the survey and the training are presented in Chapter 3 and 4. the capacity change of AIS as a result of this work is summarized in Chapter 5, and recommendations to awareness raising activities in the Project are presented in Chapter 6.

## 2. Contents of Implemented Activities

### 2.1 Overall Workflow and Schedule of Activities

The figure on the next page shows the overall flow chart of implemented activities. The initial plan was to visit the Project site in Vietnam to conduct the activities listed on the right side in the figure. But due to COVID-19, all planned on-site activities had to be replaced with online activities connecting the Project site with the awareness raising experts in Japan.

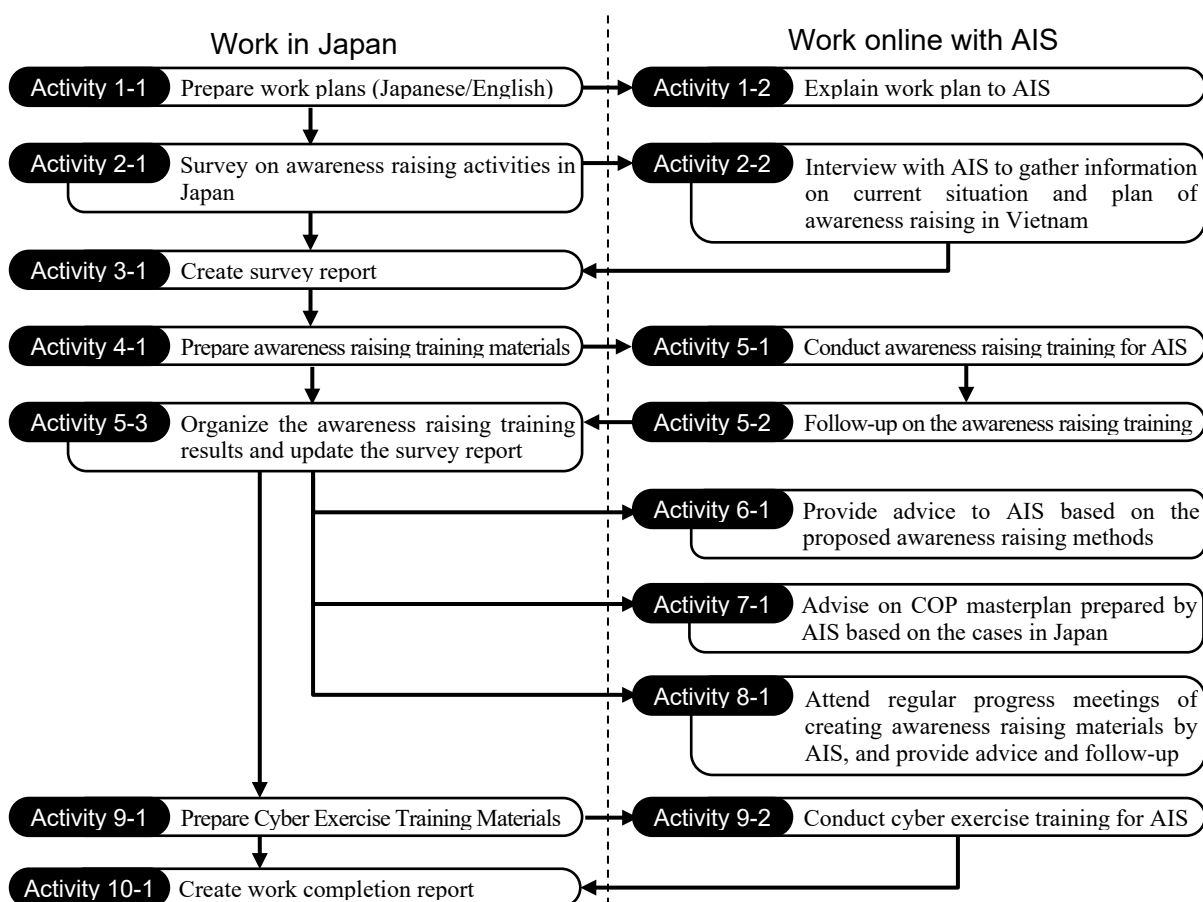


Figure-1 Overall Flowchart of this Work

The actual schedule that has been implemented is shown in Figure-2.

