UNIVERSITY OF INDONESIA
REPUBLIC OF INDONESIA

REPUBLIC OF INDONESIA

PROJECT FOR HUMAN RESOURCES DEVELOPMENT FOR CYBER SECURITY PROFESSIONALS (SOFTWARE QUALITY IMPROVEMENT / CS COURSE DEVELOPMENT / INSTRUCTIONAL DESIGN)

FINAL REPORT

MAY 2022

JAPAN INTERNATIONAL COOPERATION AGENCY

TOKYO CO., Ltd.

GP
JR
22-058

Table of Contents

List of Tables

List of Figures

Abbreviations

Abbreviation	Definition
ADDIE	Analysis, Design, Development, Implementation, and Evaluation
ASCCE	ASEAN-Singapore Cybersecurity Centre of Excellence
BSSN	Badan Siber dan Sandi Negara (National Cyber and Crypto Agency)
CCIT	Center for Computing and Information Technology
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CPU	Central Processing Unit
CS	Cyber Security
CSA	Cyber Security Agency of Singapore
CSIRT	Computer Security Incident Response Team
CSIRT.ID	Cyber Security Independent Resilient Team of Indonesia
DTE	Departemen Teknik Elektro (Department of Electrical Engineering)
ELK	Elasticsearch, Logstash, Kibana
FTUI	Fakultas Teknik Universitas Indonesia (Faculty of Engineering, University of Indonesia)
ICT	Information and Communication Technology
idCARE	Indonesia Cyber Awareness and Resilience Centre
IDS	Intrusion Detection System
JICA	Japan International Cooperation Agency
KSA	Knowledge, Skill, and Ability
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
ME	Mata Elang (Eagle Eye)
OSS	Open-Source Software
PENS	Politeknik Elektronika Negeri Surabaya (Electronic Engineering Polytechnic Institute of Surabaya)
R&D	Research and Development
RFP	Request for Proposal

Abbreviation	Definition
SecBoK	Security Body of Knowledge
TAP	Terminal Access Point
TTT	Train The Trainer
UFW	Uncomplicated Firewall
UI	University of Indonesia
URL	Uniform Resource Locator

0. SUMMARY

Objectives of Work

The objectives of the work “Software Quality Improvement / CS Course Development / Instructional Design” consist of the following three points:

1) Make custom courses, which are nine courses developed in the project, ready for opening by modifying and improving the courses and training lecturers.
2) Establish the procedure of curriculum revision for the University of Indonesia (UI) to be able to continuously improve the curriculum in the future.
3) Establish the system necessary to continuously release stable versions of Open-Source Software (OSS) tools that are being developed in the project.

Results of Activities

The activity “Software Quality Improvement” aimed to establish a system for open-source development and to improve its software quality. The major results of the activities are as follows:

1) The OSS community “Mata Elang community”, which is a communication society of Mata Elang users and developers, was established.
2) The committee “UI-PENS Mata Elang Steering Committee” was also defined and its initial members were assigned. The steering committee is the decision maker for the strategy, release plan, and the specifications of Mata Elang.
3) The distinction between Stable and R&D versions of Mata Elang was clarified. This also clarified the role of Mata Elang Stable and the guidelines to create its development strategy.
4) The strategy and the roadmap for the next five years of Mata Elang Stable were developed. The steering committee can consider the future development and release plan of Mata Elang by referring to this strategy.
5) The “Mata Elang Community Management Guidelines” was developed. This defines the structure of the community as well as the roles of community, steering committee, and project, and its minimum rules.
6) The project “Mata Elang Stable Version” was launched under the supervision of the steering committee. The project immediately started working as the responsible body for the development of the Mata Elang Stable 1.0.
7) The Request for Proposal (RFP) for “Development of Mata Elang Stable Version” was developed. This RFP was immediately submitted to software development

companies and the development of Mata Elang Stable 1.0 had started.

8) The source code and Docker images were prepared. Through the development of Mata Elang Stable, the source code on GitHub and Docker images on DockerHub were reviewed and the improved contents were prepared.
9) The Mata Elang Stable 1.0 was released. In this version, the quality of the software as well as the features, response speed, useability, and stability of Mata Elang were improved.
10) The "Developers' Guide" was prepared. It will be a book for unified development to ensure the software quality among the various developers and contributors.
11) The "Installation Manual" was updated and its quality was improved. The improved manual reduced the difficulty of deploying Mata Elang and encouraged the participation of the Mata Elang Community.
12) "Acceptance Testing" was performed and the quality assurance method was introduced. The project member will be able to perform the future acceptance testing of Mata Elang Stable by referring to this material.
13) Mata Elang workshop was held at Politeknik Elektronika Negeri Surabaya (PENS), Surabaya. The workshop was a good opportunity to introduce the Mata Elang Stable version to the people who are interested in the installation of OSS cybersecurity tools.

Meanwhile, the activity "CS Course Development" aimed to establish a process for sustainable development and revision of the curriculum. The major results of the activities are as follows:

1) The curriculum revision manual and flow were developed by the consultant and approved by UI and the Chief Advisor. These deliverables will be used in the curriculum revision process every two years.
2) The knowledge, skill, and ability mapping of Indonesia Cyber Awareness and Resilience Centre (idCARE) program was updated. This mapping reflects the latest National Initiative for Cybersecurity Education (NICE) Framework and the Security Body of Knowledge (SecBoK).
3) Training for Center for Computing and Information Technology- Fakultas Teknik Universitas Indonesia (CCIT-FTUI) on the curriculum revision was held. The unit leader of CCIT-FTUI can operate the feedback collection system for curriculum revision.
4) The curriculum revision work group was established under idCARE program. This group is an implementation body of curriculum revisions.
5) Both SecBoK and NICE workshop and curriculum revision trial workshop were held. These workshops improved their knowledge regarding NICE Framework and SecBoK, making cluster leaders able to implement curriculum revisions by referring to the manual.

Finally, the activity “Instructional Design” aimed to improve teaching materials based on instructional design, to maximize online training availability, and improve the training contents and preparation of teachers in cybersecurity education. The major results of the activities include:

1) Revision of teaching materials for the nine subjects in line with the specifications of revisions and instructional design. Curriculums and teaching materials based on instructional design provides an effective learning environment.
2) Pre-learning and online learning of each subject were defined for each method of delivery, as a result of the revision of curriculums and teaching materials. The maximization of online training reduces the impact of infectious disease and expands the education opportunity beyond location and time limits.
3) A total of 105 participants joined Train the Trainer (TTT) sessions and learned the modifications of the teaching materials. A total of 63 participants got evaluations that are more than 70 percent on the post-tests and more than 50 percent on mock lessons. They were determined as eligible lecturers.

Lessons Learned / Recommendations

1) Mata Elang Community and Steering Committee

a. Due to the characteristics and difficulties of OSS development, the participation of a person with experience in software engineering and software development management is required for better project management.

b. It is highly recommended to assign a person as a core software engineer under the responsibility of the steering committee. To progress in OSS development, this engineer is expected to allocate a certain amount of working hours to the project.

c. It is recommended to hold Mata Elang workshops to promote the use of Mata Elang. The expansion of Mata Elang users will make the community autonomous and sustainable. For example, it is possible to hold a Mata Elang introduction seminar at the same time as the promotion seminar of the idCARE program.

2) Mata Elang Stable Version

From the viewpoint of verifying the practicality and stability of Mata Elang, the long-term operation of Mata Elang in a real network environment is indispensable. The Mata Elang deployment in Departemen Teknik Elektro (DTE) should be completed before the next development to reveal hidden issues of the current Mata Elang.

a. To make Mata Elang Stable more practical, the development of Mata Elang Stable 1.1 is requested. The major requirements for the next version are as follows:

- ✓ Analysis function of IPv6 traffic
- ✓ Applying Snort v3 (adopting new features and improving performance)
- ✓ Further improvement of stability in long-term operation of Mata Elang
- ✓ Analysis support function of raw data of network event

b. Due to the differences between the condition of Mata Elang development, there are some difficulties and risks for software development of Mata Elang Stable 1.1. Therefore, it is recommended to adopt "Interactive and Incremental Model" as the software development model. However, this model requires more committee involvement compared to the development of Stable 1.0.

3) CS Course Development

a. As the result of curriculum revision trial, two new courses, "Designing secure IoT system" and "IoT Forensic," are proposed. However, the Internet of Things (IoT) security is more challenging than general cybersecurity due to its enormous attack surface and the increased vulnerability of IoT devices. Therefore, it is suggested to have an option of new program pathway for IoT with more subjects from basic to advance.

b. Considering the feasibility of the curriculum revision process, the following are recommended:

- ✓ Have a close relationship among CCIT-FTUI and the cluster leaders to update the curriculum. Currently, communication between them is not frequent.
- ✓ Encourage the technical staff of CCIT to join the training. The technical staff is required to study the system well before the regular class starts.
- ✓ Develop an annual plan for classes to calculate the income of idCARE program. The plan is required to define the budget for development of new subjects or existing subjects as well as the training of trainers.
- ✓ Consider the feasibility of the new course in the curriculum revision process. Budget, program path, and existing plan of classes should be examined before developing the course.

4) Instructional Design

a. As the common topics and common prerequisite knowledge were found in the existing courses, it is recommended to develop the following four pre-learning materials to reduce overlap.

- ✓ Common Cyberattacks and Malwares
- ✓ Basis of Information Security
- ✓ Introduction of National Institute of Standards and Technology (NIST) Frameworks
- ✓ NICE Framework / SecBoK

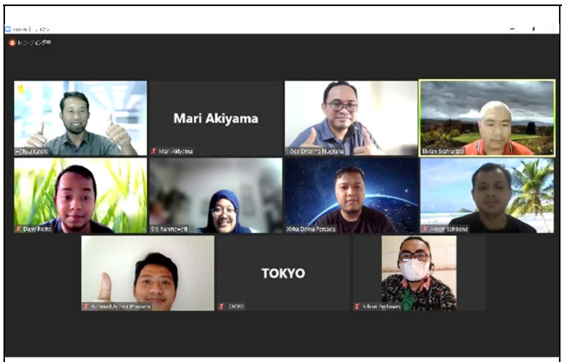
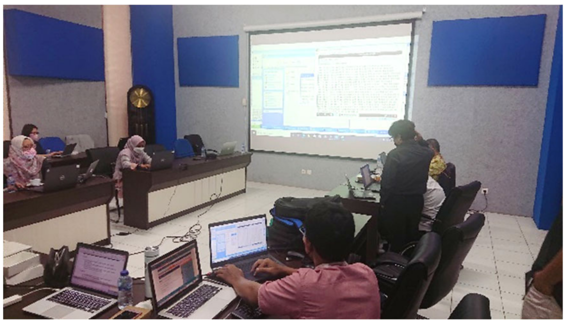
b. At the TTT of “FOR0010a Malware Analysis”, there was a request from the participants regarding the reference to study the assembly language. Therefore, the idCARE manager should notify the subject applicants about the additional reference book for learning the assembly language in advance along with the syllabus.

c. Screening of participants before and after the TTT is recommended to ensure fulfillment of duties in the idCARE program. This is due to several participants being unable to complete their duties especially during the online training.

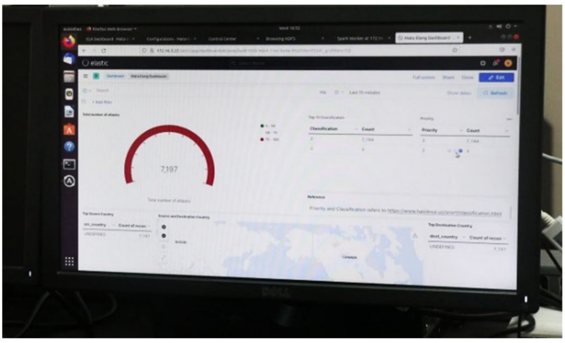
d. Careful check of the feedback from students and lecturers by the cluster leaders are necessary, especially in its first year of regular class operation. The idCARE manager should hold some cluster meetings to collect active feedback from the lecturers and analyze data of the feedback collection system of idCARE program. Some topics may need to be enriched or reorganized depending on the result of feedback analysis.

Photos

1) Instructional Design and TTT

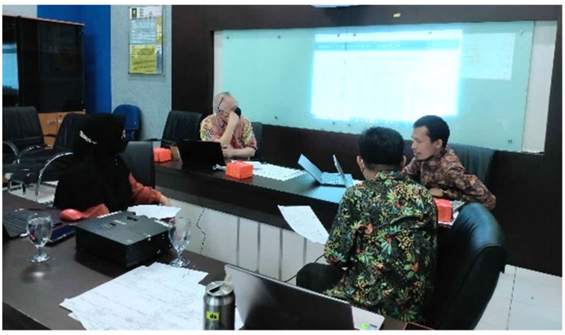
	
CMP0010a Comprehensive exercise: CSIRT online TTT	FOR0010a Case Study and Practice: Malware analysis offline TTT
Discussion among the participants of FOR0010a Malware analysis TTT	Learn how to use forensic tools in FOR0040a Computer forensic

2) Software Quality Improvement and Mata Elang

	
Mata Elang workshop at PENS, Surabaya	Mata Elang Stable 1.0: Network Intrusion Detection System

Setting up the Mata Elang Environment for Workshop by PENS	Technical assistance for Mata Elang installation between UI and PENS

3) CS Course Development

Opening remarks by the head of DTE department, Dr-Eng. Arif Udhiarto	Group photo with participants of the workshop
	
Group work to check the latest commercial courses and cyber security trend	Group work to check the latest cyber security framework

1. INTRODUCTION

1.1. Project Background

1) Development status and issues of the cyber security sector

As information and communication technology (ICT) becomes increasingly important, the risk of cyber-attacks and information leakage is also rising. Incidents such as the fraudulent remittance of USD 81 million that the Central Bank of Bangladesh suffered have been confirmed around the world. Thus, cyber-attacks on critical infrastructure are recognized as a major national risk.

In Indonesia, the establishment of the central government department in charge of cyber security (CS) and the formulation of rules have been generally completed. However, the lack of quantity and quality of CS human resources in private institutions and public sector has been pointed out by the government and economic organizations. The reasons behind this are the lack of training opportunities and the vague definition of roles for each CS personnel.

2) Cyber security sector development policy and positioning of this project

As one of the pillars of the Indonesian CS strategy formulated by the Ministry of Information and Communication in 2016, it is planned to produce human resources based on the needs of the industry and promotion of CS awareness through higher education institutions. Moreover, eight fields, including electricity, transportation, and finance, are designated as critical information infrastructure (CII), which is the focus of CS measures.

1.2. Project Overview

The "Project for Human Resources Development for Cyber Security Professionals" (hereinafter called "the project") began in May 2019. The project has been developing the CS education system at the University of Indonesia (UI). It aims to continuously supply CS human resources to private organizations and government institutions, mainly in the field of CII. It has also been targeting to improve the skills of CS human resources and promote mutual exchange among them in Asian governments by providing project training, teaching materials, and open-source security (OSS) tools.

1.3. The Overall Goal of the Project

Enterprises, government, education entities, and non-government organizations in Indonesia are able to take appropriate security measure to prevent and counter cyber threat.

1.4. Project Purpose

The education system in the University of Indonesia for CS professionals is strengthened based on demand by ICT entities.

1.5. Project Output

The following services and products are expected to be produced through the project activities.

Output 1: World-class CS professional training program is held by the University of Indonesia.

Output 2: Open-source cyber security tools required by the ICT entities are localized or developed.

Output 3: Open courseware in cyber security is developed and opened to public.

Output 4: A global network for cyber security entities is strengthened to increase the number of participants and stakeholders for the course.

1.6. Project Activities

To achieve the above outputs, the following activities are planned.

Output 1:

1-1. Study other countries' ICT skill standard, including the National Initiative for Cybersecurity Education (NICE) in the United States of America (US), Security Body of Knowledge (SecBoK) in Japan

1-2. Design up-to-date and comprehensive CS curriculum

1-3. Develop syllabuses based on the curriculum

1-4. Train university lecturers (including guest lecturers from private sector)

1-5. Establish various short-term training courses that are components of the long course

1-6. Monitor activities related to training courses and improve them when necessary

Output 2:

2-1. Study existing open-source cyber security tools

2-2. Study the demand of cyber security tools

2-3. Select the highly demanded tools to localize or develop

2-4. Provide implementation support for the localized and/or developed tools

Output 3:

3-1. Choose the appropriate topics from the CS curriculum

3-2. Develop open courseware of chosen topics

3-3. Release the developed courseware

3-4. Collect feedback from users and improve the courseware when necessary

Output 4:

4-1. Strategically conduct CS trainings to human resource with other countries

4-2. Disseminate course outcomes through International/Regional organizations or other appropriate forums

2. OVERVIEW OF WORK

2.1. Objectives

As part of this project, the objectives of our work “Software Quality Improvement / CS Course Development / Instructional Design” (hereinafter called “the work”), are the following:

1) Make custom courses, which are nine courses developed in the project, ready for opening by modifying and improving the courses and training lecturers.
2) Establish the procedure of curriculum revision for the University of Indonesia to be able to continuously improve the curriculum in the future.
3) Establish the system necessary to continuously release stable versions of Open-Source Software (OSS) tools that are being developed in the project.

2.2. Situation and Issues of the Project

Our understanding of the situation of this project and the issues it faces at the start of work are as follows:

1) Since teaching materials are not based on instructional design, there is room for improvement in its quality.
2) Custom courses are not designed for online training delivery and are thus terribly affected by COVID-19 and its restrictions on face-to-face training sessions.
3) Although teacher trainings of some courses were already conducted, its duration, content, and number of participants are limited due to the impact of COVID-19.
4) The method of curriculum development and revision has not been established.
5) Open-source development is not organized.
6) The open-source development rules are not clear and its software quality has not reached the product level.

2.3. Critical Points of the Work

Based on the analysis of the situation and issues, the critical points (most important matters) of the work are described below:

Table 2-1 Situation and issues of the project, and critical points

Situation and Issues	Critical Point
1) The quality of teaching materials is low.	Revision and improvement of teaching materials based on instructional design
2) Custom courses are not designed for online training.	Maximize online training available anytime, anywhere
3) The content of teacher training that was already implemented is limited.	Improvement of training content and preparation of teachers involved in CS education
4) The method of curriculum development and revision has not been established.	Establish a process for sustainable development and revision of the curriculum
5) Open-source development is not organized. 6) The quality of open-source development is low.	Establish a system for open-source development and improving its quality

2.4. Implementation Method of the Work

We have divided this work into six task components, including a local subcontractor, as shown in the Figure 2-1.

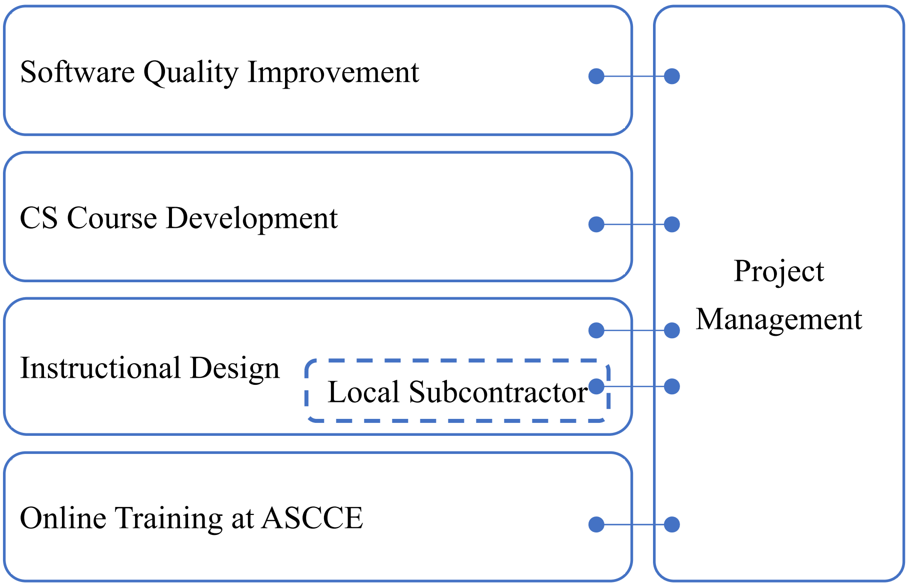


Figure 2-1 Six task components of the work

Table 2-2 Six task components and its description

Task component	Task description
Project Management	✓ Coordinate and manage project activities, and conduct comprehensive quality management of the work.
Software Quality Improvement	✓ Establish an OSS development system and improve software quality.
CS Course Development	✓ Establish a process for sustainable development and revision of the curriculum.
Instructional Design	✓ Improve of teaching materials based on instructional design theory. ✓ Redesign courses to maximize online training for participation anytime, anywhere. ✓ Prepare the trainings of lecturers related to CS education.
Local Subcontractor of CS	✓ Revise teaching materials under the instruction of Japan International Cooperation Agency (JICA) consultant of Instructional Design and conduct trainings of lecturers.
Online Training at ASCCE	✓ Conduct CS trainings for CS personnel in South East Asian countries upon request from ASEAN-Singapore Cybersecurity Centre of Excellence.

2.5. Deliverables

The following tables show the project management and technical deliverables.

Table 2-3 List of administrative documents and reports

No	Administrative Document and Report
1	Work Plan
2	Final Report
3	Request for Proposal (RFP) of "Material enhancement and Training of trainers of Cybersecurity training courses"
4	Service Contract of "Material enhancement and Training of trainers of Cybersecurity training courses"

No	Administrative Document and Report
5	Service Contract of “Additional Training of trainers of Cybersecurity training courses”
6	Certificate of Handover and List of Equipment for Mata Elang

Table 2-4 List of technical deliverables

No	Technical Deliverables
1	Mata Elang Community Structure Diagram and Member Assignment
2	Mata Elang Community Management Guideline
3	Task List for Mata Elang Stable Release
4	Strategy of Mata Elang Stable Development
5	RFP of Mata Elang Stable 1.0 Development
6	Source Code and Docker images of Mata Elang Stable 1.0
7	Mata Elang Installation Manual
8	Acceptance Testing Plan and Checklist of Mata Elang Stable 1.0
9	OSS Developers Guide
10	Curriculum Revision Manual
11	SecBoK-idCARE Program Mapping
12	Proposal for New Subjects and Plan of Train the Trainers (TTT)
13	Syllabus of nine CS custom courses
14	Specifications of Teaching Material Revision
15	Plan of TTT
16	Teaching Materials of nine CS custom courses
17	Proposal for Common Pre-learning Materials
18	Lectures Training Implementation Report
19	Evaluation report of Trainers

2.6. Work Flow

The following figure shows how the work was carried out:

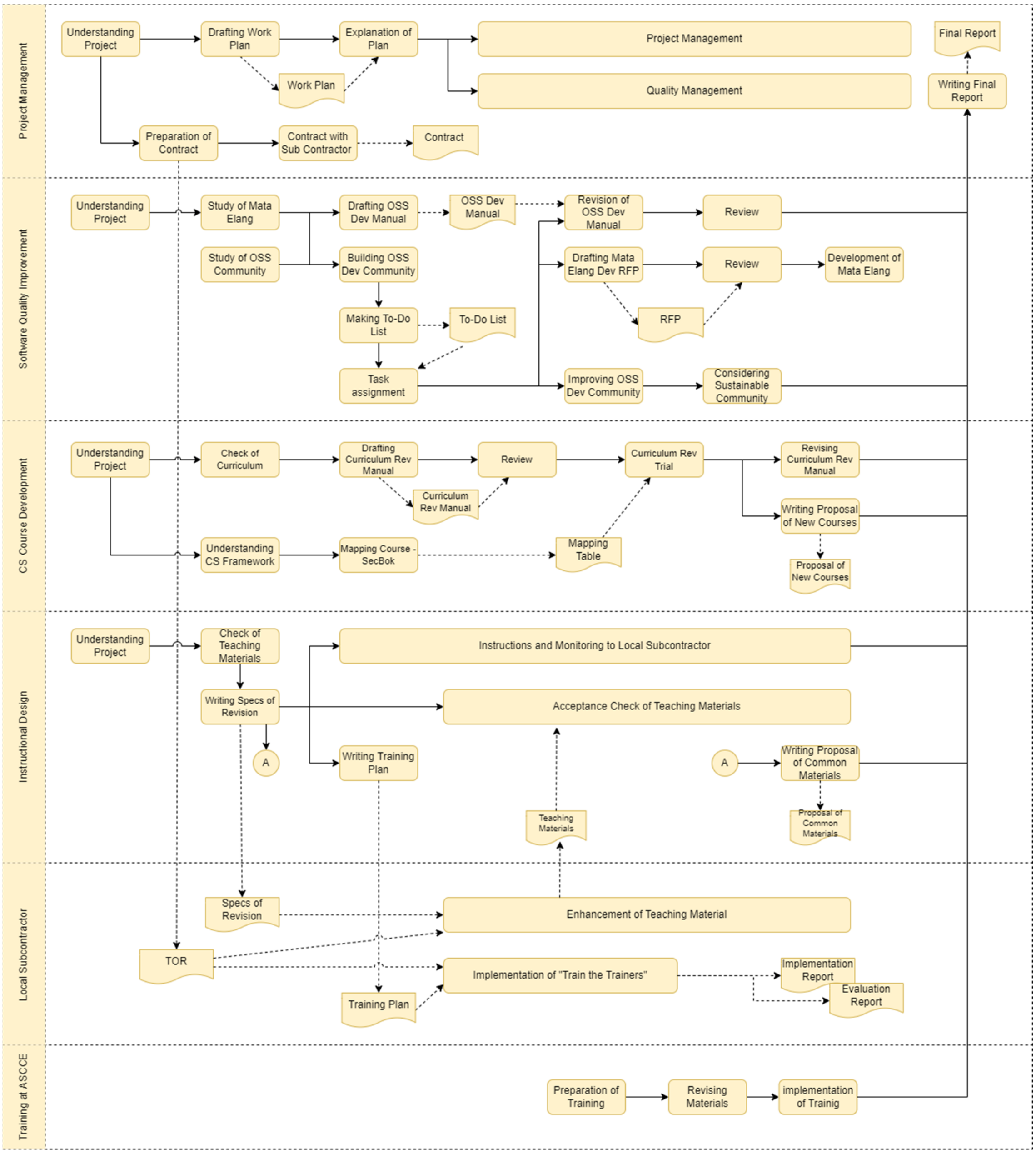
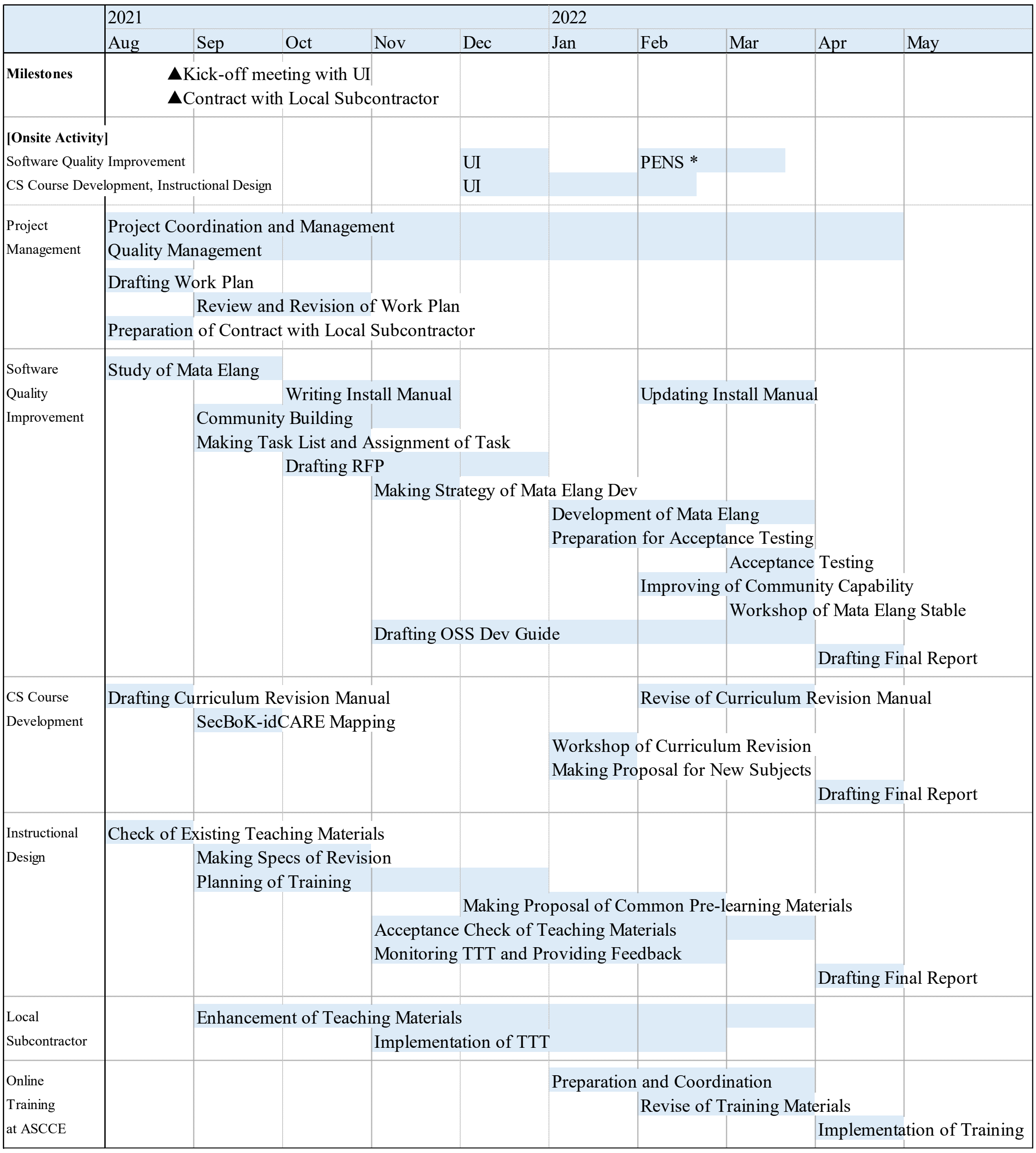


Figure 2-2 Work Flow

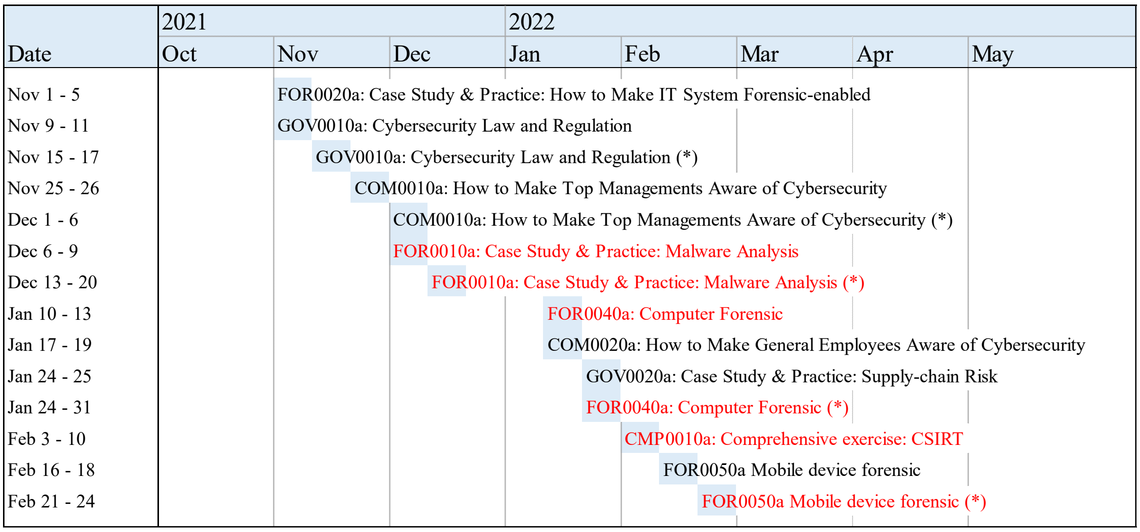
2.7. Work Schedule

The schedule of this work is shown below. Meanwhile, the subsequent figure shows the training schedule.



* Politeknik Elektronika Negeri Surabaya (Electronic Engineering Polytechnic Institute of Surabaya)

Figure 2-3 Work Schedule



	2021			2022				
Date	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May
Nov 1 - 5		FOR0020a: Case Study & Practice: How to Make IT System Forensic-enabled						
Nov 9 - 11		GOV0010a: Cybersecurity Law and Regulation						
Nov 15 - 17		GOV0010a: Cybersecurity Law and Regulation (*)						
Nov 25 - 26		COM0010a: How to Make Top Managements Aware of Cybersecurity						
Dec 1 - 6			COM0010a: How to Make Top Managements Aware of Cybersecurity (*)					
Dec 6 - 9			FOR0010a: Case Study & Practice: Malware Analysis					
Dec 13 - 20			FOR0010a: Case Study & Practice: Malware Analysis (*)					
Jan 10 - 13				FOR0040a: Computer Forensic				
Jan 17 - 19				COM0020a: How to Make General Employees Aware of Cybersecurity				
Jan 24 - 25				GOV0020a: Case Study & Practice: Supply-chain Risk				
Jan 24 - 31				FOR0040a: Computer Forensic (*)				
Feb 3 - 10					CMP0010a: Comprehensive exercise: CSIRT			
Feb 16 - 18					FOR0050a Mobile device forensic			
Feb 21 - 24					FOR0050a Mobile device forensic (*)			

RED indicates "Offline Training", BLACK indicates "Online Training", SUFFIX (*) means "Additional Training".

Figure 2-4 Training Schedule

2.8. Consultant Assignment

The following table shows the consultant assignment for each task component. In addition to the chief consultant, some key components have deputy consultants and assistants assigned to them.

Table 2-5 Assignment of Consultants / Assistant

Task component	Position	Name and Company
Project Management	Chief Consultant	SAKURAI Hitohiro, TOKYO Co., Ltd.
	Deputy Consultant	AKIYAMA Mari, TOKYO Co., Ltd.
	Assistant	KISHI Mako, TOKYO Co., Ltd.
	Assistant	YASUKAWA Ikiko, TOKYO Co., Ltd.
Software Quality Improvement	Chief Consultant	SAKURAI Hitohiro
	Deputy Consultant	SUGAWARA Maiko, TOKYO Co., Ltd.
	Assistant	KISHI Mako
CS Course Development	Chief Consultant	AKIYAMA Mari
	Deputy Consultant	SAKURAI Hitohiro
Instructional Design	Chief Consultant	HIGURASHI Kaoru, Uchida Human Development Co., Ltd.
	Deputy Consultant	AKIYAMA Mari
	Assistant	KISHI Mako

Task component	Position	Name and Company
Online Training at ASCCE	Chief Consultant	AKIYAMA Mari,
	Lecturer	KONDO Sasagu, COL LEGNO Co., Ltd.