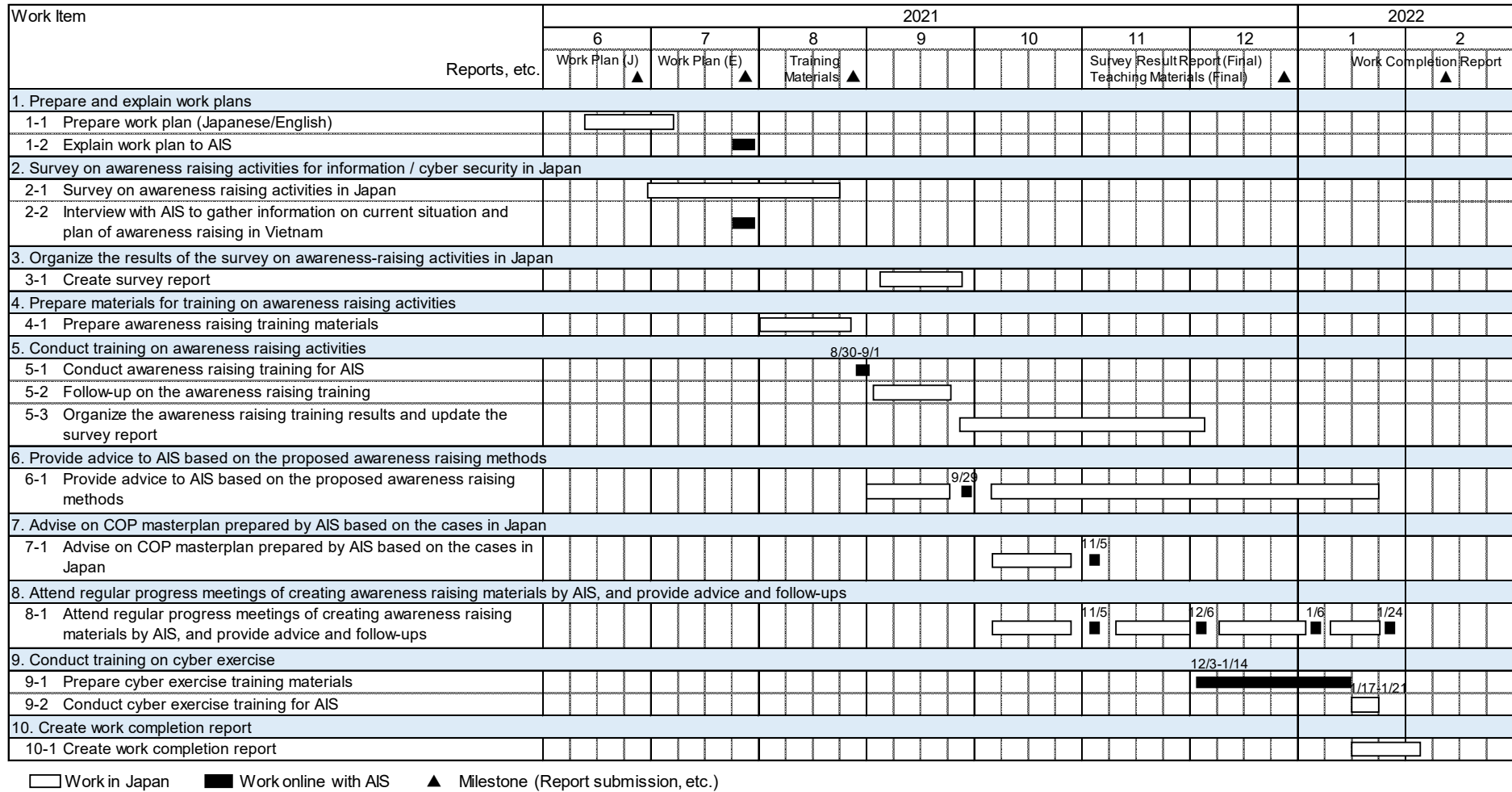


Figure-2 Actual Schedule of the Implemented Activities

## 2.2 Content of Implemented Activities

The content of each implemented activity is described in the following sections.

### Activity 1-1 Prepare work plans (Japanese/English)

We obtained information on the Project from JICA headquarters, chief advisor, short term experts, and a long-term expert to understand the past efforts of the Vietnamese government on cyber security and the overall activities of the Project, and then prepared the work plans in Japanese and English. The Japanese version was presented and explained to JICA for approval.

### Activity 1-2 Explain work plan to AIS

### Activity 2-2 Interview with AIS to gather information on current situation and plan of awareness raising in Vietnam

The explanation of the work plan and the interview to AIS were both carried out on the same online meeting on July 30<sup>th</sup>, 2021.

Table-1 Meeting on Explanation of Work Plan and Interview to AIS

Date & Time	July 30 <sup>th</sup> , 2021 9:00-11:00 (Vietnam time)
Participants	AIS: 7 including Deputy Director General JICA: 3 including 1 awareness raising expert
Main Points	<ul style="list-style-type: none"> <li>• Work plan was explained and AIS side agreed with the content of plan</li> <li>• AIS side explained about the current status of master plan 2020-2025 that includes awareness activities scheme.</li> <li>• The strategy in the master plan has 3 focuses:             <ol style="list-style-type: none"> <li>1. Mass media channel where AIS believe most of the youth are landing as targets.</li> <li>2. Fostering the domestic products and services serving the creative cyberspace for children</li> <li>3. Developing educational materials and implementing such contents into the school system</li> </ol> </li> <li>• Facebook Messenger, Viber, Instagram, Zalo are popular instant message apps in Vietnam. YouTube is still popular besides the social media, especially for children, but they cannot judge whether the content is good or bad without support from parents.</li> <li>• IT subjects are integrated in the current educational curriculum but the influence of massive information from SNS is overwhelming. From the scheme of Child Online Protection (COP)<sup>1</sup>, the target of communication should not only be children, but also their parents. Hotline is needed for children because they may prefer not to directly talk to their parents.</li> <li>• Vietnam is trying to establish the COP network including the schools as a top-down method from the government. This network is not only for the school system, but also for the parent, children themselves and front-line staffs (social services employees).</li> <li>• There is very limited cooperation between Government and private sectors in Vietnam. However, the scheme is also trying to foster domestic products and services for children.</li> <li>• The current master plan approved by the Prime Minister last year calls on the 64 provincial governments to take responsibility on awareness raising promotion in their provinces. Inside MIC, they have also got the monitoring plan to follow up the strategy.</li> <li>• As for the content of planned training, the proposed plan is fine. AIS would like to know the "know-how" of applying the Japanese policy in daily operation of awareness raising. For the education materials, it seems that animations may be effective, for example. It would be helpful if there is some content about prevention of child abuse.</li> </ul>

<sup>1</sup> COP has been first raised as a big issue at ITU (<https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx>)

## Activity 2-1 Survey on awareness raising activities in Japan

The following information on awareness raising activities in Japan was surveyed in order to develop training materials. Contents of these information sources are summarized in the survey report.

Table-2 Surveyed Information on Awareness Raising Activities in Japan

Survey Items	Main sources of information
Policies and Guidelines in Japan on Awareness Raising Activities	<ul style="list-style-type: none"> <li>• The Basic Act of Cybersecurity (revised in 2014, R1)</li> <li>• Cyber Security Strategy (Cabinet decision: target years 2021-2024)</li> <li>• International Strategy on Cybersecurity Cooperation (NISC: 2013)</li> <li>• Common guidelines for government agencies (NISC: 2018)</li> <li>• Cybersecurity 2021 (NISC Annual Report)</li> </ul>
Organizations and Bodies related to Cybersecurity in Japan	<ul style="list-style-type: none"> <li>• Cybersecurity Strategy Headquarters</li> <li>• NISC (National Center of Incident Readiness and Strategy for Cybersecurity)</li> <li>• IPA (Information-technology Promotion Agency)</li> <li>• NPA (National Police Agency)</li> <li>• “Kan-min Board” (Public-Private Board)</li> <li>• GSOC (Government Security Operation Coordination team)</li> </ul>
National budget	<ul style="list-style-type: none"> <li>• National Budget on Cybersecurity in Japan</li> </ul>
Policy, Guideline and Practice regarding Cybersecurity Education in Japan	<ul style="list-style-type: none"> <li>• Cybersecurity Human Resource Development Program (NISC: 2017)</li> <li>• A Guide to the Informatization of Education (MEXT: 2020)</li> <li>• Information Moral Education at Schools (MEXT: 2019)</li> <li>• Other Educational Materials for Schools in Japan</li> </ul>
Human Resource Development in Japan for Awareness Raising	<ul style="list-style-type: none"> <li>• Registered Information Security Specialist (IPA)</li> <li>• CAIS-Auditor (JASA)</li> <li>• SPREAD Meister/SPREAD Supporter (SPREAD)</li> <li>• Information Security Management Examination (All-Japan Association for the Promotion of Information Learning)</li> <li>• Cybersecurity Helpers Service Project (IPA)</li> <li>• Education Committee, Japan Network Security Association (JNSA)</li> <li>• Prefecture-level Activities for Cybersecurity Awareness</li> </ul>
Materials for Cybersecurity Awareness Raising in Japan (Web sites)	<ul style="list-style-type: none"> <li>• Information Security Portal site “Start here for security!” (IPA)</li> <li>• Information Security Site for People/for Kids (MIC)</li> <li>• Is your child safe? Beware of smartphones! The pitfalls of online crime. (Government of Japan Public Relations Online)</li> <li>• Internet Dangers and Security to Remember with Kids (JAO)</li> <li>• Useful Web for School Information Security (ISEN)</li> <li>• NPO Information Security Forum</li> <li>• Free! Educational Materials and Countermeasures Guide for Information Security (ISM)</li> </ul>
(Textbooks/ Materials)	<ul style="list-style-type: none"> <li>• Information Security White Paper 2021 (IPA)</li> <li>• White Paper on Information and Communication Technology (MIC)</li> <li>• 10 Major Security Threats 2021 (IPA)</li> <li>• Training Materials on Information Security and ICT Environment Maintenance in Schools (MEXT)</li> <li>• Response Manual and Case Studies on “Cyber Bullying” (MEXT)</li> <li>• Kodomo Anzen Zukan: Smartphone, PC, SNS (Kodansha)</li> <li>• Let’s Think Safe Usage of SNS! (Kanagawa Prefectural Police)</li> </ul>