2.9. Equipment

The following equipment are purchased for the development of Mata Elang and were handed over to UI.

Table 2-6 List of equipment

Device	Nos	Description
Network TAP, IXIA TAP2-CU3	1	The copper tap Two network ports and two monitoring ports Throughput: 10/100/1000Mbps
Network TAP, Gigamon GTP-ATX01	1	The copper tap Two network ports and two monitoring ports Throughput: 10/100/1000Mbps
Notebook Lenovo ThinkPad P14s Gen 2	2	Sensor PC x 1, Control PC x 1 Intel Core i7-1165G7 Processor Mem: 16 GB Disk: SSD 512 GB

3. SOFTWARE QUALITY IMPROVEMENT

3.1. About Mata Elang

“Mata Elang” (referred to as "ME") is an OSS IDS (Intrusion Detection System) to be target in this activity. For more details, please refer to Mata Elang project site (https://github.com/mata-elang-stable/mataelang-platform/wiki).

3.2. Objectives, Critical points, Issues, and Countermeasures

Based on the situation and issues of the project and the analyzed critical points of the work, the objectives, critical points, issues, and countermeasures of “Software Quality Improvement” are summarized in Table 3-1.

Table 3-1 Activity indicators of “Software Quality Improvement”

Item	Description
Objectives	Establish the system necessary to continuously release stable versions of the OSS tools that are being developed in the project
Critical points	Establishing an open-source development system and improving quality
Issues	✓ Open-source development is not formally organized. ✓ Open-source development rules are not documented. ✓ There is no definition of stable version of OSS tools and no quality management rules. ✓ Configurations are complicated and the manual is not ready for newcomers. ✓ There is no rule and no contact point on who is willing to join the OSS development.
Countermeasures for the issues	✓ Build up an OSS development community and support its organizing process. ✓ Organize a quality assurance team within the community to help improve the quality of OSS tools. ✓ Develop support documents to help introduce OSS tools and promote the participation of other engineers to the community. ✓ Prepare an OSS tool development manual and guidelines that contains development rules.

Item	Description
	✓ Clarify the distinction between stable and R&D versions of OSS tools and develop a plan for the continuous release of stable versions.

3.2.1. Activities and Workflow

To achieve the objectives of the activity “Software Quality Improvement,” the following activities and workflow was applied.

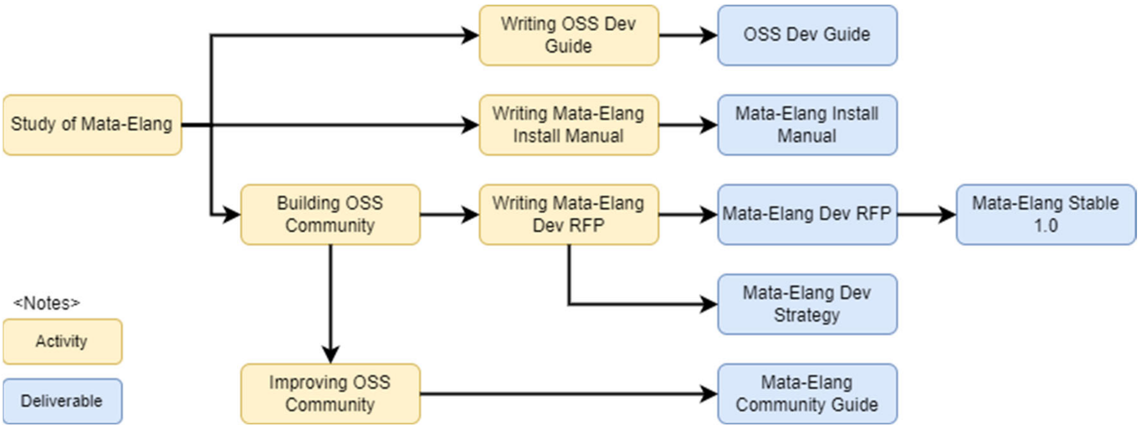


Figure 3-1 Workflow of “Software Quality Improvement”

Table 3-2 Major activity of “Software Quality Improvement”

Activity	Explanation
Study of Mata Elang	Understand ME through reading documentation and actual installation and operation.
Building OSS Community	Define the OSS community of ME and establish ME committee.
Writing OSS Development Guide	Identify the necessary items to develop the OSS within the community and write a development guide.
Writing Mata Elang Installation Manual	Review the installation procedure of ME and write it down as much as possible so that users can install it themselves.

Activity	Explanation
Writing Mata Elang Development RFP	Consider the development strategy of ME over the next four years and write RFP for the development of ME Stable 1.0.
Improving OSS Community	Improve the capacity of ME community from the view of quality management.

3.3. Activity Schedule

The activities for "Software Quality Improvement" were performed with the following schedule.

Table 3-3 Activity Schedule

Phase	Period	Location	Activity
1st Off-site /Online	July 2021 – Nov. 2021	Off-site / Online	• Study of ME • Building OSS community • Writing OSS developers guide • Writing ME installation manual
2nd On-site	Dec. 2, 2021 – Dec. 21, 2021 (20 days)	UI, Depok	• Writing ME Development RFP
3rd Online	Jan. 2022	Online	• Writing OSS developers guide • Writing ME installation manual
4th On-site	Feb. 9, 2022 – Feb. 18, 2022 (10 days)	UI, Depok	• Improving OSS community • Writing OSS developers guide • Writing ME installation manual
	Feb. 19, 2022 – Mar. 15, 2022 (25 days)	PENS, Surabaya	
	Mar. 16, 2022 – Mar. 18, 2022 (3 days)	UI, Depok	

3.4. Activity Report

3.4.1. Study of Mata Elang

1) Current Issues

As a result of the ME study, we confirmed the basic functions as IDS are working properly. However, we found some issues regarding stable operation as described below.

Table 3-4 Current issues of Mata Elang

No	Current Issue
1	The installation procedure of Mata Elang is not clear, and some information is missing.
2	The URL in the installation procedure is out-of-date and abolished.
3	Due to the lack of checkpoints in the installation procedure, it is difficult to determine the cause of the installation failure.
4	There is not enough explanatory material for the configuration of ME.
5	The version of the Linux library is out-of-date, and some commands are not executed.
6	Some versions of OSS products of ME no longer provide its software maintenance.
7	Some of OSS products of ME are not specified in the version during the installation process, which may result in the installation of the latest version that no one has tested.
8	The operation of starting services / stopping services is not clearly documented, and it causes the unexpected trouble such as port conflict.
9	The administrator account and its password are set by default. However, there is no explanation on how to change the settings of the administrator account.
10	The combination of Docker and UFW (Linux Firewall) may allow unintended access from outside in some cases.
11	Log rotation is not implemented in some OSS products.
12	Large-size log data squeezes disk space, causes disk full failure, and unexpected down of ME.
13	The specification of ME is not well documented.
14	The contents of the ME GitHub were not updated in some repositories.

3.4.2. Building OSS Community

1) One community and two committees

“Mata Elang community” (hereinafter called “the community”) is a common society of ME related projects.

The community consists of two committees; one is “UI-PENS Mata Elang Steering Committee” and the other is “Mata Elang Core Project for Research Committee”.

“UI-PENS Mata Elang Steering Committee” (hereinafter called “the steering committee”) has a mission to release a stable version for their target users, such as government, CII operators, and educational entities. The steering committee can also receive support from JICA.

“Mata Elang Core Project for Research Committee” (hereinafter called “the research committee”) aims to study security tools, apply new technologies, and develop new features.

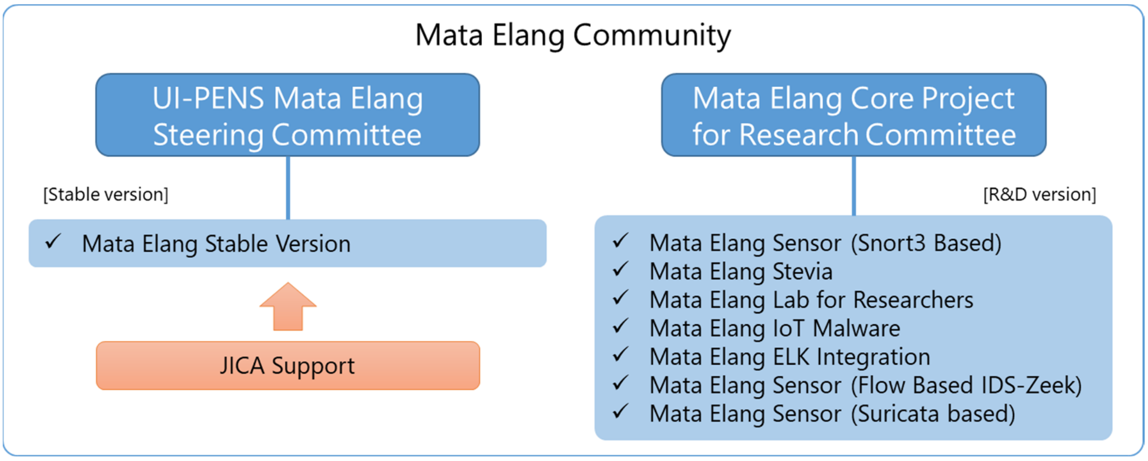

Mata Elang Community
UI-PENS Mata Elang Steering Committee
Mata Elang Core Project for Research Committee
[Stable version]
[R&D version]
✓ Mata Elang Stable Version
JICA Support
✓ Mata Elang Sensor (Snort3 Based)
✓ Mata Elang Stevia
✓ Mata Elang Lab for Researchers
✓ Mata Elang IoT Malware
✓ Mata Elang ELK Integration
✓ Mata Elang Sensor (Flow Based IDS-Zeek)
✓ Mata Elang Sensor (Suricata based)

Figure 3-2 Mata Elang community and two committees

2) Relationship between two committees

The steering committee receives the social demands, requests the study of new version to the research committee, and delivers the stable version to their target users.

The research committee absorbs cutting-edge technologies into ME and reflects its new features in the stable version.

The community serves as a bridge between these two committees.

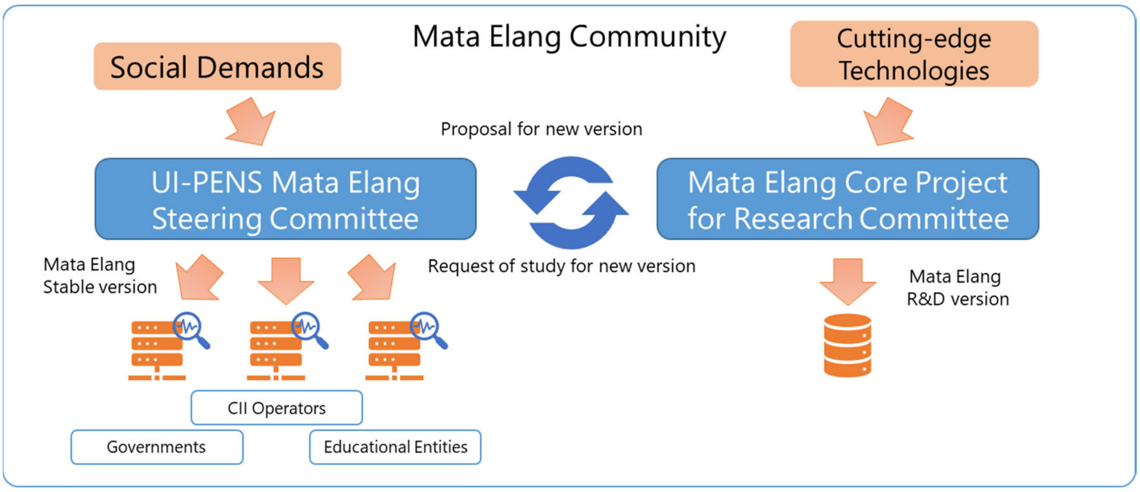

Mata Elang Community
Social Demands
Cutting-edge Technologies
Proposal for new version
UI-PENS Mata Elang Steering Committee
Mata Elang Core Project for Research Committee
Request of study for new version
Mata Elang Stable version
Mata Elang R&D version
CII Operators
Governments
Educational Entities

Figure 3-3 Relationship between two committees

3) Mata Elang Stable version

The mission of the ME Stable version is to be an OSS security tool that meets the demands of government, industry, and educational institutions, as well as to improve the security environment of the users and to contribute the human resource development for cybersecurity professionals.

To achieve this mission, the ME Stable version must meet social demands in terms of both the same quality as industrial products and long-term support.

Table 3-5 shows the differences between two versions of ME developed by each committee.

Table 3-5 Differences between Stable and R&D

	Mata Elang (Stable version)	Mata Elang (R&D version)
Purpose	Released as a Stable version, it aims to meet the business demand from target users such as Indonesian CII operators and other interested parties.	For research and development of new technologies and new functions applied to security OSS tools.
Management Body	UI-PENS Mata Elang Steering Committee	Mata Elang Core Project for Research Committee
User	Business users such as CII operators in Indonesia, and	Security OSS researchers and developers

	Mata Elang (Stable version)	Mata Elang (R&D version)
	Computer Emergency Response Teams (CERTs) in Laos, Timor-Leste, and Cambodia	

4) Member assignment

The members of the steering committee at startup are shown below.

Table 3-6 Members of the steering committee

Position	Name and Organization
Chair	Prof. Dr-ing Kalamullah Ramli, UI
Co-Chair	Dr. Rudi Lumanto, CSIRT.ID
Member	Dr. Udin Harun Al Rasyid, PENS
	Mr. Ferry Astika Saputra, PENS
	Dr. Muhammad Salman, UI
	Dr. I Gde Dharma Nugraha, UI
Project Leader	Mr. Ferry Astika Saputra, PENS

All members assignment, including the research committee and projects, are listed in Appendix 12 “Mata Elang Community Member List”.

5) Mata Elang Community Management Guidelines

After the definition and roles of the community and two committees were determined, “Mata Elang Community Management Guidelines” was developed. See Appendix 11 “Mata Elang Community Management Guidelines” for details.

The guideline includes the following topics:

i. About Mata Elang
ii. Why do we need the Stable version?
iii. Requirements of Stable version
iv. ME Community and Two Committees
v. Differences between Stable and R&D
vi. Basic Information of Community

vii. Basic Information of Committee
viii. Management and Implementation Structure
ix. Roles and Responsibilities
x. Member Assignment
xi. How to Join or Be Appointed

6) Task list

After reviewing the outline of the steering committee, a list of tasks was created to start the activity of committee and to start the development of ME Stable version. Details can be found in Appendix 13 “Mata Elang Committee Task List”.

Table 3-7 Task list of the steering committee

No	Task
1	Confirm the demand about ME from the target users
2	Use ME in idCARE program
3	Establish the ME Community
4	Define committers and developers for projects under committees
5	Complete ME Community Management Guidelines
6	Report results of ME installation trial
7	Confirm the mission and purpose of the Stable version
8	Decide the license of Stable version
9	Fix the architecture of Stable version 1
10	Define required functions for Stable version 1
11	Define the strategy of Stable version release and its life cycle
12	Establish quality assurance method of Stable version
13	Prepare GitHub repositories for Stable version
14	Establish method of source code and document management
15	Establish the stable version support team for the users
16	Propose activities for JICA financial support
17	Prepare RFPs for developing the Stable version with JICA financial support
18	Make a short list of candidates to distribute the RFP of stable version development
19	Prepare environment for the RFP recipients
20	Prepare testing environment

No	Task
21	Propose a business model to continue ME development
22	Prepare a community website for public relations
23	Conduct activities to spread ME to the target users.

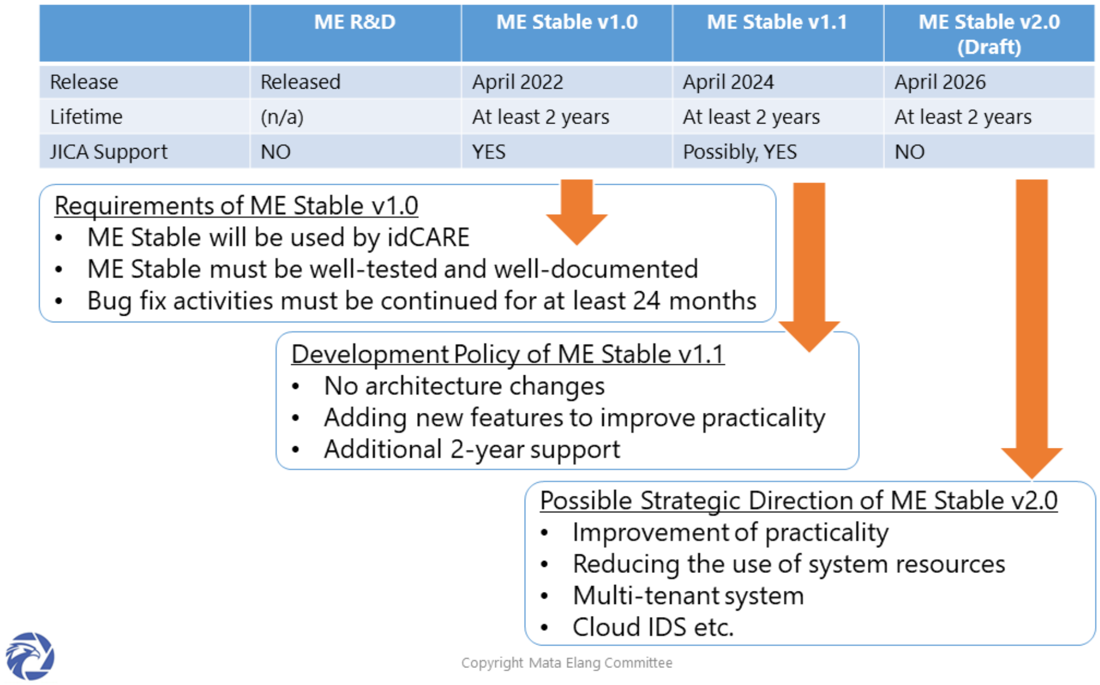
3.4.3. Writing Mata Elang Development RFP

1) Development Strategy of Mata Elang Stable version

Before starting the development of Mata Elang Stable, the strategy and its roadmap must be considered from a future perspective on ME.

In this activity, the roadmap for next five years was reviewed and three versions of ME Stable were proposed.

- Mata Elang Stable v1.0: Initial release of ME Stable
- Mata Elang Stable v1.1: New features release and performance improvement
- Mata Elang Stable v2.0: Comprehensive update of ME Stable



	ME R&D	ME Stable v1.0	ME Stable v1.1	ME Stable v2.0 (Draft)
Release	Released	April 2022	April 2024	April 2026
Lifetime	(n/a)	At least 2 years	At least 2 years	At least 2 years
JICA Support	NO	YES	Possibly, YES	NO

Requirements of ME Stable v1.0

- ME Stable will be used by idCARE
- ME Stable must be well-tested and well-documented
- Bug fix activities must be continued for at least 24 months

Development Policy of ME Stable v1.1

- No architecture changes
- Adding new features to improve practicality
- Additional 2-year support

Possible Strategic Direction of ME Stable v2.0

- Improvement of practicality
- Reducing the use of system resources
- Multi-tenant system
- Cloud IDS etc.

Copyright Mata Elang Committee

Figure 3-4 Strategy roadmap of Mata Elang (basics)

The following tables show the strategy roadmap from the perspective of Mata Elang functionality.

Table 3-8 Strategy roadmap of Mata Elang (Functions 1/2)

	ME R&D	ME Stable v1.0	ME Stable v2.0 or later (Draft)
IDS	Network IDS	Network IDS	Cloud IDS?
Data Collecting	MQTT	MQTT	Optimized MQTT?
Data Processing	Streaming Data Processing - Realtime Processing - Batch Data Aggregation	Streaming Data Processing - Realtime Processing	Distributed Streaming Data Processing?
Data Storage	Big Data Storage	Big Data Storage	Distributed Big Data Storage?
Search Engine	(n/a)	Data Aggregation	Data Aggregation
Dashboard	Simple Dashboard - Signature-base and protocol-base analysis - Time-series analysis	Customizable Dashboard - Signature-base and protocol-base analysis - Time-series analysis - Geographical analysis	Multi-Tenant Dashboard? Risk-Threat Analysis?

Table 3-9 Strategy roadmap of Mata Elang (Functions 2/2)

	ME R&D	ME Stable v1.0	ME Stable v2.0 or later (Draft)
Operation & Management	(n/a)	[Operation] ✓ Server Resource Monitoring ✓ Log Rotation	Functions of ME Stable v1.0 + [Management] ✓ Sensor Management ✓ User Management ✓ Rule Management [Notification] ✓ Incident Notification - e.g. High Severity Incident ✓ Anomaly Detection Alert - e.g. Change-point Detection [Data Analysis] ✓ Enrich Query for detail analysis ✓ Threat-intelligent for detail analysis [Visualization] ✓ Enrich Visualization [Inter-organizational Cooperation] ✓ STIX Format Support

More details regarding the development strategy are described in Appendix 14 "Strategy of Mata Elang Stable Development."

2) RFP for Mata Elang Stable 1.0

After the strategy and its roadmap were determined, the RFP of Mata Elang Stable 1.0 was written. For more details, refer to Appendix 15 "RFP Development of Mata Elang

Stable Version".

Following the strategy and roadmap of Mata Elang Stable, the scope of this development was focused on "Development," "Quality Improvement," and "Documentation."

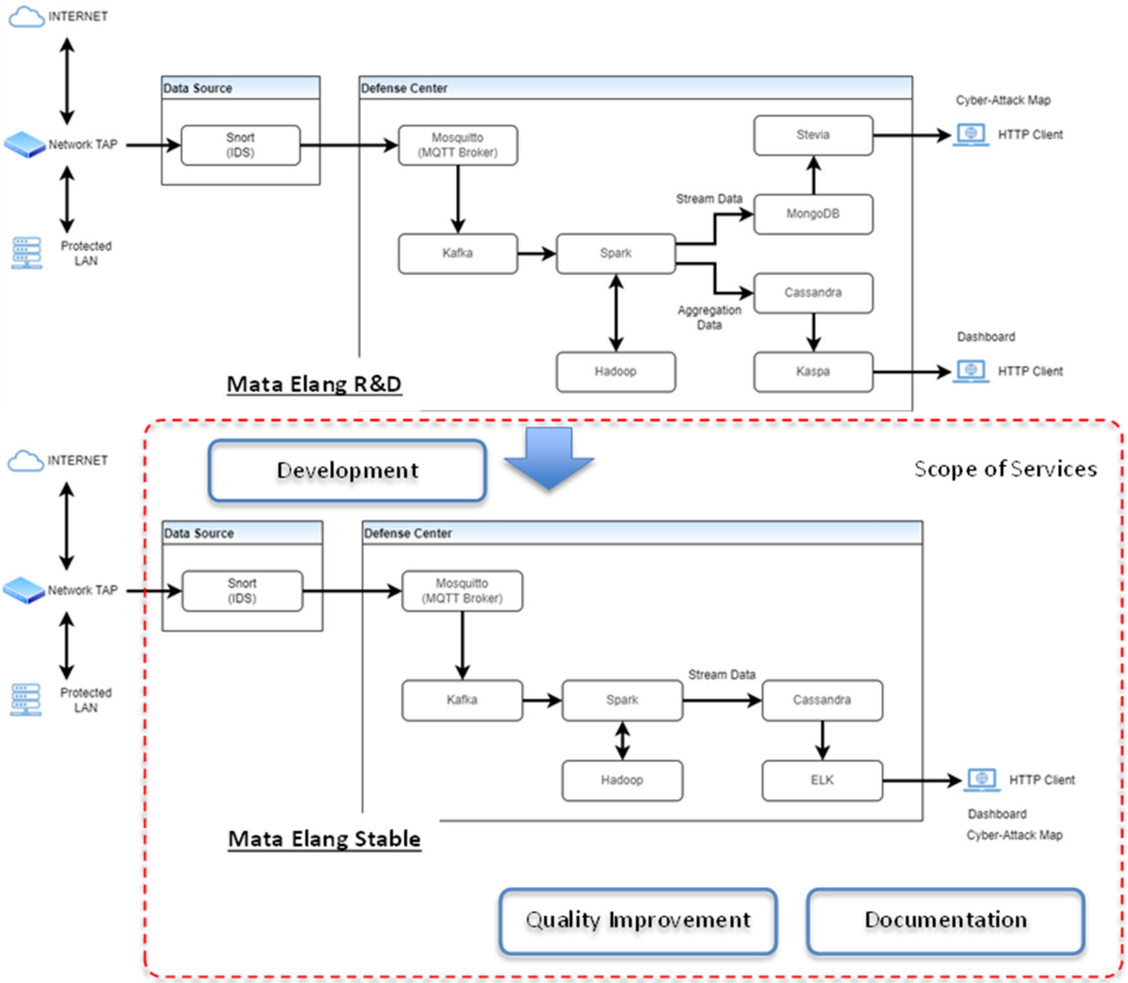


Figure 3-5 Scope of services of ME Stable 1.0 development

There are various requirements for the development of ME Stable. They are derived from the current issues in the study of ME. In the development of Stable 1.0, several requirements were selected as targets for this development, depending on its level and priority of needs. The selected requirement has a light-yellow background color.

Table 3-10 Requirements of Mata Elang Stable development

No	Requirement	Activity	Level, Priority
1	Test Requirements	Unit Testing	Mandatory
		System Testing	Mandatory

No	Requirement	Activity	Level, Priority
		Stability Testing	Mandatory
		Simulator Attack Testing	Mandatory
2	Documentation Requirements	Installation Manual	Optional, Priority High
		Configuration Settings	Optional, Priority High
		Developers' Guide	Optional, Priority High
3	Dashboard Implementation	Chart, Graph of Attack	Mandatory
		IP-Geolocation Map	Optional, Priority Middle
4	System Resource Monitoring	Resource Monitoring	Mandatory
		Notification to administrators	Mandatory
		Services Monitoring	Optional, Priority Middle
5	Log Rotation	Snort Log	Mandatory
6	Data Aggregation	Shift to Elasticsearch, Logstash, Kibana (ELK) platform	Mandatory
7	Repository Update	Updating contents on repositories	Optional, Priority High
8	Fixing the Version	Specifying versions at installation	Optional, Priority High
9	Eliminating Unnecessary Build Processes	To put parameters into external files and avoid unnecessary build	Optional, Priority High
10	Docker Containerization	Making of Docker images of Spark	Optional, Priority Middle
11	User Account Management	Making of a procedure to change account settings	Optional, Priority Middle
12	Implementation of Resource Update	Making of a procedure to download frequent update files	Optional, Priority Middle
13	Installation under Offline Environment	Creating installation media for offline environments	Optional, Priority Middle

No	Requirement	Activity	Level, Priority
14	Explanation for Security Issues	Adding explanation to avoid the known security issues	Optional, Priority Low
15	ARM CPU Support	Support for ARM CPU	Optional, Priority Low

3.4.4. Writing OSS Developers' Guide

1) Developers' Guide

To unify the development manner among various developers and improve the quality of the product, a "Developers' Guide" is essential for OSS development. Only the minimum requirements are defined here and will be updated from time to time according to the situation of the community.

For details, refer to "Developers' Guide Wiki" (https://github.com/mata-elang-stable/developersguide/wiki) or see Appendix 16 "OSS Developers Guide".

The following are the table of contents of the developers' guide.

Table 3-11 Table of contents of the developers guide

1 Overview
- Purpose of This Document
- Background
- Mata Elang Community

2 System Overview
- System Architecture
- System Configuration
- List of Products
- List of Port Numbers
- Memory Usage per Service

3 Development
- Development Policy
- Source Code Management
- Development Procedure
- Test Requirements
- Coding Standards
- License

4 Management

- Version Control
- Support and Quality Assurance
- Document Management

3.4.5. Writing Mata Elang Installation Manual

1) Installation Manual

To solve the issue #1 “The installation procedure of Mata Elang is not clear, and some information is missing” in “Table 3-4 Current issues of Mata Elang,” it is important to make the installation procedure clear and concise. Therefore, the installation manual was prepared on GitHub site.

Refer to “Installation Manual Wiki” (https://github.com/mata-elang-stable/mataelang-platform/wiki) or see Appendix 17 “Mata Elang Install Manual” for details.

The followings are the table of contents of the installation manual.

Table 3-12 Table of contents of the installation manual

1 Installation
- Time Zone and NTP
- Snort
- Defense Center
- Mosquitto
- Cassandra
- Hadoop
- Kafka
- Spark & KaspaCore
- ELK Dashboard
- Zabbix

2 Configurations
- Configurations

3 Others
- Operation Procedures
- Errors and Solutions

3.4.6. Improving OSS Community

1) Acceptance Testing

To assure the quality of Mata Elang Stable, the ME project planned to implement the acceptance testing. The planning procedure of an acceptance testing is as follows:

1. Test Planning (Purpose, Schedule, Roles, and Tasks)
2. Test Design (Test Scenario, Case, and Data)
3. Building Environments for Testing
4. Establishing Communication Rules
5. Test Execution
6. Quality Evaluation

In general, the acceptance testing is for a client to sign-off on the system development as satisfying the defined requirements. For ME project, the final check before publishing a new version is an acceptance testing. Through the acceptance testing, ME will be proven to be of the same quality as the market products.

Specifically, the acceptance testing will check the following viewpoints and items.

- ✓ Check whether the function and performance are satisfied according to the requirements.
- ✓ Check whether the usage and convenience throughout the entire operation are satisfied.
- ✓ Check whether the quality criteria are satisfied.
- ✓ Check the contract's acceptance criteria defined in the contract.

Table 3-13 List of test items for the acceptance testing

ID	Test Item
UAT001	Attacks are detected by sensors and displays it on the dashboard.
UAT002	Installation is successful using the source codes on GitHub and docker images on DockerHub according to the installation manual
UAT003	The test result report is submitted on time and approved by the client
UAT004	The completion report is submitted
UAT101	Count display of detected events within one hour
UAT102	Count display of detected events of each sensor today
UAT103	Latest event list with the function of pagination, sort, and filtering

ID	Test Item
UAT104	Overall hourly event count graph with the function of changing the target period
UAT105	Five (5) types of time-axis event count graph of each sensor and event list with the function of changing the target period and year-axis.
UAT106	Hour-axis integrated event count graph of each sensor with the function of changing the target period
UAT107	Top 20 event signature chart and event list by day with function of changing period
UAT108	Top 20 protocol chart and event list by day with function of changing period
UAT109	Event signature chart and event list by day/month/year with function of changing period
UAT110	IP source chart and event list by day/month/year with function of changing period
UAT111	IP destination chart and event list by day/month/year with function of changing period
UAT112	IP-Geolocation map and event list of IP source detected at recent one hour
UAT113	The system can monitor system resources such as CPU, memory, and disk usage
UAT114	The system can notify administrators when resource shortages are detected
UAT116	Snort log is retained for at least three (3) months
UAT117	Snort log will be automatically deleted after the retention period
UAT119	The ELK platform aggregates dashboard data
UAT120	Cron jobs are not required to aggregate data anymore
UAT901	The system runs continuously over 10 days without any termination
UAT902	No severe failures and issues for the operation are found during the above stability testing
UAT903	Concurrent attacks from two (2) sources are detected by sensors and displays them on the dashboard within one (1) minute
UAT904	The user interface is easy to use and understand
UAT905	Concurrent attacks from two (2) sources are detected by sensors and displays every attack on the dashboard.
UAT906	Attacks are detected by sensors and displays it consistently on the dashboard.

2) Mata Elang Workshop

To explain the new Mata Elang Stable 1.0 and implement the acceptance testing, the Mata Elang project held a workshop at PENS, Surabaya.

The outline of the workshop is as follows:

Date : 7-9 March 2022

Venue : C.307 Computer Network Room, PENS

Agenda :

Day 1: March 7, 13:00-17:00

- Brief Explanation of Mata Elang Stable 1.0
- Explanation of Acceptance Testing
- Mata Elang Stable Installation

Day 2: March 8, 9:00-17:00

- Mata Elang Stable Installation

Day 3: March 9, 9:00-12:00

- Simulator Attack Testing

Attendees : total 21 persons

- Two Lecturers from UI
- Two Assoc. Prof. and Two Senior Lecturers from PENS
- Project Manager of ME from PENS
- JICA Consultant of Software Quality Improvement
- Two representatives from Badan Siber dan Sandi Negara (BSSN)
- Six students and alumni from PENS
- Five representatives from ICT industry in Surabaya

At the workshop, after the explanation of new Mata Elang and question-and-answer session, participants installed ME as an acceptance testing and performed the simulator attack testing. At the conclusion of the workshop, we received the following comments and suggestions:

- ✓ Mata Elang functioned without any defects or issues.
- ✓ There is also no significant error in the documentation.
- ✓ Some of the cyber-attacks were not displayed properly due to implementation of snort.rules. This may need to improve.

- ✓ There is a problem regarding the system resources. Therefore, it is better to clarify the specifications of server resources.
- ✓ It is a good idea to write information about processes that take a long time.
- ✓ It would be better if the result of command execution is posted.
- ✓ It is recommended to add a description of getting an oink code used to download snort.rules.
- ✓ There was also a suggestion to clarify whether the installation user was the root user or the general user. But this suggestion was not applied to simplify the installation procedure.

4. CS COURSE DEVELOPMENT

4.1. Objectives, Critical points, Issues, and Countermeasures

Based on the situation and issues of the project and the analyzed critical points of the work, the objective, critical point, issue, and countermeasures of "CS Course Development" are summarized below:

Table 4-1 Activity indicators of "CS Course Development"

Item	Description
Objective	Establish the procedure of curriculum revision so that UI can continuously revise the curriculum in the future.
Critical point	Establishing a process for sustainable development and revision of the curriculum.
Issue	Curriculum development and revision methods have not been established.
Countermeasures for the issues	✓ Support the understanding of the human resources development framework in the cyber security field, which is the basis of the curriculum development in the project. ✓ Analyze the gaps between current curriculum and the latest CS human resources development framework. Then, confirm the completeness of knowledge and skills. ✓ Develop a curriculum revision manual and revision flow. ✓ Deliver a trial of curriculum revision, and then identify issues in the revision process and consider how to deal with them. ✓ If the necessity of establishing a new course is recognized in the process of trial, prepare a draft proposal for establishing a new course.