Survey Items	Main sources of information
(Manga/ Cartoons)	<ul style="list-style-type: none"> <li>• Our Smartphone Lives (IPA)</li> <li>• Understanding 5 Phishing Prevention Measures (Council of Anti-Phishing Japan)</li> <li>• Learning Security Management by Manga for SMEs (EnterpriseZin)</li> <li>• Introduction to Security for First-time Smartphone Users (Google)</li> <li>• IT Passport Exam Preparation Episode 3 “Beware of phishing!” (IPA)</li> </ul>
(Videos/ Animations)	<ul style="list-style-type: none"> <li>• Awareness Raising Videos by IPA</li> <li>• Awareness Raising Videos by National Police Agency</li> <li>• Safety on the Internet and SNS (Experience based Safety Education Program)</li> <li>• Smartphone &amp; Mobile Phone Family Guide (KDDI)</li> <li>• Let’s Experience the Dangerous World of the Internet! (Kanagawa Prefectural Government)</li> </ul>
(Games/E-learning/ Simulation)	<ul style="list-style-type: none"> <li>• Let’s find out what’s “suspicious” on the Internet! (Kaspersky x Shizuoka Univ.)</li> <li>• Learning School Information Security through Case Studies (Hiroshima Kyohan)</li> <li>• Vulnerability Experience Learning Tool: AppGoat (IPA)</li> <li>• Cybersecurity Education Game (JNSA)</li> <li>• Phishing fraud VR “Where is the criminal?” (NPA)</li> </ul>
Experiences, Knowledge, and Issues related to Awareness Raising Activities in Japan	<ul style="list-style-type: none"> <li>• Awareness Survey on Ethics and Threats of Information Security Report (IPA)</li> <li>• Survey Report on Security Trends in Corporate Organizations (Trend Micro)</li> <li>• Whitepaper on Crime (MOJ)</li> </ul>
Characteristics of Awareness Raising Activities for each Target Audience in Japan	<ul style="list-style-type: none"> <li>• Overall Characteristics of Awareness Raising Materials in Japan</li> <li>• Issues on Child Protection in Japan</li> <li>• Cybersecurity of elderly people in Japan</li> </ul>
Strategies and Theories for Awareness Raising Activities in Japan	<ul style="list-style-type: none"> <li>• New Information Security Promotion and Awareness Program (Information Security Policy Council)</li> <li>• Cybersecurity Awareness and Action Enhancement Program (Cybersecurity Strategy Headquarters)</li> </ul>

### Activity 3-1 Create survey report

The results obtained from the above survey were organized, and the numerical information was analyzed using statistical methods, and a survey report was prepared in English.

### Activity 4-1 Prepare awareness raising training materials

Training materials including practice materials were developed in English, based on the results of the survey. The materials contain comprehensive reference information on where to obtain Japanese awareness raising/educational materials that have been found in the survey.

### Activity 5-1 Conduct awareness raising training for AIS

Three-days’ online training was conducted from August 30<sup>th</sup> to September 1<sup>st</sup> 2021 by using the teaching materials developed in the above activities. The timetable of the implemented training is shown in the table below.

Number of participants: 11 staffs from AIS

Table-3 Schedule of the Implemented Awareness Raising Training

Date	Time (Vietnam)	Contents	Lecture	Practice	Discussion
Aug 30 <sup>th</sup> (Mon)	9:00	Opening Session (~9:10)			
	9:10-11:30	<ul style="list-style-type: none"> <li>• Japan's Policy on Awareness raising Activities</li> <li>• Introduction of educational materials for awareness raising in Japan</li> </ul>	✓		
	11:30	Lunch Break (~13:00)			
	13:00-15:30	<ul style="list-style-type: none"> <li>• Characteristics of activities and educational materials for each target audience of awareness-raising activities (e.g., government-related, business, general users, young people, and elderly people)</li> <li>• Experiences, knowledge, and issues related to awareness-raising activities in Japan               <ul style="list-style-type: none"> <li>▪ Especially on the cultural and social background of Japan</li> </ul> </li> </ul>	✓		
Aug 31 <sup>st</sup> (Tue)	9:00-11:30	<ul style="list-style-type: none"> <li>• Japan's Human Resources for Awareness raising, Education, and Materials Development               <ul style="list-style-type: none"> <li>▪ Optional online meetup sessions</li> </ul> </li> <li>• Information Security Education Policy and practice</li> </ul>	✓		✓
	11:30	Lunch Break (~13:00)			
	13:00-15:30	<ul style="list-style-type: none"> <li>• Strategies and theories on awareness-raising activities (general discussion)</li> <li>• Effective and measurable awareness-raising methods (general discussion)</li> </ul>	✓		
Sep 1 <sup>st</sup> (Wed)	9:00-11:30	<ul style="list-style-type: none"> <li>• Marketing methods and theories for the effective use of extension materials               <ul style="list-style-type: none"> <li>▪ SNS marketing, especially to young people</li> </ul> </li> <li>• How to Measure the Effectiveness of Awareness raising Activities               <ul style="list-style-type: none"> <li>▪ Use of online marketing tools, etc.</li> <li>▪ Introduction of methods that are in line with the actual situation in Vietnam</li> </ul> </li> </ul>	✓		✓
	11:30	Lunch Break (~13:00)			
	13:00-15:30	<ul style="list-style-type: none"> <li>• Effective and measurable awareness-raising methods (hands-on)               <ul style="list-style-type: none"> <li>▪ Including an introduction to the use of the tool.</li> </ul> </li> <li>• Recommendations for Awareness raising Activities in Vietnam               <ul style="list-style-type: none"> <li>▪ Session with the DDG of AIS</li> </ul> </li> </ul>	✓	✓	✓
	15:30	Closing Session (~15:45)			

At the end of each day of training, a Q & A session was conducted, and efforts were made to provide feedback on the following day. Questions and requests from participants that require additional survey were brought back to the experts for further research and answered in the follow-up activity described in the next section.

**Activity 5-2 Follow-up on the awareness raising training**

During the training course, there were several requests raised by the participants for additional information and contents such as shown below, and the experts prepared additional information and materials. This additional information was incorporated in updated teaching materials as well as the updated survey reports.

- National budget of Japan allocated to cybersecurity awareness raising
- List of links to information introduced in the training
- Detailed information on “Cybersecurity Helpers Service Project” by IPA

**Activity 5-3 Organize the training results and update the survey report**

Based on the results of the feedback obtained during the training as well as the results of subsequent online discussions with AIS, the experts organized the training results and updated the survey report.

**Activity 6-1 Provide advice to AIS based on the proposed awareness raising methods**

Based on the theories and strategies for effective awareness raising activities that were transferred during the training, the experts made necessary recommendations for future awareness raising activities in a follow-up online meeting on September 29<sup>th</sup> as shown in the table below.