4.2. Activity Schedule

The activities "CS Course Development" were performed with the following schedule:

Table 4-2 Activity Schedule

Phase	Period	Target of Activities	Main Activities
1st Online	Sep-Nov 2021	• Project manager and vice manager	• Review the draft of curriculum revision manual

Phase	Period	Target of Activities	Main Activities
		• Center for Computing and Information Technology Fakultas Teknik Universitas Indonesia (CCIT-FTUI)	and flow • Meeting with CCIT-FTUI on curriculum revision
2nd On-site	Dec 2021	• CCIT-FTUI	• Training for CCIT-FTUI on curriculum revision
3rd On-site	Jan-Feb 2022	• Project manager and vice manager	• SecBoK / NICE workshop • Curriculum revision trial workshop

4.3. Activity Report

Some of planned on-site activities was replaced with online activities due to COVID-19. In addition, the 3rd on-site activity has been changed to a continuation activity from the 2nd on-site activity.

In this second phase, we performed the activity "Training for CCIT-FTUI on curriculum revision." This activity was not scheduled at the planning. However, the necessity of the training for CCIT-FTUI on curriculum revision was recognized in the implementation of the relevant activities.

4.3.1. Review the Draft of Curriculum Revision Manual and Flow

1) Purpose

This activity aims to establish the process of curriculum revision for keeping the curriculum up to date.

2) Meeting Overview

Date : 29 September 2021

Venue : Online meeting via Zoom

Agenda : Explanation of the draft of curriculum revision manual and flow

Attendees : Project Manager, Vice Project Manager, Chief Advisor, Project Coordinator, and JICA Consultant of CS Course Development (5 in total)

3) Details

The consultant proposed a curriculum revision process with following topics:

i. Methodology of curriculum revision by using Analysis, Design, Development, Implementation, and Evaluation (ADDIE) Instructional Design together with SecBoK and NICE framework
ii. Creating a work group of the curriculum revision
iii. Curriculum revision life cycle in line with the university level curriculum updates
iv. Introduction of five phases in ADDIE instructional design and Kirkpartick's model of evaluation
v. Introduction of Google Data Studio as an implementation method of Kirkpartick's model of evaluation
vi. Discussion on the curriculum revision flow

4) Output

The curriculum revision process was basically agreed. In particular, the systematic approach of existing curriculum evaluation by using Google Forms and Google Data Studio were accepted well.

There were some discussions on members of the work group and the life cycle of revision. As a result, a new position of curriculum advisor, who shall advise credit mapping between the idCARE program and master course program, is introduced.

5) Issues and Concerns

The life cycle of revision was not concluded within the meeting. It is agreed that the vice project manager check the proper information regarding university-level curriculum updates. The consultant proposed the cycle after she got the proper information.

4.3.2. Meeting with CCIT-FTUI on Curriculum Revision

1) Purpose

This activity aims to explain the duty of CCIT-FTUI in regard with the curriculum revision as well as to introduce a system on Google for the revision.

2) Meeting Overview

Date : 28 October 2021

Venue : Online meeting via Zoom

Agenda : Explanation of curriculum revision tasks on CCIT-FTUI

Attendees : Unit Leader of CCIT, Supervisor of CCIT, Technical Officer of CCIT, Project Coordinator, and JICA Consultant of CS Course Development (5 in total)

3) Details

The consultant explained and demonstrated the duty of CCIT by using Google Forms and Google Data Studio as below:

i. Collect feedback from students at the end of class
ii. Collect feedback from lecturers after the class
iii. Collect feedback from supervisors of students after 3-6 months of the class
iv. Record tests results with a spreadsheet on Google Drive after classes
v. Update the Google Forms file on request by cluster leaders
vi. Update the Google Data Studio after the update of Google Forms file or on demand of cluster leaders

The attendees then discussed the method of collecting questionnaire from supervisors, because it might be more difficult to reach supervisors than students. The agreed approaches are as follows:

i. Deliver the questionnaire for supervisors after 3-6 months of classes
ii. Marketing officers visit companies and help supervisors answer the questionnaire
iii. Target collection rate: 50 percent
iv. If it is required to add questions, use closed questions which is mostly preferred by supervisors

4) Output

The meeting went well. CCIT staff accepted their duties and learnt how to use the Google Forms and Google Data Studio to implement their tasks. It is also agreed to have a short training on the Google system before idCARE starts the regular classes.

5) Issues and Concerns

There are no issues with the meeting.

4.3.3. Training for CCIT-FTUI on Curriculum Revision

1) Purpose

This activity aims to train a member of CCIT-FTUI to operate the system for curriculum revision.

2) Overview

Date	: 10 December 2021
Venue	: JICA project office
Agenda	: Exercise on Google system for curriculum revision
Participants	: 1 (Unit leader of CCIT)
Instructor	: JICA Consultant of CS Course Development

3) Details

The unit leader updated the questionnaire on Google Forms and made the necessary update on Google Data Studio accordingly. She also handled several troubleshooting issues on Google Data Studio.

4) Output

The unit leader learnt the operation of Google Forms and Google Data Studio well.

5) Issues and Concerns

Technical staff of CCIT couldn't join the training. Hence, the unit leader needs to convey her experience to the technical staff. The technical staff is also requested to study the system well before the regular class starts.

4.3.4. SecBoK / NICE Workshop

1) Purpose

This activity aims to support the cluster leaders in understanding the human resources development framework in the field of cyber security. This is the basis of the idCARE curriculum development in the project.

2) Workshop Overview

Date & Time	: 20 January 2022, 9:00-11:30
Venue	: MRPQ Building, Depok Campus, University of Indonesia
Agenda	: Introduction of NICE Framework, SecBoK, and its usage in the project.
Participants	: 7
Instructor	: JICA Consultant of CS Course Development

3) Details

As a pre-requisite of the curriculum revision trial, the participants learnt the structure of framework, the latest update of the framework, usage of the framework in U.S and Japan, and how the framework, especially SecBoK, is used in the idCARE curriculum. The pre-test and post-test were prepared to monitor the achievement.

The program is as stated below.

i. What is the NICE Framework?
ii. How is the NICE Framework used in U.S?
iii. What is the SecBoK?
iv. How is the SecBoK used in Japan?
v. Usage of NICE Framework and SecBoK in the project
vi. Revision of NICE and SecBoK

4) Output

The workshop went smoothly. The participants did several exercises. The result of the post-test shows an average of 20 percent improvement compared to the pre-test, proving an improvement in their knowledge regarding NICE Framework and SecBoK.

Table 4-3 The evaluation of the workshop

Participant	Pre-test (20 points)	Post-test (20 points)
Yan Maraden	9 points	19 points
I Gde Dharma Nugraha	16 points	18points
Dodi Sudiana	17 points	18 points
Diyanatul Husna	13 points	N/A (Sick leave)
Ruki Harwahyu	14 points	17 points
Prima Dewi Purnamasari (Observer)	-	18 points
Muhammad Salman (Observer)	-	15 points

5) Issues and Concerns

There is no issue with the workshop.

4.3.5. Curriculum Revision Trial Workshop

1) Purpose

This activity aims to analyze the gaps between the current curriculum and the latest cyber security human resources development framework. Subsequently, the participants confirmed the completeness of knowledge and skills in the curriculum. In the exercises, the participants are expected to identify issues in the revision process and the possibility to establish new courses.

2) Workshop Overview

Date & Time: 20 January 2022, 11:30-16:30
21 January 2022, 9:00-11:30
Venue : MRPQ Building, Depok Campus, University of Indonesia
Agenda : Curriculum revision trial
Participants : 7 (7 on 20 January, 5 on 21 January)

Instructor : JICA Consultant of CS Course Development

3) Details

The curriculum revision manual and its flow are introduced. Participants learnt how to evaluate, analyze, design, develop, and implement the curriculum through exercises.

4) Output

The participants, mainly as cluster leaders, experienced the process of curriculum revision. Everyone actively participated in the program and had a lively discussion on the revision process.

In the result of exercises, there were three major outcomes:

a. Drafted proposals of two new courses
b. Drafted plans for training of trainers
c. Modification of curriculum revision manual

a. Drafted proposals of two new courses

The participants proposed two new courses, “Designing secure IoT system” (VAP00xxa) and “IoT Forensic” (FOR00xxa) as advanced level subject in CS Tech path. See Appendix 32 “Proposal for New Subjects” for details.

In the analysis phase of the curriculum revision, the participants found that there was an emerging trend of using IoT devices in the world, such as home IoT, medical IoT, etc. It causes significant increase of IoT attacks especially under the pandemic. The NIST, known world-wide for publishing technical standard/framework, published several documents for IoT security. Hence, the two courses are suggested to be in the curriculum.

b. Drafted plans for training of trainers

No updates were found on existing subjects during the trial. Therefore, “Training of Trainers” does not need to be delivered for the existing subjects.

Regarding the proposed new courses, a plan is drafted. See Appendix 33 “Plan of TTT” for details.

c. Modification of curriculum revision manual

There were several feedbacks on the revision manual.

1. Teaching materials should have a versioning scheme while at the development phase to avoid degradation.
2. Some questions are not clear or are missing.

The following is a list of modification made accordingly.

Table 4-4 List of modifications of curriculum revision manual

Item	Modification
0xxx_CurriculumUpdate Manual.docx	Added a note to use "manage versions" on Google Drive for versioning.
Appendix C. Worksheet for Curriculum revision.docx	1. Evaluation sheet a) Google Form URL and Google Data Studio URL are replaced for CCIT-owned URL after the form transition. b) Added a sentence to make the question clearer on "1.1 B)" 2. Questionnaire a) Questionnaire for students • Before: Nothing • After: "What do you find interesting about this course? (e.g., Topic of xxx, hands-on for xxx, instructors, facilities, and etc.)" b) Questionnaire for lecturers • Before: "Required resources are well defined" • After: "Required resources (HW/SW) to implement the course are well defined" c) Google Data Studio • Refresh data fields and set updated fields on Metric of the Evaluation Lev1 Lecturers Feedback - Material evaluation Refresh data fields and add a field on Dimension of the Analysis - Comments from Students

Item	Modification
Appendix F. Specifications of Revisions.xlsx	3. Added a column “Modification ID” for managing versions on Google Drive.

NOTE: Managing Versions

In default, Google Drive can do versioning only for 30 days or 100 versions. To store the previous versions properly, the following procedure is required.

1. On the file, click “More options” > “Manage versions” > “Keep forever”.

   (In other option, click the more options icon (kebab menu/three vertical dots) > “Manage versions” > “Upload new version”.)
2. Open the file and click “Last edit was xxx” to see the version history. Click “More options” > “Name this version” > put “Modification ID”. If required, click “Restore this version” under the version history.

5) Issues and Concerns

There is no issue with the trial workshop. However, the following concerns remain when it comes to the real curriculum revision process.

i. The group leader is expected to take strong leadership.

ii. Credit mapping between idCARE program and the master course program should be carefully checked by the curriculum advisor.

iii. Budget should be well prepared for the development and implementation phase.

5. INSTRUCTIONAL DESIGN

5.1. Objectives, Critical points, Issues, and Countermeasures

Based on the situation and issues of the project and the analyzed critical points of the work, the objectives, critical points, issues, and countermeasures of "Instructional Design" are summarized as below.

Table 5-1 Activity indicators of "Instructional Design"

Item	Description
Objective	Make the courses ready for opening by modifying and improving the custom courses developed in the project (9 courses in total) and conducting the lecturer training.
Critical points	✓ Modification and improvement of teaching materials based on instructional design ✓ Redesign courses to maximize online training for participation anytime, anywhere ✓ Prepare the training of lecturers related to CS education
Issues	✓ The quality of teaching materials is not efficient enough because it is not based on instructional design. ✓ Not all custom courses support online training and are severely affected by COVID-19. ✓ Although lecturer training for some courses has begun, the period, content, and participants are limited due to the influence of COVID-19.
Countermeasures for the issues	✓ Improvement of existing subjects by applying instructional design (including maximization of online delivery of learning) and implementation of lecturer training at the same time. ✓ Maximize the range of online lectures and establish a process that facilitates the cycle of analysis, design, development, implementation, and evaluation. ✓ Utilize local companies for content correction and lecturer training in each subject, with consultants evaluating the implementation status.

The nine custom courses are shown in the table below.

Table 5-2 Nine custom courses

ID	Title
CMP0010a	Comprehensive exercise: CSIRT
COM0010a	How to make the top management aware of cybersecurity
COM0020a	How to make general employees aware of cybersecurity
GOV0010a	Cybersecurity law and regulation
GOV0020a	Case Study and Practice: Supply-chain risk
FOR0010a	Case Study and Practice: Malware analysis
FOR0020a	Case Study and Practice: How to make IT system forensic-enabled
FOR0040a	Computer forensic
FOR0050a	Mobile device forensic

5.2. Activity Schedule

The activities under "Instructional Design" were performed with the following schedule:

Table 5-3 Activity Schedule

Phase	Period	Target of Activities	Main Activities
1st Online	Sep - Nov 2021	• Cluster leaders • Sub-contractor	• Conduct meeting with local sub-contractor for Work instruction • Develop training plan with UI and sub-contractor • Monitor the progress of revision and gain approval for revision • Implement the TTTs and mock lessons
2nd On-site	Dec 2021	• Cluster leaders • Sub-contractor	• Conduct meeting with sub-contractor for Work improvement • Monitor the progress of revision and gain approval for revision • Implement the TTTs and mock lessons • Inspect mid-term deliverables
3rd On-site	Jan - Feb 2022	• Cluster leaders • Sub-contractor	• Implement the TTTs and mock lessons

Phase	Period	Target of Activities	Main Activities
			• Conduct meeting with Sub-contractor for Knowledge, Skill, and Ability (KSA) mapping • Inspect final version of deliverables

5.3. Activity Report

5.3.1. Conduct meeting with local sub-contractor for Work instruction

1) Purpose

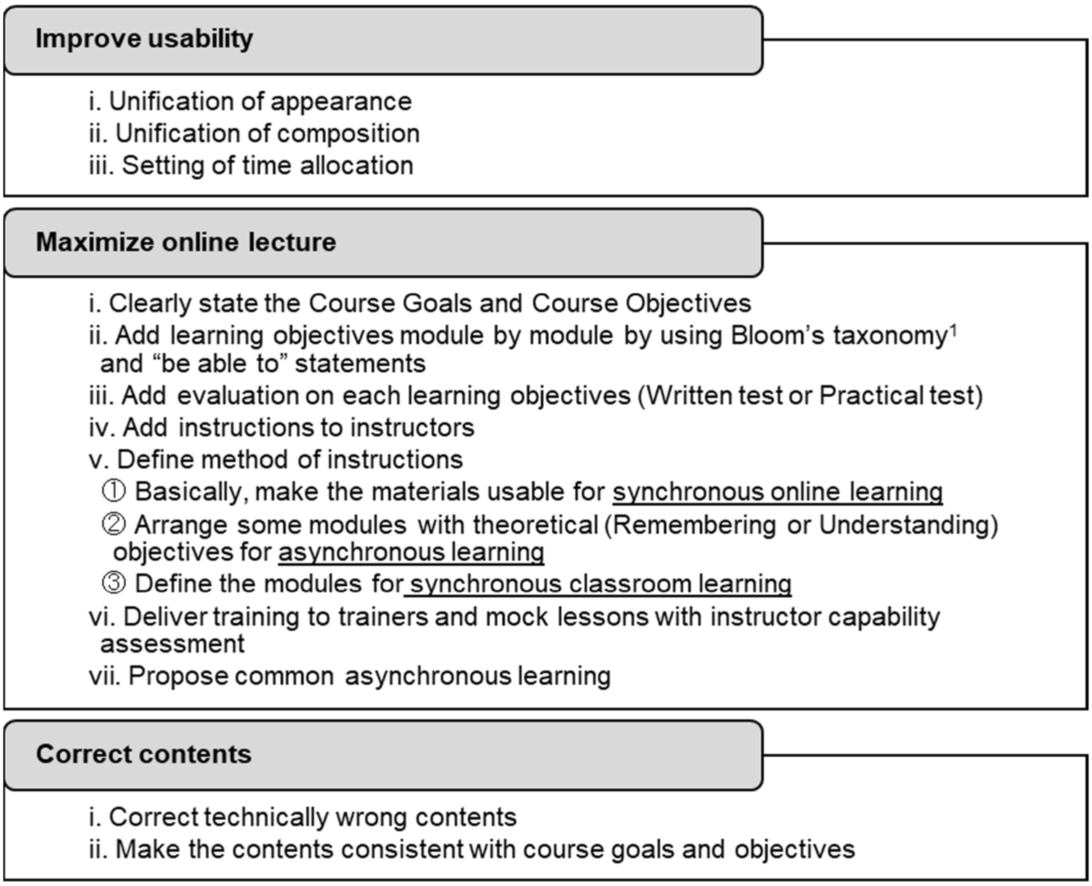
This activity aims to create a common understanding between the consultants and the local experts of the sub-contractor for the material revisions.

2) Meeting Overview

Date : 30 August 2021
Venue : Online meeting via Zoom
Agenda : Explanation of specification of revision
Overview of instructional design in line with the revision
Attendees : Sub-contractor team and consultant team (7 in total)

3) Details

The consultant defined a basic concept of revisions in line with the instructional design as indicated in Figure 5-1.



Improve usability

i. Unification of appearance
ii. Unification of composition
iii. Setting of time allocation

Maximize online lecture

i. Clearly state the Course Goals and Course Objectives
ii. Add learning objectives module by module by using Bloom's taxonomy[1] and "be able to" statements
iii. Add evaluation on each learning objectives (Written test or Practical test)
iv. Add instructions to instructors
v. Define method of instructions
① Basically, make the materials usable for synchronous online learning
② Arrange some modules with theoretical (Remembering or Understanding) objectives for asynchronous learning
③ Define the modules for synchronous classroom learning
vi. Deliver training to trainers and mock lessons with instructor capability assessment
vii. Propose common asynchronous learning

Correct contents

i. Correct technically wrong contents
ii. Make the contents consistent with course goals and objectives

Figure 5-1 Concept of Revisions

Along with the concept, the consultant prepared a form of Specifications of Revisions which describes a guideline of revision and detail direction of modifications. The guideline includes objectives, revision processes, and viewpoints of revisions such as instructional design, appearance integrity, and technical correctness (cybersecurity / instruction).

The consultant explained the form and key points of the revisions as follows.

i. Correct the appropriateness of word usage for "Course Goals" and "Course Objectives"
ii. Clarify learning objectives module by module
iii. Using verbs of Blooms' Taxonomy[1] for learning objectives
iv. Add pre- and post-test for each subject

[1] https://citt.ufl.edu/resources/the-learning-process/designing-the-learning-experience/blooms-taxonomy/

v. Add module tests, theoretical or practical, according to the module learning objectives

vi. Add instructions to instructors

4) Output

The local experts received instructions from the consultants as well as a form for continuous updating.

5) Issues and Concerns

There was no issue with the meeting.

5.3.2. Develop training plan with UI and sub-contractor

1) Purpose

This activity aims to create a common understanding between the consultants and the local experts for the material revisions. It also targets to develop a tentative plan of "Train the Trainers" (hereinafter referred to as TTT).

2) Meeting Overview

Date	: 14 September 2021
Venue	: Online meeting via Zoom
Agenda	: Discussion on specification of revision
	Discussion on training plan
Attendees	: Sub-contractor team and consultant team (7 in total).

3) Details

The consultants discussed with the local experts and gave feedback on the progress of revisions. The chief consultant added approaches of instructional design for better understanding of his direction of revisions.

The sub-contractor team and the consultant team discussed the timeframe of revision and the TTTs.

4) Output

The sub-contractor understood the requests from consultants. The specifications of revisions were updated accordingly.

The two teams developed a tentative plan of TTTs in the meeting. Afterwards, the deputy consultant adjusted the plan in line with the available schedule of instructors and the cluster leaders, respectively.

5) Issues and Concerns

There was no issue with the meeting.

5.3.3. Monitor the progress of revision and gain approval for revision

1) Purpose

This activity aims to make sure the works of sub-contractors are in line with the expectation of the consultants and the cluster leaders.

2) Task Overview

The consultants monitored the progress of the work in a hybrid manner through text-chat and video-chat. Periodical video meetings were held as detailed in Table 5-4 until the training started in November 2021. The deputy consultant followed up the revisions and set approval meetings with the cluster leaders.

3) Details

The "Specification of Revisions" was continuously updated with records of actions taken for each revision items. "Appearance Integrity" and "Technical Correctness" were also reviewed as the revision progressed. The chief consultant introduced a form of "Instructor Capability Assessment" for mock lessons.

Table 5-4 List of periodical meetings with the local experts

No	Date	Agenda	No. of Attendees
1	29 Sep 2021	Discussion for the revision details	8
2	12 Oct 2021	Discussion for the revision details	8

No	Date	Agenda	No. of Attendees
3	27 Oct 2021	Explanation of instructor capability assessment Discussion for the revision details	7

The revisions on each subject were approved by the cluster leaders before it was integrated for training as described below.

Table 5-5 List of revision approval meetings from Oct to Nov

Subject	Date	Status
FOR0020a: Case Study and Practice: How to make IT system forensic-enabled	18 Oct 2021	Basically approved, with few modifications requested by the cluster leader. It was subsequently approved after modifications were implemented.
GOV0010a: Cybersecurity law and regulation	22 Oct 2021	
COM0010a: How to make the top management aware of cybersecurity	29 Oct 2021	
FOR0010a: Case Study and Practice: Malware analysis	24 Nov 2021	

4) Output

Teaching materials modification on FOR0020a, GOV0010a, COM0010a, and FOR0010a were completed and approved subject by subject by the cluster leaders. Specifications of revisions were updated accordingly.

The local experts understood how to evaluate the TTT participants in mock lessons.

5) Issues and Concerns

There were difficulties in remote communication with cluster leaders to get approval of revisions. The deputy consultant received a lot of support from the project manager for this issue.

5.3.4. Implement the TTTs and mock lessons

1) Purpose

This activity aims to explain the updates of teaching materials to lecturers who have been in the previous training and to let the participants (future lecturers) demonstrate teaching the subject. Moreover, it aims to deliver five (5) full-size trainings, in response to the request of the project to the consultants to add five trainings for new lecturers who have never joined the subject training.

2) Training Overview

The trainings, including the five additional trainings, are delivered as indicated below.

Table 5-6 List of TTT delivery in November

No	Subject	Method	Planned Date	Delivery Date
1	FOR0020a Case Study and Practice: How to make IT system forensic-enabled	Online	1st week of Nov	1-5 Nov
2	GOV0010a: Cybersecurity law and regulation	Online	3rd week of Nov	9-11 Nov
3	GOV0010a: Cybersecurity law and regulation	Online	N/A (additional training)	15-17 Nov
4	COM0010a: How to make the top management aware of cybersecurity	Online	4th week of Nov	25-26 Nov

3) Details

Trainings were delivered in combination with the TTTs and the mock lessons. Participants for additional trainings were able to learn the entire contents of the subjects. The other training participants who previously underwent training were able to learn the new structure of materials and points of modifications.

In the TTT, participants were assessed through written (theoretical) and practical tests according to the module objectives.

In the mock lessons, participants were assessed on their capability to teach and instruct based the course. The consultant monitored the training (GOV0010a: Cybersecurity law and regulation) on 16 and 17 November 2021, and gave feedback to the participants and to the local experts afterwards.

4) Output

Completion reports and updated materials were submitted by the sub-contractor. The report includes the following topics:

i. Attendance
ii. Result of pre- and post-exams and module exams
iii. Result of practical skill assessment
iv. Result of Instructor capability check

5) Issues and Concerns

There were difficulties in confirming the attendance of participants and their participation during the online training. The instructor requested the participants to turn on their camera at the start of trainings. However, it didn't go well due to several reasons. The main issue was a weak network at participants' homes. However, there were also some participants who had other tasks to attend to at the same time while training.

5.3.5. Meeting with sub-contractor for work improvement

1) Purpose

This activity aims to meet the management team and the experts of the sub-contractor to hear the progress of their work and to request work improvement.

2) Meeting Overview

Date	: 15 December 2021
Venue	: Office of the sub-contractor
Agenda	: Report of work progress Discussion on issues found on expert's work

Attendees : Sub-contractor team and consultant team and the project coordinator (8 in total)

3) Details

The sub-contractor team reported the progress of their work. Due to areas needing improvement, the consultant team requested the sub-contractor to improve the quality of their output. The request includes the following issues.

i. The updated materials had many mistakes in English.

ii. The local experts modified the materials before reporting their plan to the consultants. It caused degradation in the material quality.

iii. Slow responses of the local experts towards the consultants or the cluster leaders. This caused delay on enhancement of the materials.

4) Output

The sub-contractor agreed to apply the following measures to address the consultant requests and areas of improvement.

i. The Director of the sub-contractor and the leading expert needs to check the English grammar of materials before submission.

ii. The experts write their plan on Specification of Revision and get approval before they start modification.

iii. The director supports communication between the local experts and the consultants.

5) Issues and Concerns

There was no issue with the visit.

5.3.6. Monitor the progress of revision and gain revision approval

1) Purpose

This activity aims to ensure the quality of revision required by the university.

2) Task Overview

The deputy-consultant followed up the updates of sub-contractors. She had set meetings with the cluster leaders and the local experts to get approval of changes before the training starts.

3) Details

Many online and offline meetings were held between the local experts and the deputy-consultant. Meetings for revision approval were also set online with the local experts and cluster leaders as described below.

Table 5-7 List of revision approval meetings in Dec

Subject	Date	Status
GOV0020a: Case Study and Practice: Supply-chain risk	22 Dec 2021	Basically approved with few modifications requested by the cluster leader. It was subsequently approved after the modifications were implemented.
COM0020a: How to make general employees aware of cybersecurity	22 Dec 2021	
FOR0040a: Computer forensic	23 Dec 2021	Many revisions were not approved. Follow-up meeting was requested.

At this point, the consultants and local experts discussed the modules for synchronous / asynchronous learning. It is agreed as detailed in Table 5-8.

Table 5-8 List of synchronous / asynchronous modules

Subject	Module for synchronous / asynchronous learning		
	Asynchronous (Pre-learning)	Synchronous (Online)	Synchronous (Classroom)
COM0010: How to make top managements aware of cybersecurity	Module 1	Module 2-6	
COM0020a How to make general employees aware of cybersecurity	Module 1, 2, 3	Module 4-8	

Subject	Module for synchronous / asynchronous learning		
	Asynchronous (Pre-learning)	Synchronous (Online)	Synchronous (Classroom)
GOV0010a: Cybersecurity law and regulation	Module 1, 2	Module 3-7	
GOV0020a: Case Study and Practice: Supply-chain risk	Module 1, 2	Module3-5	
CMP0010a: Comprehensive exercise: CSIRT	N/A	Module 4 (Module 1-3, 5-8)[2]	Module 1-3, 5-8
FOR0010a: Case Study and Practice: Malware analysis	N/A		Module 1-5
FOR0020a: Case Study and Practice: How to make IT system forensic-enabled	N/A	(Module 1-4)[2]	Module 0-4
FOR0040a: Computer forensic	N/A	Module 2,4	Module 1,3
FOR0050a: Mobile device forensic	N/A	Module 1-4, except lab preparation and practices	Module 1.5, Practices on Module 2, 3

4) Output

Many revision items were approved in this activity. As a result, teaching materials for GOV0020a and COM0020a were finalized. Specification of Revisions were updated accordingly. Furthermore, as a result of synchronous / asynchronous learning discussion, re-learning materials for asynchronous learning were developed.

[2] These modules could be delivered online only if the participants have enough experience and knowledge before the training.

5) Issues and Concerns

As a result of adding five trainings from the initial plan, the revision schedule became tighter and delayed, especially after some training had started. The deputy consultant frequently met with the sub-contractor and the cluster leaders in-person to follow up the revisions and approvals.

5.3.7. Implement the TTTs and mock lessons

1) Purpose

This activity aims to explain the updates of teaching materials to current lectures or to deliver full-size trainings to new lecturers.

2) Training Overview

The trainings, including the five additional trainings, were delivered as indicated below.

Table 5-9 List of TTT delivery in Dec

No	Subject	Method	Planned Date	Delivery Date
1	COM0010a: How to make the top management aware of cybersecurity	Online	N/A (additional training)	1-6 Dec
2	FOR0010a Case Study and Practice: Malware analysis	Offline	1st week of Dec	6-9 Dec
3	FOR0010a Case Study and Practice: Malware analysis	Offline	N/A (additional training)	13-20 Dec

3) Details

Trainings were delivered in combination with the TTT and the mock lessons. Participants for additional training were able to learn the entire contents of the subjects. The other training participants were also able to learn the new structure of materials and points of modifications.

Amongst the TTTs, two Forensic subjects were delivered offline with small number of participants due to COVID-19 restrictions. However, the mock lessons were held online to minimize the number of offline classes. The deputy consultant assisted and monitored the experts to deliver offline classes.

4) Output

Completion reports and updated materials were submitted from the sub-contractor.

5) Issues and Concerns

There were no issues with the training.

5.3.8. Inspect mid-term deliverables

1) Purpose

This activity aims to check the completion status of revisions and receive the completed training reports.

2) Task Overview

The sub-contractor submitted the mid-term report on 14 December 2021. The deputy consultant received and inspected the report and its attachment.

3) Details

The sub-contractor submitted the mid-term report with the following items:

i. Percentage of work completion subject by subject
ii. Status of implementation subject by subject
iii. TTT completion reports for GOV0010a, FOR0020a, and COM0010a. The completion reports include the revised teaching materials.

4) Output

Mid-term reports and teaching materials.

5) Issues and Concerns

There was no issue with the report.

5.3.9. Implement the TTTs and mock lessons

1) Purpose

This activity aims to explain the updates of teaching materials to current lectures or to deliver full-size trainings to new lecturers.

2) Training Overview

The trainings, including the five additional trainings, were delivered as indicated in Table 5-10.

Table 5-10 List of TTT delivery from Jan to Feb

No	Subject	Method	Planned Date	Delivery Date
1	FOR0040a: Computer forensic	Offline	4th week of Feb	10-13 Jan
2	COM0020a: How to make general employees aware of cybersecurity	Online	3rd week of Jan	17-19 Jan
3	GOV0020a: Case Study and Practice: Supply-chain risk	Online	4th week of Jan	24-25 Jan
4	FOR0040a: Computer forensic	Offline	N/A (additional training)	24-31 Jan
5	CMP0010a: Comprehensive exercise: CSIRT	Offline/ Online*	1st Week of Feb	3-10 Feb
6	FOR0050a: Mobile device forensic	Online*	1st Week of Mar	16-18 Feb
7	FOR0050a: Mobile device forensic	Offline	N/A (additional training)	21-24 Feb

* The training venue was changed due to COVID-19 cases at the university.

3) Details

a. Training implementation

Trainings were delivered in combination with the TTT and the mock lessons. Participants for additional trainings were able to learn the entire contents of the subjects. The other training participants also learned the new structure of materials and points of modifications.

The deputy consultant assisted and monitored the local experts to deliver offline classes. Moreover, the chief consultant monitored the training (FOR0040a: Computer forensic and COM0020a: How to make general employees aware of cybersecurity) on 17 and 24 January. Feedback was afterwards provided to the participants and to the sub-contractor.

b. Revision approvals

Approval of revisions on each subject were made simultaneously while other TTTs were on going. The list of approval meetings is indicated in Table 5-11.

Table 5-11 List of revision approval meetings from Jan to Feb

Subject	Date	Status
FOR0040a: Computer forensic	7 Jan 2022	Basically approved with few modifications requested by the cluster leader. It was subsequently approved after the modifications were implemented.
CMP0010a: Comprehensive exercise: CSIRT	14 Jan 2022	Many revisions were not approved. Follow-up meeting was requested.
CMP0010a: Comprehensive exercise: CSIRT	19 Jan 2022	Basically approved. Few modifications were requested by the Cluster leader. It was subsequently approved in the succeeding meetings after the modifications were implemented.

Subject	Date	Status
FOR0050a: Mobile device forensic	27 Jan 2022	Basically approved. Few modifications were requested by the Cluster leader. It was subsequently approved after the modifications were implemented.
CMP0010a: Comprehensive exercise: CSIRT	11 and 15 Feb 2022	Additional requests were made by the cluster leader. It was subsequently approved after the modifications were implemented.

c. Supplementary briefing session

The Cluster leader requested additional modifications on CMP0010a after the TTT. This is to make the materials more visually attractive and engaging for the students. Hence, the local experts modified the materials, followed by a supplementary briefing session on 17 February 2022.

4) Output

Completion reports and updated materials were submitted by the sub-contractor.

5) Issues and Concerns

The COVID-19 countermeasures were frequently changed. This affected the training schedule, especially for subjects which require offline instruction and exercises. Some trainings were re-scheduled while some had to reduce the number of participants.

For instance, “CMP0010a Comprehensive exercise: CSIRT” was planned to be delivered offline for the whole period of the class but was changed to online delivery from the second day. Some COVID-19 cases were reported at the campus after the first day of offline classes, resulting to campus closure on the second day. Originally, this subject is designed to be delivered offline or in physical face to face setting. However, this TTT was able to go online given the rich experience of the participants in CSRIT activities.

5.3.10. Meeting with Sub-contractor for KSA mapping

1) Purpose

This activity aims to solve conflicts of understanding between the local experts and the consultants regarding a map of SecBoK KSAs and idCARE program (revised materials).

2) Meeting Overview

Date	: 18 February 2022
Venue	: Office of sub-contractor
Agenda	: Clarify the rule of KSA mapping Review the updated KSA map by the experts
Attendees	: Sub-contractor team and the deputy consultant (4 in total)

3) Details

The mapping activity started before the meeting. However, there were misunderstandings between the local experts and the consultants. The meeting discussed critical points to resolve this.

Initially, the deputy consultant reminded the experts of the mapping criteria as below:

i. Map the KSAs and the subject, if the KSAs are taught in the class
ii. Exclude the KSAs required as pre-requisite

After which, the deputy consultant showed some examples to the local experts. The experts understood that they must remove the pre-requisite KSAs from the map.

Lastly, the local experts reviewed the mapped KSAs according to the criteria that was previously set.

4) Output

“SecBoK- idCARE program mapping” has been updated.

5) Issues and Concerns

The mapping process could not be completed on the day of meeting. The remaining part was updated by the local experts and submitted to the consultants. Afterwards, the consultants shared the map to cluster leaders and received their approval.

5.3.11. Inspect final version of deliverables

1) Purpose

This activity aims to inspect the deliverables and conclude the activity.

2) Task Overview

The sub-contractor submitted all the teaching materials and the completion report of TTTs. The consultants inspected the deliverables and accepted it.

3) Details

The consultants had checked the following points and shared the finalized materials to the project team.

i. Completeness of "Specifications of Revisions"
ii. Completeness of shared data
iii. Dead URL links on materials
iv. Copyright violation of materials

In addition to the acceptance of deliverables, the consultants determined the common learning topics among the nine subjects. It is proposed to develop pre-learning materials of common topics for the curriculum.

4) Output

The finalized materials were shred to the project team through Google Drive and an external hard disk storage. The external hard disk storage is used for the large-sized hands-on data.