Table-4 Online Discussion with AIS on Recommendations and Additional Activities

Date & Time	September 29 <sup>th</sup> , 2021 11:00-12:00 (Vietnam time)
Participants	AIS: 3 from inspection division JICA: 5 including 2 awareness raising experts
Main Points	The expert team has provided advice on the following topics. <ul style="list-style-type: none"> <li>• The 4<sup>th</sup> awareness raising video</li> <li>• Development of branding kit</li> <li>• Development of COP portal site</li> </ul> AIS and JICA team has discussed on the following topics. <ul style="list-style-type: none"> <li>• Plan to support COP master plan – Draft is available in early October 2021</li> <li>• Extended support from awareness raising experts until January 2022</li> </ul>

**Activity 7-1 Advise on COP masterplan prepared by AIS based on the cases in Japan**

The expert team received the draft COP master plan from AIS on October 8<sup>th</sup>, 2021. The expert read the full content and provided various comments and suggestions to it, and then returned the commented version back to AIS. The AIS acknowledged the comments and suggestions during the next meeting (see later) and told the expert team that they will examine these and act properly.

Activity 8-1 Attend regular progress meetings of creating awareness raising materials by AIS, and provide advice and follow-up

The expert team attended the following regular meetings to provide advice and follow-up on the awareness raising activities of AIS. In each meeting, there were several requests from AIS regarding additional information in Japan as well as the recommendations to their activities.

Table-5 Regular Meeting with AIS on Awareness Raising Activities #1

Date & Time	November 5 <sup>th</sup> , 2021 11:00-13:00 (Vietnam time)
Participants	VNCERT/CC: 4 from inspection division JICA: 5 including 2 awareness raising experts
Main Points	Review of the COP masterplan (The expert has already sent commented version before). <ul style="list-style-type: none"> <li>• The expert recommended to add “Child emergency call” telephone number as well as email/SNS contacts like in Japan.</li> <li>• Vietnam has the 111-call center for similar purpose, but people tend to forget about it.</li> </ul> Regarding cybersecurity education contents <ul style="list-style-type: none"> <li>• Since there is no cybersecurity education in Vietnam, AIS is looking for the focused and consolidated contents for awareness raising of each target age group.</li> <li>• Three content types in Japan now: message -based, storytelling -based, and case study.</li> </ul>

Table-6 Regular Meeting with AIS on Awareness Raising Activities #2

Date & Time	December 6 <sup>th</sup> , 2021 14:00-15:00 (Vietnam time)
Participants	VNCERT/CC: 4 from inspection division JICA: 5 including 2 awareness raising experts
Main Points	The expert prepared and sent materials containing the answers to the request made in the previous meeting (“Information Moral Education – Model Curriculum”). <ul style="list-style-type: none"> <li>• Enhancing the management ability is the answer for the question about how to manage many tasks with limited time and resources.</li> <li>• It is hard to create KPI for evaluating contents for each target age group. The expert created sample CyberSec KPIs so it would be a reference.</li> <li>• Evaluation should be done by hiring a consultant company, but it does not have to be expensive foreign consultants.</li> </ul>

Table-7 Regular Meeting with AIS on Awareness Raising Activities #3

Date & Time	January 6 <sup>th</sup> , 2022 14:00-15:00 (Vietnam time)
Participants	VNCERT/CC: 3 from inspection division JICA: 5 including 2 awareness raising experts
Main Points	The expert prepared and sent materials (before the meeting) containing the answers to the request made in the previous meeting (“Government control on applications for children in Japan”). <ul style="list-style-type: none"> <li>• There is no government control on applications for children in Japan, but some industry associations do screening.</li> <li>• AIS is aiming to establish criteria to evaluate the application, and games to ensure the child protection policy. Game rating or equivalent criteria are supposed to be issued by Government, but the actual evaluation may be done by other entities. Such request is to protect children from abusive activities via the reporting system.</li> <li>• No update for COP masterplan</li> </ul>

	<p>Questions of AIS to the experts (to be answered in the next meeting)</p> <ul style="list-style-type: none"> <li>• Is there any fee required for evaluation from the organization such Cero? What are their evaluation criteria? Who will do the evaluation?</li> <li>• Are there any examples of evaluation criteria (such as checklist or template) in Japan that can be obtained?</li> <li>• Recently, VNCERT has been assigned more tasks about the communication e.g., YouTube and FB channel to gain 100,000 followers/subscribers for each channel. How to do that with the limited budgets? Now they have the support from Google, but they are looking for the expert’s support to build such plan as adapting KPIs.</li> </ul>
--	--

Table-8 Regular Meeting with AIS on Awareness Raising Activities#4

Date & Time	January 24 <sup>th</sup> , 2022 14:00-15:40 (Vietnam time)
Participants	VNCERT/CC: 4 from inspection division JICA: 5 including 2 awareness raising experts
Main Points	<p>The expert team prepared and sent materials containing the answers to the requests made in the previous meeting (updated version of “Government control on applications for children in Japan”<sup>2</sup>, and presentation on how to design KPI for reaching 100,000 followers/subscribers).</p> <ul style="list-style-type: none"> <li>• CERO is for game evaluation only, but how should we control PC applications?</li> <li>• There is no rating system for general applications in Japan except for some. There is filtering software for mobile phones, but kids tend to bypass it.</li> </ul> <p>The expert did comprehensive presentation<sup>3</sup> on how to reach 100,000 followers/subscribers by using detailed analysis of existing YouTube videos on COP in Japan and by deriving potential KPI based on the analysis with consideration of children’s environment in Vietnam.</p>

**Activity 9-1 Prepare cyber exercise training materials**

The training was aimed at AIS engineers/managers who are responsible for delivering cyber exercises. The expert team has taught them how to conduct various types of exercises such as Practice/Training/Exercise/Drill, Tabletop/Hands-on and Real-time/Preliminary. The training also provides a step-by-step explanation on how to design and implement a cyber exercise environment using virtualization technology. The figure below shows the system design for cyber exercise environment in for this training.

<sup>2</sup> The material is submitted to JICA for archiving purpose, and is not open for public view.

<sup>3</sup> The presentation material titled “For the last discussion topic” is submitted to JICA for archiving purpose, and is not open for public view.