The structure of materials is written on Appendix 52 "Structure of idCARE Materials."

Development of common pre-learning materials is also proposed. See Appendix 56 "Proposal for Common Pre-learning Materials" for details.

5) Issues and Concerns

While inspecting the URL links, the consultants found dead links on CMP0010a Module 4. It was an official demo site of open-source ticketing system, namely the OSTicket. The demo site was closed after the revision of materials. The local experts provided another demo site developed by CSIRT.ID. However, it is recommended to develop a demo site using OSTicket under the university environment to ensure continuous functionality.

6. ONLINE TRAINING AT ASCCE

6.1. Objectives, Issues, and Countermeasures

The objectives, issues, and countermeasures of "How to Make Top Managements Aware of Cyber Security" are summarized as below based on the request of the Project and the Cyber Security Agency of Singapore (CSA), the provider of the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) program.

Item	Description
Objectives	Deliver "How to Make Top Managements Aware of Cyber Security" course for the ASCCE program.
Issues	✓ Target audiences are slightly different from idCARE program. There will be no participants from private sectors. ✓ Impact on Financial Statement may not be relevant to the participants.
Countermeasures for the issues	✓ Introduce a framework by using "Public Policy in an Uncertain World: Analysis and Decisions by Charles F. Manski." It is for governance officials to predict the impact of cyber risks instead of the predicting the Impact on Financial Statement.

6.2. Activity Schedule

The activities "Online Training at ASCCE" were performed with the following schedule:

Period	Method	Activity
Nov 2021 - Apr 2022	Online	• Discussion with CSA. • Discussion among instructors and facilitators. • Training delivery.

6.3. Activity Report

6.3.1. Discussion with CSA

This activity aimed to determine the training expectations of CSA.

A short online meeting with CSA and Japanese stakeholders was held on 5 November 2021 to provide a briefing on the training of "How to Make Top Managements Aware of Cyber Security" and to hear CSA's requests. Detailed discussions were made through email correspondence.

Requests and responses are as follows:

Requests	Responses
Revise the course name to show the relevance to Critical Information Infrastructure Protection (CIIP).	Keep the course name as original to avoid any confusion as this course is same as the one in the UI.
Shorten or remove the section “Calculation of the Impact on Financial Statement” under Module 5. Because the target audience will be government officials, this topic might not be as relevant.	Modify the contents of module 5 and 6 based on the participants needs. Introduce "Public Policy in an Uncertain World: Analysis and Decisions by Charles F. Manski" to predict the impact of cyber risks.
Deliver the training in April. Preferably from 20 to 22 April.	The training shall be delivered as below. (UTC+8/SST) 27 April (Wed), 9am to 12pm and 1.30pm to 4pm 28 April (Thu), 9am to 12pm and 1.30pm to 4pm 29 April (Fri), 9am to 12pm

6.3.2. Discussion among instructors and facilitators

The consultant invited three instructors and three facilitators to deliver the online training. All of them have experience in developing this subject or has attended the training.

This training includes several group discussions using Zoom breakout rooms. Therefore, the facilitators need to lead discussions in a breakout room.

The main instructor explained the modified contents for ASCCE. After some discussions on the modification, it was finalized with some additional revision.

6.3.3. Training delivery

The training was delivered from 27 to 29 April with 12 participants (18 in plan) from five ASEAN countries.

7. RESULT OF ACTIVITIES

7.1. Software Quality Improvement

7.1.1. Achievements

The following are achievements of the activity “Software Quality Improvement.”

1) The OSS community “Mata Elang community” was established.

   The community is a society of ME users and developers. The community is a place for announcements and information exchange, and serves as a contact point for everyone interested in ME.

2) The committee “UI-PENS Mata Elang Steering Committee” was also defined and its initial members were assigned.

   The steering committee has a mission to release a stable version for their target users such as government, CII operators, and educational entities. The steering committee is also the decision maker for the strategy, release plan and the specifications of ME.

   The steering committee created a task list and started its activities immediately after its establishment. The committee is the central body for subsequent activities.

3) The distinction between Stable and R&D versions of ME was clarified.

   This clarified the role of ME Stable and the guidelines to make a development strategy for it. In addition, the interaction relationship between Stable and R&D versions were defined.

4) The strategy and the roadmap for the next five years of ME Stable were developed.

   This strategy provided an indicator for building an RFP for the development of ME Stable 1.0. The steering committee can consider the future development and release plan of ME by referring to this strategy.

5) The “Mata Elang Community Management Guidelines” was developed.

   This document defines the structure of the community as well as the roles of community, steering committee, and project, and its minimum rules. The steering committee member can perform basic management of the community and the steering committee by referring to this document.

6) The project “Mata Elang Stable Version” was launched under the supervision of the steering committee.

The project immediately started working as the responsible body for the development of the ME Stable and began to consider the ME development strategy as well as to develop the RFP for Stable 1.0 development.

7) The RFP "Development of Mata Elang Stable Version" was developed.

This RFP was immediately submitted to software development companies and the development of ME Stable 1.0 has started. The committee can use this RFP as a template for future development of the ME Stable.

8) The source code and Docker images were prepared.

Through the development of ME Stable, the source code on GitHub and Docker images on DockerHub were reviewed and the improved contents were prepared.

9) The ME Stable 1.0 was released.

In this version, the quality of the software as well as the features, response speed, useability, and stability of ME were improved.

10) The "Developers' Guide" was prepared.

"Developers' Guide" is a guidance for the developers who want to contribute to ME. It will be a book for unified development to ensure the software quality among the various developers and contributors.

11) The "Installation Manual" was updated and its quality was improved.

The improved manual reduced the difficulty of deploying ME and has the effect of encouraging the participation of the ME Community.

12) "Acceptance testing" was performed and the quality assurance method was introduced.

The acceptance testing ensured that ME Stable 1.0 didn't have a serious defect and proved that the quality of the software has improved. The project member will be able to perform the acceptance testing of Mata Elang Stable by referring to this material for the acceptance test.

13) ME workshop was held at PENS, Surabaya.

The workshop was a good opportunity to announce ME Stable version to the persons who are interested in the installation of OSS cybersecurity tools.

7.1.2. Result for Activity Indicator

Based on Table 3-1 Activity indicators of “Software Quality Improvement” the results of the activity “Software Quality Improvement” are described below.

Table 7-1 Results for activity indicator of “Software Quality Improvement”

Activity Indicator	Result
[Objective] Establish the system necessary to continuously release stable versions of the OSS tools that are being developed in the project	• The OSS community and the steering committee was established and started their activities. • The distinction between Stable and R&D versions of Mata Elang was clarified. • The steering committee crafted the development strategy of ME as well as the RFP. • The source code and Docker images of Mata Elang Stable were prepared and Mata Elang Stable 1.0 was released. • The “Acceptance testing” was performed through the workshop and the quality assurance method was introduced. • The “OSS Developers’ Guide” was prepared. This is a guidance for the developers who want to contribute to ME development. • The “Installation Manual” was updated and its quality
[Critical point] Establishing an open-source development system and improving quality	
[Issues] ✓ Open-source development is not formally organized. ✓ Open-source development rules are not documented. ✓ There is no definition of stable version of OSS tools and no quality management rules. ✓ Configurations are complicated and the manual is not ready for newcomers. ✓ There is no rule and no contact point for who is willing to join the OSS development.	
[Countermeasures for the issues] ✓ Build up an OSS development community and support its organizing process. ✓ Organize a quality assurance team within the community to help improve the quality of OSS tools. ✓ Develop support documents to help introduce OSS tools and promote the participation of other engineers to the community. ✓ Prepare an OSS tool development manual and guidelines that contains development rules.	

Activity Indicator	Result
✓ Clarify the distinction between stable and R&D versions of OSS tools and develop a plan for the continuous release of stable versions.	was improved for the persons who are interested in the installation of OSS cybersecurity tools.

7.2. CS Course Development

7.2.1. Achievements

As a result of this activity, cluster leaders and other group members of curriculum revision improved their knowledge on the NICE Framework and the SecBoK. They have also gained an ability to implement the Curriculum revision according to the developed manual and flow. The manual defines the following contents:

i. Target readers of the manual
ii. Curriculum revision work group
iii. Target image of human resources of cybersecurity professional program
iv. Cycle of curriculum revision
v. Transitional measures to the new curriculum
vi. Flow of the curriculum revision

The curriculum revision work group was developed under the idCARE program with members described in Table 7-2.

Table 7-2 Positions of curriculum revision work group

Position	Description
Group Owner	*Concurrent post of idCARE Manager* Review and authorize the updated curriculum
Group Leader	*Concurrent post of a cluster leader* Conduct the curriculum revision cycle
Curriculum Advisor	Advise credit mapping on the updated curriculum
CCIT Unit Leader (CCIT)	Collect feedbacks, disseminate new curriculum, and execute contracts with content developers when necessary
Framework Advisor	Advise on the latest cybersecurity work force framework

Position	Description
Commercial Course manager	*Concurrent post of a cluster leader* Share information of commercial course updates
Framework Manger	*Concurrent post of a cluster leader* Share information of framework updates
Cluster Leaders	Evaluate, Analyze, and Design the curriculum

The revision process, based on the curriculum revision manual, is shown in Figure 7-1.

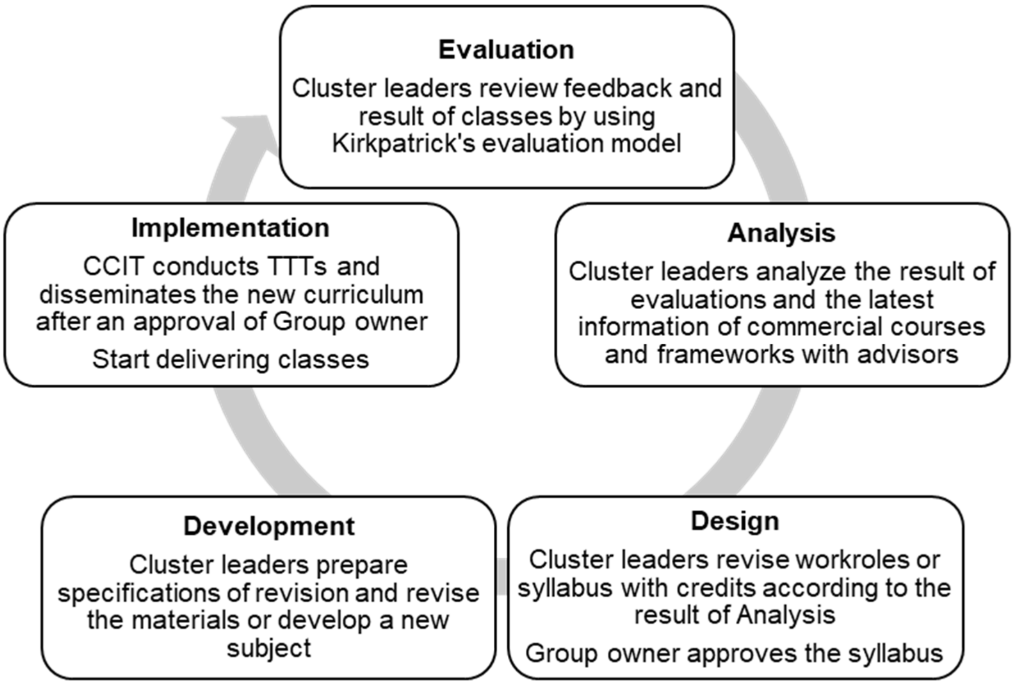

Evaluation
Cluster leaders review feedback and result of classes by using Kirkpatrick's evaluation model
Analysis
Cluster leaders analyze the result of evaluations and the latest information of commercial courses and frameworks with advisors
Design
Cluster leaders revise workroles or syllabus with credits according to the result of Analysis
Group owner approves the syllabus
Development
Cluster leaders prepare specifications of revision and revise the materials or develop a new subject
Implementation
CCIT conducts TTTs and disseminates the new curriculum after an approval of Group owner
Start delivering classes

Figure 7-1 Curriculum revision process

The achievements of each activity are indicated in Table 7-3.

Table 7-3 Achievement of activities and its output

No	Activity	Status	Achievement / Output
1	Understanding of the project and the details of curriculum development method	Done	Figured out existing curriculum development method and procedure. Created a slide to describe the method.
2	Examine the latest cybersecurity human resources development	Done	Prepared a learning material for the understanding of NICE and SecBoK. It includes the introduction of latest update

No	Activity	Status	Achievement / Output
	framework. Check the framework comprehension level of the cluster leaders.		and the use of the framework in the project. The latest framework “NICE rev1” has not been completed. Hence, the project needs to monitor the update to keep the curriculum up to date.
3	Develop curriculum revision manual and flow	Done	Proposed a curriculum revision process. It is approved by UI and the Chief advisor. See Appendix 31 “Curriculum Revision Manual”.
4	Map custom courses and SecBoK KSAs	Done	Appendix 31 “Curriculum Revision Manual - Appendix H. SecBoK-idCARE program mapping.xlsx” is updated according to the latest teaching materials.
5	SecBoK / NICE workshop and Curriculum revision trial workshop	Done	The workshop improved their knowledge regarding NICE Framework and SecBoK. The cluster leaders are able to implement the curriculum revision by referring to the manual.
6	Plan new curriculum briefing sessions and training	Done	The plan was drafted during the curriculum revision trial. The consultant arranged it for reporting. See Appendix 33 “Plan of TTT”.
7	Prepare proposal for new courses when necessary	Done	The proposal was drafted during the curriculum revision process. The consultant arranged it for reporting. See Appendix 32 “Proposal for New Subjects”.

7.2.2. Result for Activity Indicator

Based on Table 4-1 Activity indicators of “CS Course Development” the result of activity “CS Course Development” are described in Table 7-4.

Table 7-4 Results for activity indicator of "CS Course Development"

Activity Indicator	Result
[Objective] Establish the procedure of curriculum revision so that UI can continuously revise the curriculum in the future	• Learning material for NICE / SecBoK understanding were prepared and its workshop was held. • SecBoK-idCARE program mapping was updated according to the latest teaching materials. • Curriculum revision manual was developed and was approved by UI and the Chief Advisor. • The trial workshop of curriculum revision was held and the draft of a curriculum of new courses was proposed.
[Critical point] Establishing a process for sustainable development and revision of the curriculum	
[Issue] ✓ Curriculum development and revision methods have not been established.	
[Countermeasures for the issues] ✓ Support the understanding of the human resources development framework in the cyber security field, which is the basis of the curriculum development in the project. ✓ Analyze the gaps between current curriculum and the latest cyber security human resources development framework. Then, confirm the completeness of knowledge and skills. ✓ Develop a curriculum revision manual and revision flow. ✓ Deliver a trial of curriculum revision, and then identify issues in the revision process and consider how to deal with them. ✓ If the necessity of establishing a new course is recognized in the process of trial, prepare a draft proposal for establishing a new course.	

7.3. Instructional Design

7.3.1. Achievements

1) Revision of Teaching Materials

Teaching materials for the nine subjects were revised using specifications of revisions in line with the concept of revisions. A total of 167 items were identified and revised as indicated in Table 7-5.

Table 7-5 Breakdown of revision of teaching materials

Subject	Categories of revisions			Total
	Appearance Integrity	Instructional Design	Technical Correctness	
All subjects	6	8	2	16
COM0010a	2	6	1	9
COM0020a	0	12	3	15
GOV0010a	4	18	9	31
GOV0020a	1	2	3	6
FOR0010a	2	23	0	25
FOR0020a	2	5	3	10
FOR0040a	0	9	9	18
FOR0050a	1	8	4	13
CMP0010a	3	4	17	24
Total	21	95	51	167

As a result of the revision, pre-learning and online learning were defined for each method of delivery. Table 7-6 shows how much the trainings were transferred to the pre- and online learning.

Table 7-6 Result of online learning maximization

Subject	Hours by method of delivery			Total hours	Ratio of pre- and online learning
	Asynchronous (Pre-learning)	Synchronous (Online)	Synchronous (Classroom)		
COM0010a	1.5	12.5	0	14	100%
COM0020a	5.1	8.9	0	14	100%
GOV0010a	3.6	10.4	0	14	100%
GOV0020a	4.8	9.3	0	14	100%
FOR0010a	0	0	35	35	0%
FOR0020a	0	32.7	2.3	35	93%
FOR0040a	0	21.3	13.7	35	61%
FOR0050a	0	11.8	9.2	21	56%

Subject	Hours by method of delivery			Total hours	Ratio of pre- and online learning
	Asynchronous (Pre-learning)	Synchronous (Online)	Synchronous (Classroom)		
CMP0010a	0	4.1	30.9	35	12%

2) TTTs and mock lessons

A total of 105 participants joined TTT and learned the modifications on the teaching materials. The participants who got evaluations that are more than 70 percent on the post-tests and more than 50 percent on mock lessons were determined as eligible to be a lecturer. About 6 out of 10 participants were determined as eligible lecturers.

On the other hand, the participants who were not able to meet the criteria were determined either as assistant lecturers or as not eligible to be a lecturer depending on their performance while participating in the training. There were some participants who have not taken the post-test or mock lessons. Hence, the instructor could not finalize their evaluation and the result is stated as N/A (Not Applicable).