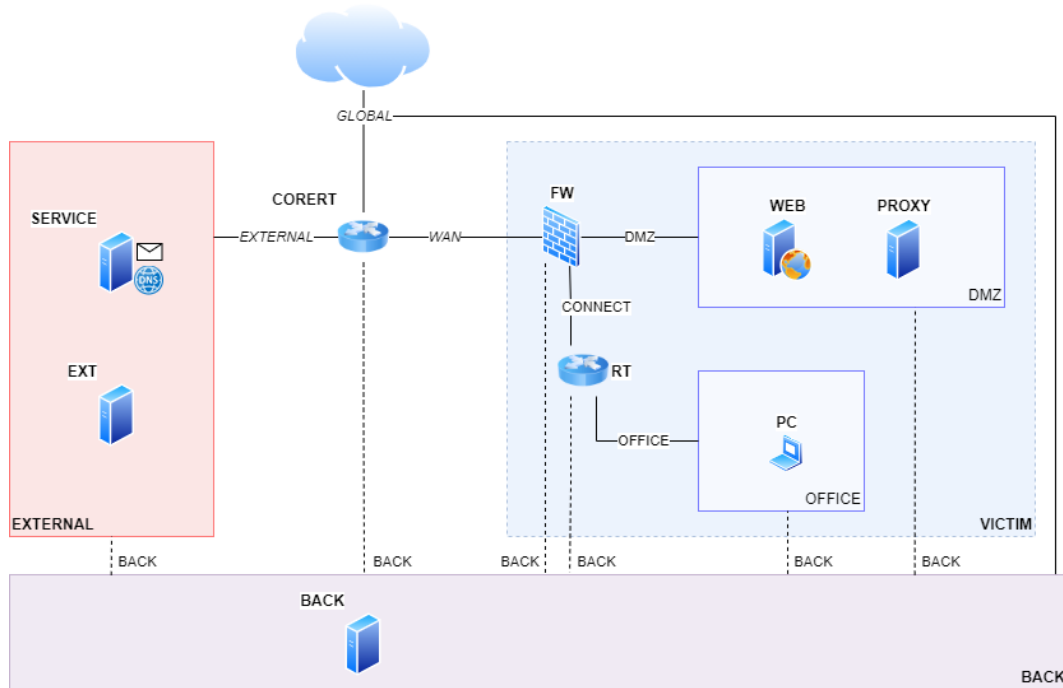


Figure-3 System Diagram for Cyber Exercise Environment

Training materials developed for this training are listed in the table below.

Table-9 Cyber exercise training materials

Category	File name	Description
Textbook	1 Topics1.pdf	Building cyber exercise environment (388 pages)
	2 Topics2.pdf	Designing cyber exercise (214 pages)
	3 Topics2 Worksheet.xlsx	Answer sheet for topics2 exercises
	4 Topics3.pdf	Implementing and operating cyber exercise (45 pages)
	5 Topics3 Hint.pdf	Hints for topics3 exercises (38 pages)
	6 Topics3 QAlist.xlsx	Answer sheet for topics3 exercises
	7 How2importVMs.pdf	Explanations for importing virtual machine images (20 pages)
	network_design.png	Network diagram of supposed cyber exercise environment
Command lines	cmd_topics1.txt cmd_topics2.tx cmd_topics3.txt	Gathered command lines that are used in each training topic. These are used for quick “copy & paste” operation during the exercises in this training.
Script files, Batch files	log-clean.sh log-collect.sh VM-CreateSnapShot.bat VM-RestoreSnapShot.bat VM-Start.bat VM-Stop.bat	Convenient scripts/batch files for the manipulation of cyber exercise environment.
Virtual machine images	BACK_A.ova CORERT_A.ova EXT_A.ova FW_A.ova PC_A.ova PROXY_A.ova RT_A.ova SERVICE_A.ova TEMPLATE_A.ova WEB_A.ova	Virtual machine images for Oracle VM VirtualBox. File names correspond to server names. (See Figure-3 for the servers)

## Activity 9-2 Conduct cyber exercise training for AIS

Five-days' online training was conducted from January 17<sup>th</sup> to 21<sup>st</sup> 2022 through online method by using the teaching materials listed in Table-9. The training included many hands-on activities to help participants acquire practical skills during training.

Number of participants (Total 17):    4 from AIS /Protection Department  
    1 from NCSC  
    11 from VNCERT Hanoi/Da Nang/ HCM  
    1 from Ministry of Information and Communication  
(11 participants attended on-site and 6 remotely.)

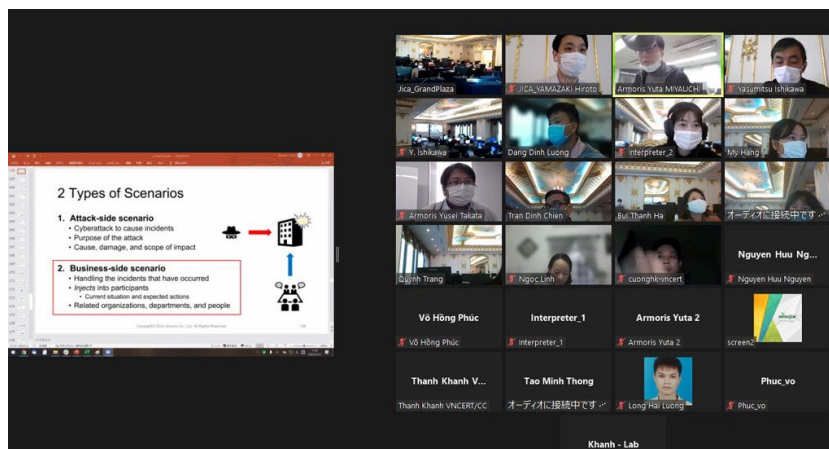
Venue: Conference room of the Grand Plaza Hotel.

The training was successfully implemented. Some comments obtained from the post-event survey are shown below. (See Appendix-A for the results summary of post-event survey.)

- The training helped me a lot with exercises and prevented me from making mistakes in the at workplace via organized content and activities. I will use all the knowledge learned in the course for my work.
- The course gave me a lot of new knowledge, which is very helpful in my work. I hope to take more classes like this in the future.
- The training provided me practical knowledge about current working environment

### Photos of the cyber exercise training (on site and online):





### Activity 10-1 Create work completion report

The results of all activities were compiled into a work completion report and submitted to JICA.

### **3. Special Efforts and Lessons Learned in the Survey Implementation**

In the survey on awareness raising activities in Japan, special efforts were made to clarify the social and educational environment of Japan compared to other countries in the world. For example, Japanese children are facing considerably high stress in schools due to the problem of bullying, and this situation leads to the cybersecurity problem of morality on the internet in Japan. Regarding the awareness raising contents in Japan, they utilize more cartoons and animation than other countries in the world. These unique characteristics of awareness raising activities in Japan were highlighted in the survey in order to guide the participants to consider the similarities and differences of Vietnam and Japan, and encourage them to consider correct and appropriate adaptation of use cases in Japan into Vietnamese context.

As a result of the training regarding the awareness raising activities in Japan, it has pointed out that majority of strategies for awareness raising in Japan could also apply to Vietnam, especially the medium or format of the content such as animation. However, it has also revealed that there are many points for consideration in Vietnam that have no similarity to Japan, such as the ethnic groups as the target group.



## **4. Special Efforts and Lessons Learned in the Training Implementation**

### **4.1 Special Efforts and Lessons Learned in the Awareness Raising Training**

The following points were considered in the design and implementation of the training.

First, although this training was designed to promote awareness, awareness is just a component of marketing as a whole. Therefore, in order to correctly understand and effectively promote the concept and approach of dissemination and awareness, it is important for participants to have a systematic understanding of the overall picture and key points of marketing, and then to understand dissemination and awareness in detail. In order to promote systematic understanding, we conducted a two-stage training program on marketing and awareness-raising. In addition, in order for the participants to efficiently acquire know-how in the limited time available, the marketing lectures other than those on dissemination and awareness-raising were limited to concepts and key points, and more time was allocated to dissemination and awareness-raising to create a lean and concise training structure.

Secondly, since there is a risk that the participants' understanding will remain superficial in a training program that focuses on one-way input, we conducted a workshop-type training program in order to achieve a state where the participants can ultimately utilize the training content. We devised a way to increase the effectiveness of the training by allowing the participants to actually apply the input content to the local situation in Vietnam and digest it themselves. For example, each participant raised a topic of awareness raising in his/her work, and then requested to apply a series of marketing analysis (segmentation, targeting, positioning, persona, etc.) for finding a better way to approach the target audience.

Thirdly, considering the possibility that participants may not be able to reach a level of concreteness in their understanding of the concepts and approaches because they tend to be explained in abstract terms, we tried to raise the resolution of participants' understanding by using examples and case studies. In the case studies, various examples from Japan were introduced and explained according to the framework, items, and perspectives on dissemination and enlightenment, so that the participants could structurally understand how the concept and approach of dissemination and enlightenment could be incorporated into measures. As for the case studies, since it is possible that the participants may not be able to visualize the measures if they are only introduced to the Japanese case studies of dissemination and enlightenment, we tried to promote their understanding by using the local contents in Vietnam. In the workshop, we presented 19 cases in Japan that are considered applicable to Vietnamese context and 3 existing cases in Vietnam for participants' reference.

### **4.2 Special Efforts and Lessons Learned in the Cyber Exercise Training**

The most difficult part of the training was how to provide a training environment for participants remotely. It is because the training requires a very high-performance PC (at least 4 cores CPU, 24GB Memory, 240GB SSD) and participants cannot participate on their own PC. As a solution, we set up the

high-performance PCs at the training site and let remote participants operate on those PCs via remote desktop through VPN. To further ensure stable connections, we distributed mobile Wi-Fi routers to all remote participants in advance. With these measures, the remote participants were able to concentrate on the training without any problems.

## **5. Capacity Change of Counterpart Institution**

Through this training, it is important for the participants to be able to effectively develop strategies and implement various measures for the direction of COP from the perspective of marketing and promotion. From this perspective, the changes in the participants' abilities before and after the training can be described as follows.

First, the literacy level of the participants was initially low, even when considering extension and awareness on its own. However, through the training, the participants were able to understand not only the concept and approach of extension and development on its own, but also to understand it systematically by positioning it within marketing as a whole. This was based on the fact that the participants' opinions became more active as the latter half of the training session progressed, and they came up with specific, targeted opinions. This systematic understanding is expected to contribute to the planning of highly accurate measures with no omissions when considering future dissemination and awareness activities.

Secondly, the introduction of various Japanese case studies along the framework and items of dissemination and awareness-raising helped the participants to recognize and understand the different dissemination and awareness-raising measures in Vietnam and ASEAN countries. As a result, the participants were able to have more options to consider when discussing the local measures in Vietnam, which would have broadened the scope of planning a more diverse dissemination strategy.

Finally, the training led to the extraction of areas where the participants had been unseeing, and the reconfirmation and strengthening of their awareness of issues, which is thought to have contributed to the improvement of accuracy and enhancement of their abilities when considering future measures. One specific example is the case study of children in Vietnam in relation to COP. In the case study, the importance of segmentation and its harmful effects were discussed from the perspective of “children living in urban areas” and “children living in rural areas near the border”, and from the perspective of “children attending school” and “children not attending school”, as well as from the perspective of “children not attending school” who are not attending school for economic reasons. In addition to understanding the importance of segmentation and its negative effects, we conducted a deep dive into the persona perspective in order to eliminate the negative effects of segmentation. These case studies contributed to the improvement of skills to raise the resolution of the target audience, which is the starting point and the most important factor when considering effective dissemination and awareness

raising activities. The skills acquired in the process of hands-on presentation through these training activities will be very useful when considering future dissemination activities in the field.

## **6. Recommendations to Awareness Raising Activities in the Project**

### **6.1 Recommendations to Awareness Raising Activities in the Project**

In this section, we summarize the essence, especially from the viewpoint of awareness raising activities based on the public relations perspective by the public sector rather than the private sector, while keeping in mind that the theme is cybersecurity.

#### Learn from experiences in Japan

The survey report and the training materials created in this work contain many examples of awareness raising activities in Japan, but not all of them have been successful. For example, various videos created by NPA on YouTube achieved very few views (hundreds at most). On the other hand, a few online videos that collaborated with influencers gained far more hits. So, it is recommended to carefully examine the results of awareness raising activities in Japan and try to learn what were their success/failure factors. By analyzing these, one can apply only the successful factors/experiences of Japan to awareness raising activities.

#### Setting the target segment in a time frame, but eventually carrying it out to the level where the entire nation is aware of it.

It is undesirable from the viewpoint of fairness that initiatives are allocated to a specific segment because public sector initiatives are based on tax, and also, cybersecurity affects all citizens. It is necessary to design initiatives with a perspective of raising awareness fairly among all citizens, including budget allocation. However, from the perspective of achieving effective awareness raising activities, it should be noted that activities should be conducted for each target segment as mentioned earlier when implementing the initiatives.

#### Planning content that can involve earned media (third parties)

The level of public awareness/interest in cybersecurity varies depending on demographic attributes and literacy, which means it is not easy for all citizens to take an interest in cybersecurity. Therefore, it is important to design content that enables each of the earned media such as newspapers and TV to share and transmit information in a proactive manner.

#### Inducing synergy effects in awareness raising activities by bundling cybersecurity initiatives with other IT-related initiatives

Various initiatives that focus only on cybersecurity may not motivate people to watch or participate as much as expected because of their demographic attributes and literacy as mentioned earlier. Thus, the number of reaches might become lower. It can be said that would happen as well for companies and

organizations in the private sector, where cybersecurity is self-evidently important. That is likely to depend on the size of the companies/organizations. On the other hand, there are certain demands for applying for government subsidies due to the benefits of funding for companies. In view of the above two points, it is effective to bundle cybersecurity initiatives such as conducting online self-diagnosis of cybersecurity, creating IT operation policies, etc. with other IT-related subsidies for productivity improvement, etc. That may increase the number of companies that can recognize and understand the importance of cybersecurity. This kind of scheme is highly recommended to achieve a wider reach.

#### Setting indicators that can be monitored at fixed points

From the operational point of view, it is obviously important to set up indicators for fixed-point observation after conducting awareness raising activities, but it is also significantly important to conduct surveys using the set indicators to set a standard value before the awareness raising activities so that evaluating and improving the initiatives appropriately becomes possible. In setting indicators, it is important to conduct not only the conventional questionnaire survey but also social listening (online) due to the characteristics of cybersecurity and the penetration of the internet and smartphones. It is also important to verify the set indicators and targeted figures every year, rather than just setting them once.

#### Improving the cybersecurity literacy of government officials (including those in local governments)

In the public sector, while certain departments such as the public relations department oversee awareness raising activities, government (including local government) employees are the ones who usually communicate with citizens. Therefore, it is important for administrative staff members, including those in ministries and local governments, to understand the importance of cybersecurity and be able to correctly convey the message whenever necessary, rather than thinking that awareness raising activities such as seminars and content distribution conducted by specific departments that have little connection to the topic. It is also important from the branding perspective to enhance the perceived quality from citizens to gain public trust. For this purpose, it is essential to provide internal training to improve cybersecurity literacy with administrative staffs including those in local governments.

## **6.2 Recommendations in Cyber Exercise Training**

The content of the training is different from the existing training for cybersecurity professionals, which deals with detection and prevention of cyber-attacks, and is aimed at those who are responsible for planning and conducting cyber exercises involving cyber-attacks. This type of training is still rare in the world, and we expect to implement trainings of this kind in similar JICA projects such as cyber security human resource development projects. Specifically, we recommend implementing a similar ToT (Training of Trainers) in the cyber security human resource development project at UI Indonesia.

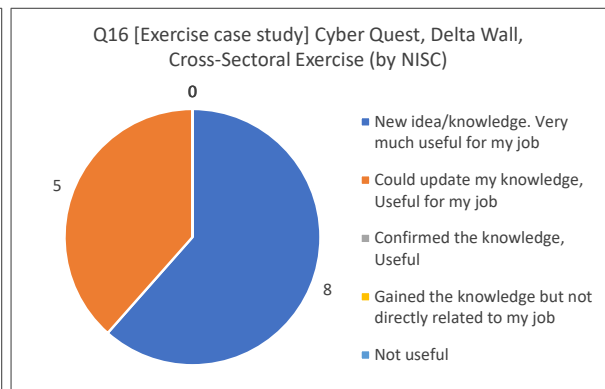
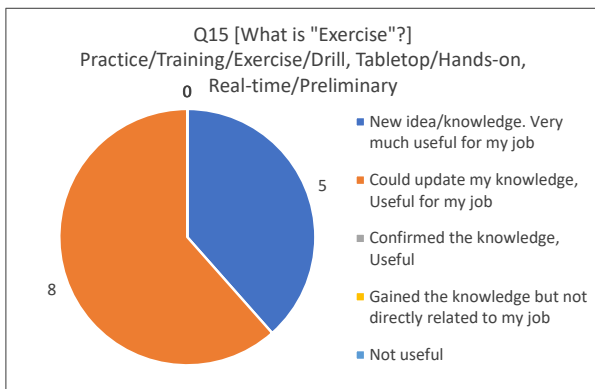
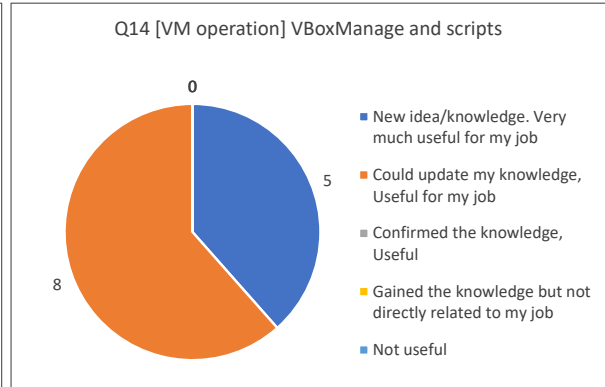
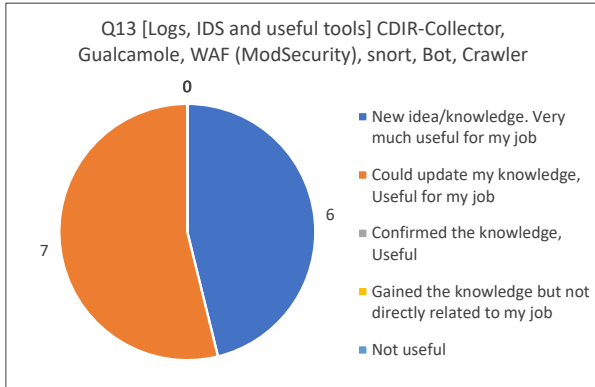
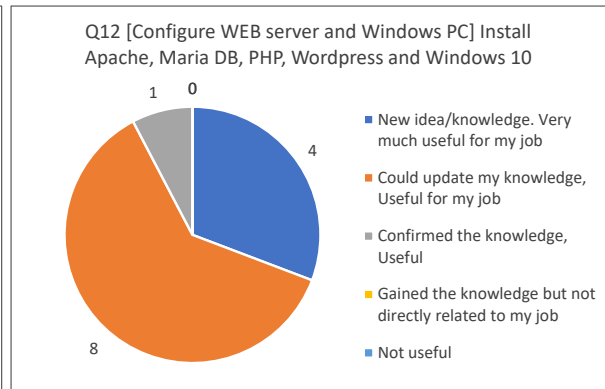
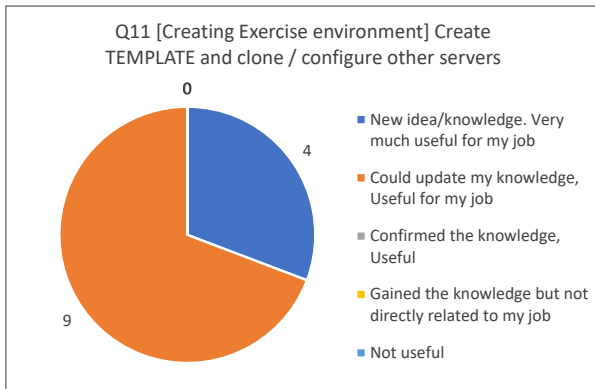
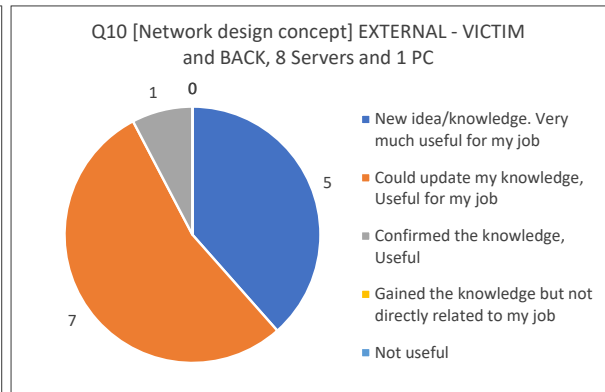
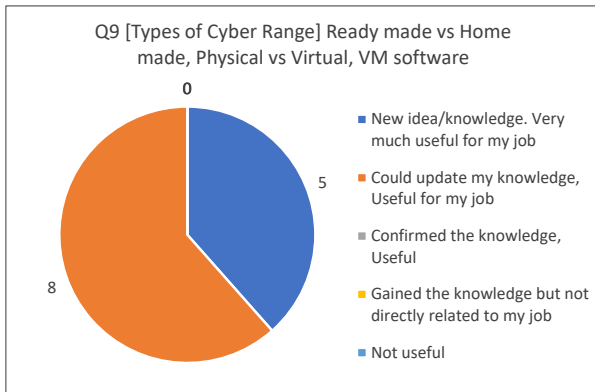
(End of Document)

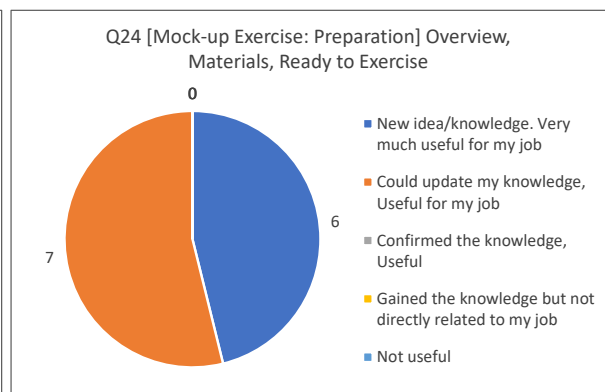
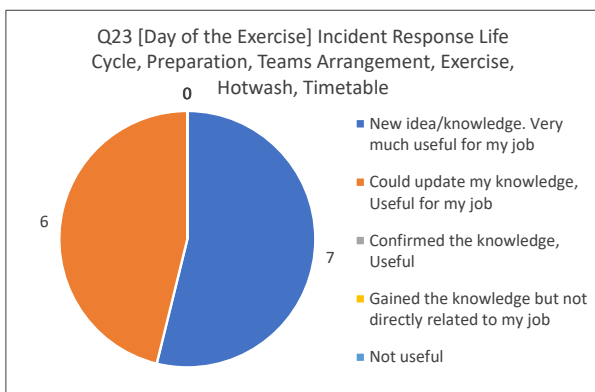
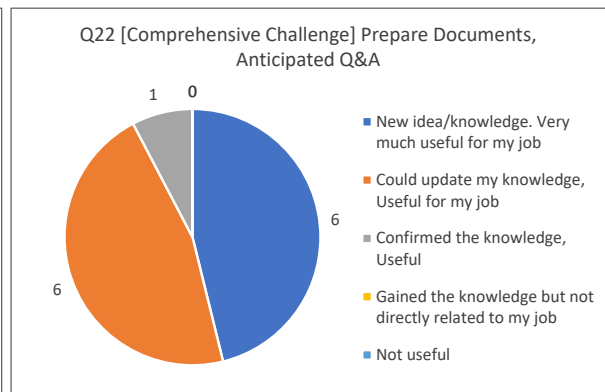
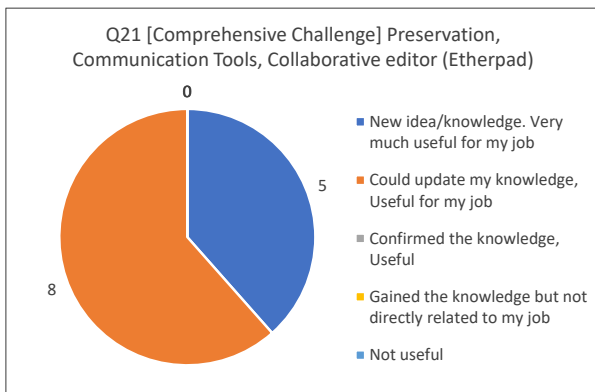
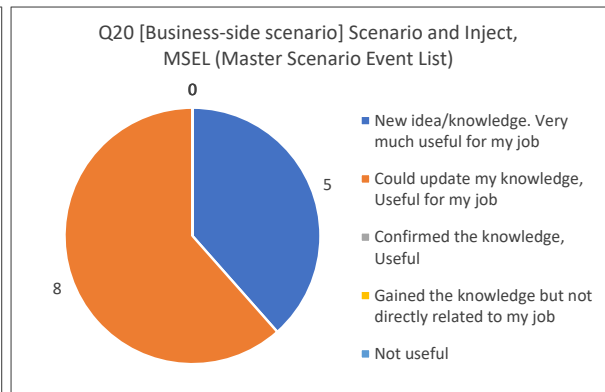
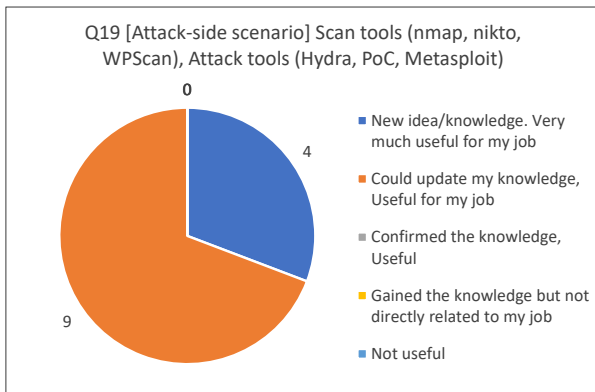
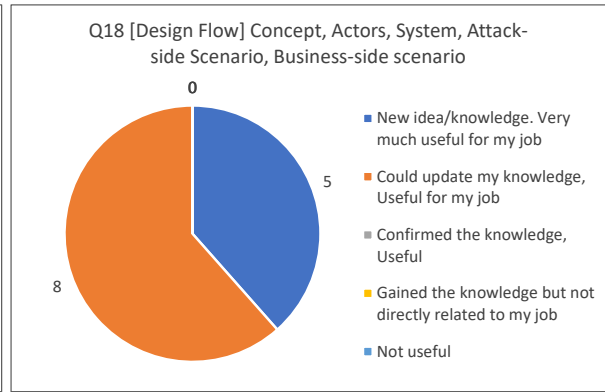
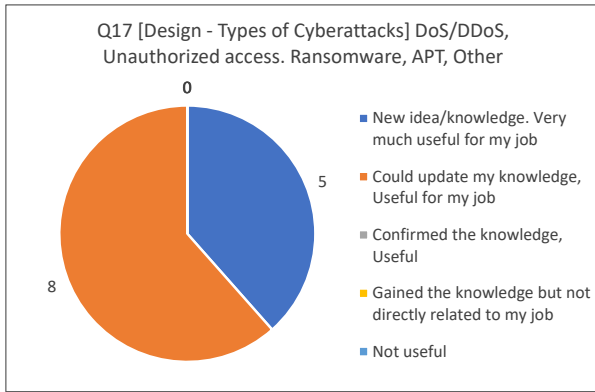
## Appendix A: Result of Post-event Survey for Cyber Exercise Training

Part -1: Please choose the most appropriate answer to the question from the choices provided.

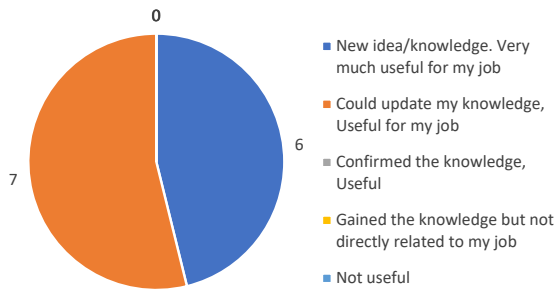


**Part -2: How useful is this course for your work? Choose the closest answer for each topic.**





Q25 [Mock-up Exercise: Exercise] Attacks and Injects, Incident Responses, Interim Reporting



Q26 [Mock-up Exercise: Preparation] Hotwash, Post-Incident Activity