Table 7-7 Result of TTTs and Mock lessons

Subject Code	Period	Number of participants	Result of eligibility to be lecturers			
			Lecturers	Assistant lecturers	Not Eligible	N/A
FOR0020a	1-5 Nov	8	**4**	-	-	4
GOV0010a	9-11 Nov	9	**3**	1	-	5
GOV0010a*	15-17 Nov	7	**7**	-	-	-
COM0010a	25-26 Nov	8	**4**	1	-	3
COM0010a*	1-6 Dec	8	**7**	-	-	1
FOR0010a	6-9 Dec	4	**1**	-	-	3
FOR0010a*	13-20 Dec	5	**3**	2	-	-
FOR0040a	10-13 Jan	5	**3**	-	-	2
COM0020a	17-19 Jan	9	**8**	-	-	1
GOV0020a	24-25 Jan	10	**2**	2	-	6
FOR0040a*	24-31 Jan	13	**10**	2	1	-
CMP0010a	3-10 Feb	10	**6**	1	1	2
FOR0050a	16-18 Feb	4	**2**	1	-	1
FOR0050a*	21-24 Feb	5	**3**	2	-	-

Subject Code	Period	Number of participants	Result of eligibility to be lecturers			
			Lecturers	Assistant lecturers	Not Eligible	N/A
Total	55 days	105	**63**	12	2	28

*Additional trainings

7.3.2. Result for Activity Indicator

Based on Table 5-1 Activity indicators of "Instructional Design" the result of activity "Instructional Design" are described below.

Table 7-8 Results for activity indicator of "Instructional Design"

Activity Indicator	Result
[Objective] Make the courses ready for opening by modifying and improving the custom courses developed in the project (nine courses in total) and conducting the lecturer training.	• Teaching Materials were revised according to the instructional design. • TTT and mock lessons were held a total of 16 times for 55 days. A total of 63 lecturers are determined as ready to begin conducting the lectures. • A technical meeting for the redesign of courses to maximize online training was held with sub-contractor and cyber security and pre-learning materials for asynchronous learning were developed.
[Critical points] ✓ Modify and improve teaching materials based on instructional design ✓ Redesign courses to maximize online training for participation anytime, anywhere ✓ Prepare the training of lecturers related to CS education	
[Issues] ✓ The quality of teaching materials is not efficient enough because it is not based on instructional design. ✓ Not all custom courses support online training and are severely affected by COVID-19. ✓ Although lecturer training for some courses has begun, the period, content, and participants are limited due to the influence of COVID-19.	

Activity Indicator	Result
[Countermeasures for the issues] ✓ Improvement of existing subjects by applying instructional design (including maximization of online delivery of learning) and implementation of lecturer training at the same time. ✓ Maximize the range of online lectures and establish a process that facilitates the cycle of analysis, design, development, implementation, and evaluation. ✓ Utilize local companies for content correction and lecturer training in each subject, with consultants evaluating the implementation status.	

7.4. Online Training at ASCCE

There were 10 out of 12 participants who have completed the training and understood how to make top-management aware of cybersecurity.

Although some participants came in and went out during the training, the average test score increased from 76.67/200 on the pre-test to 118/200 on the post-test.

The Materials of Module 5 and 6 were modified according to the requests from CSA. See Appendix 71 “Module 5 of How to Make Top Managements Aware of Cybersecurity for ASCCE” and Appendix 72 “Module 6 of How to Make Top Managements Aware of Cybersecurity for ASCCE” for details.

8. LESSONS LEARNED / RECOMMENDATIONS

8.1. Software Quality Improvement

8.1.1. Mata Elang Community and Steering Committee

1) Participation of a person who has experience in software engineering

Managing OSS development is difficult because the group of participants are volunteers, and are not business-oriented.

In OSS software development, various type of software developers and contributors are gathered to collaborate with each other. Their technical skills and professional background also vary.

Therefore, in order to maintain united development rules and software quality, a certain amount of experience in software development management is required.

Well-managed OSS development requires the participation of someone with experience in software engineering and software development management.

2) Assignment of core software engineers to the community activity

To progress in OSS development, regardless of the size of a project, the participation of a person who will become the core to the development and be able to allocate a certain amount of working hours to the project is necessary.

It is highly recommended to assign a person as a core software engineer under the responsibility of the steering committee.

3) Expansion of Mata Elang community

It is necessary to promote the use of Mata Elang and expand the ME community.

Expansion of the ME community will bring in many software developers and contributors and will make the community autonomous and sustainable.

The ME workshop at PENS was a good opportunity to promote Mata Elang to the public. It is recommended to hold several similar workshops in other regions. For example, it is possible to hold a ME introduction seminar at the same time as the promotion seminar of the idCARE program.

8.1.2. Mata Elang Stable version

1) Deployment to the real network environments

Mata Elang has been used in experimental network environments. However, there was not enough experience of running it in real network environments and of analyzing real network traffic.

Therefore, through the first running test under real network environments, it was determined that necessary functions such as IPv6 analysis were not yet implemented.

From the viewpoint of verifying the practicality and stability of ME, the long-term operation of ME in a real network environment is indispensable. The ME deployment in DTE should be completed before the next development of ME Stable.

2) Development of Mata Elang Stable 1.1

The development of Stable 1.0 had a time-restriction due to the budget execution. Therefore, there is still a positive demand in the community for the subsequent development of Stable 1.1.

The expected requirements to develop Mata Elang Stable 1.1 are the following:

- ✓ Analysis function of IP v6 traffic
- ✓ Applying Snortv3 (Adopting new features of Snort v3 and improving performance)
- ✓ Further improvement of stability regarding the long-term operation of ME
- ✓ Analysis support function of raw data of network event
- ✓ Completion of the remaining requirements deferred in Mata Elang Stable 1.0

At this time, these requirements were also identified as the weak points of the current Mata Elang Stable version.

3) Proposal of software development model for Stable 1.1

There are some difficulties and risks for software development of Mata Elang Stable 1.1. These depend on the state of study and preparation before the start of development.

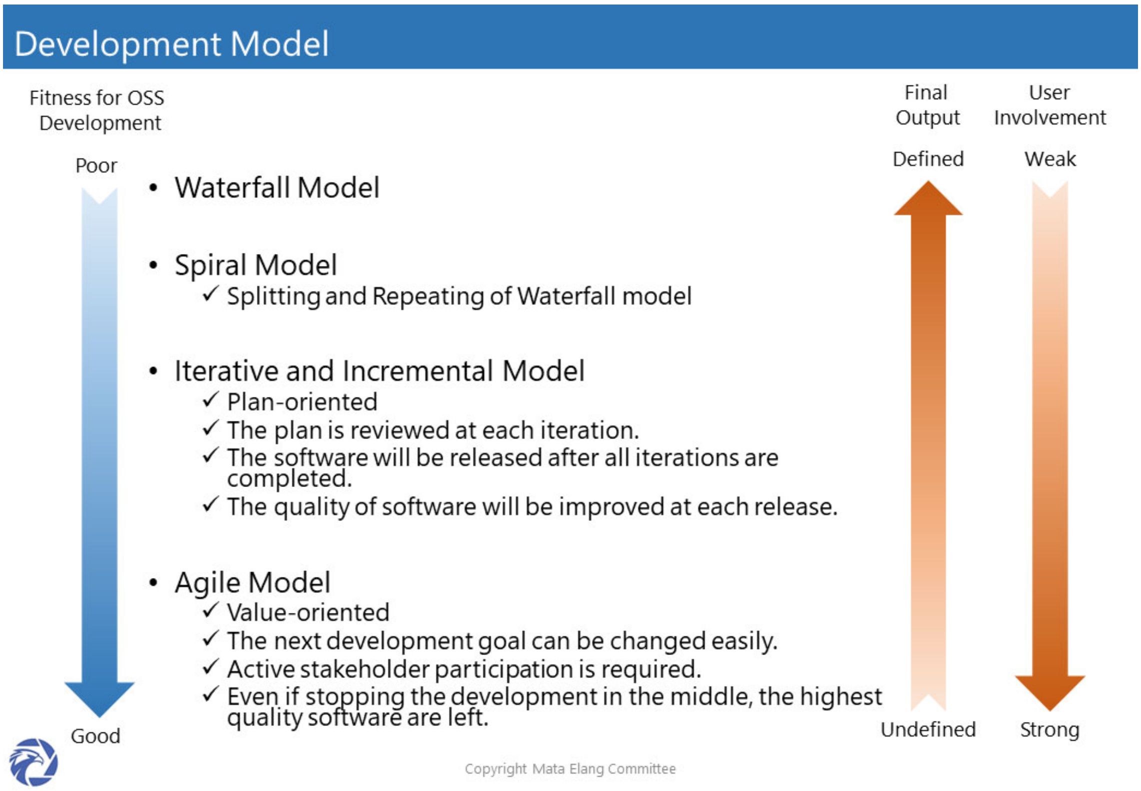
Table 8-1 The difference in condition between Stable 1.0 and Stable 1.1

Item	Stable 1.0	Stable 1.1
Source code	Already exists	Does not exist on GitHub
Preliminary study	Sufficient preliminary study could be done in advance	Due to the lack of source code, sufficient preliminary study is difficult.
Involvement of project leader	The leader could allocate a certain amount of time.	Lower level of involvement of the leader will be expected
Quality management	Weak	Depends on the software development company
Participation of full-time professional engineers	None. Participation was only as a voluntary activity or side business	Depends on software development company

The Mata Elang study team at PENS has the knowledge and strong motivation for development of Stable 1.1. However, the strong advantages seen in the development of Stable 1.0 cannot be expected.

To address the identified risks, difficulties, and disadvantage, compared to Stable 1.0, the development structure of Mata Elang Stable needs to be considered.

Figure 8-1 OSS software development model shows the representative software development models.



Development Model

- Waterfall Model
- Spiral Model
  - ✓ Splitting and Repeating of Waterfall model
- Iterative and Incremental Model
  - ✓ Plan-oriented
  - ✓ The plan is reviewed at each iteration.
  - ✓ The software will be released after all iterations are completed.
  - ✓ The quality of software will be improved at each release.
- Agile Model
  - ✓ Value-oriented
  - ✓ The next development goal can be changed easily.
  - ✓ Active stakeholder participation is required.
  - ✓ Even if stopping the development in the middle, the highest quality software are left.

Figure 8-1 OSS software development model

The "Agile Model" is the most suitable model for OSS development. However, the goal of the development is undefined and unclear. This model also requires frequent user involvement during the development process.

Therefore, for the next development, it is recommended to adopt the second most suitable model, the "Interactive and Incremental Model". This model still requires user involvement but development goals are somewhat more manageable.

In particular, this model has several iteration phases for the project goal, checking the output at each iteration, and providing feedback to the software developer.

Table 8-2 shows the responsibility of each stakeholder in "Interactive and Incremental Model"

Table 8-2 The responsibility of each stakeholder at next development

Stakeholder	Planning Phase	Development Phase	Testing Phase
ME Steering Committee as User	✓ Determination of requirements ✓ Approval of RFP	✓ Participation in a progress meeting ✓ Responding to questions from the developer	✓ Acceptance test
Consultant as Client	✓ Writing RFP ✓ Procurement of software developer	✓ Project management ✓ Holding a progress meeting	✓ Acceptance test
Software Developer		✓ Software development ✓ Project management ✓ Quality management ✓ Participation in a regular meeting	✓ Support for the acceptance test

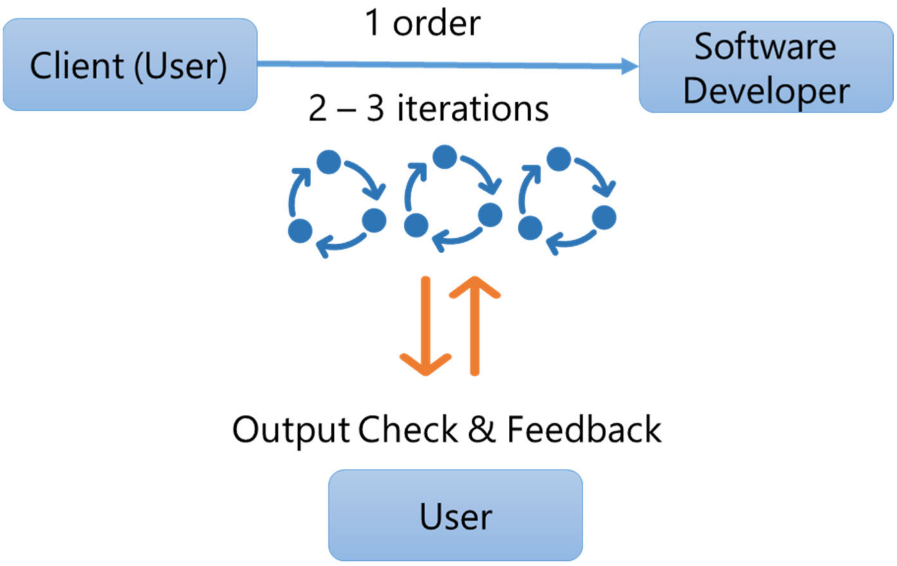


Figure 8-2 Interactive and Incremental Model

8.2. CS Course Development

8.2.1. Proposal for New Subjects

In the curriculum revision trial, two new courses, "Designing secure Internet of Things (IoT) system" (VAP00xxa) and "IoT Forensic" (FOR00xxa) are proposed. The two proposals were made because of significant increase of IoT attacks along with emerging trend of using IoT devices. It is proposed to be added in CS Tech Path during the trial. However, IoT security is more challenging than cybersecurity due to its enormous attack surface and the increased vulnerability of IoT devices. Hence, it is suggested to have an option of new program pathway for IoT with more subjects from basic to advance. See Appendix 32 "Proposal for New Subjects" for details.

8.2.2. Feasible Curriculum Revision

Considering the feasibility of the curriculum revision process, the following are recommended:

1) Human resources

✓ CCIT-FTUI and the cluster leaders are currently not communicating regularly. It is recommended to have a close relationship among them to continuously update the curriculum.

✓ However, the cluster leaders may not have sufficient time due to their regular workload. With that, the group owner is expected to support cluster leaders to manage their assignments from the department or faculty.

✓ The technical staff of CCIT could not join the training. Hence, the unit leader needs to convey her experience to the technical staff. The technical staff is also encouraged to study the system well before the regular class starts.

2) Finance

✓ It is suggested to estimate the income of idCARE program to consider budget allocation for curriculum revision. In this context, CCIT-FTUI and UI needs to develop an annual plan for classes. The plan is required to define the budget for development of new subjects or existing subjects as well as the training of trainers.

3) Operation

- ✓ If the new course is proposed while the curriculum revision process is ongoing, feasibility should also be considered. Budget, program path, and existing plan of classes should be examined before developing the course.

8.3. Instructional Design

8.3.1. Proposal for Common Pre-learning Materials

Throughout the activities, common topics were found in the existing courses. It is also found that international standard like NIST Frameworks were not understood well. It is recommended to develop four pre-learning materials to reduce overlap of materials and to improve prerequisite knowledge of the students.

1) Common Cyberattacks and Malwares
2) Basis of Information Security
3) Introduction of NIST Frameworks
4) NICE Framework / SecBoK

See Appendix 56 "Proposal for Common Pre-learning Materials" for details.

8.3.2. Reference for learning Assembly for Malware Analysis

While the TTT of "FOR0010a Malware Analysis", some TTT participants requested the consultants to provide reference to study the assembly language at their own pace or for self-study. It is proposed to study the basic topics on "The Art of 64-bit assembly, Volume 1". There is recommendation of topics for fast learning. See Appendix 57 "Reference for Learning Assembly for Malware Analysis" for details.

The idCARE manager should notify the subject applicants of this reference book for learning the assembly language in advance along with the syllabus.

8.3.3. Keep Effectiveness of the Curriculum

Given the effectiveness of the training, the following recommendations are made:

1) Human resources

- ✓ In the TTT, there were several participants who have not completed their duties, such as taking tests and delivering mock lessons. It is difficult to force the participants to take the tests especially while the online instruction is ongoing. We recommend the screening of participants before and after the TTT to see if they are the persons who can fulfill the duties in the idCARE program.

2) Operation

- ✓ The cluster leaders should carefully check the feedback from students and lecturers especially in its first year of regular class operation. Moreover, after the completion of some TTTs of the custom course, for example in 2023, the idCARE manager should hold some cluster meetings to collect active feedback from the lecturers and analyze data of the feedback collection system of idCARE program. Depending on the result of feedback analysis, some topics may need to be enriched or reorganized.

8.4. Online Training at ASCCE

It is suggested to allocate facilitators and timekeeper with enough experience for the third country training.

It is also suggested to extend the duration of training/discussions to ease difficulties of interactive training by online especially when the background of participants is varied. Suggestions are as below.

- ✓ Add 30 more minutes for discussions on module 3, 4, 5, and 6 respectively.
- ✓ Add 30 minutes at the beginning of the training to break the ice and develop rapport among lecturers and participants.
- ✓ Ground rules should be prepared well. See Appendix 73 "Online Training Ground Rules" used for this online training.
- ✓ Prepare report templates with hints.

9. APPENDICES

The appendices are as follow:

1) Appendix 1x – 2x: Software Quality Improvement

- Appendix 11 Mata Elang Community Management Guidelines
- Appendix 12 Mata Elang Community Member List
- Appendix 13 Mata Elang Committee Task List
- Appendix 14 Strategy of Mata Elang Stable Development
- Appendix 15 RFP: Development of Mata Elang Stable Version
- Appendix 16 OSS Developers Guide (*)

  Refer to: https://github.com/mata-elang-stable/developersguide/wiki
- Appendix 17 Mata Elang Install Manual (*)

  Refer to: https://github.com/mata-elang-stable/mataelang-platform/wiki
- Appendix 18 Workshop: Mata Elang Acceptance Testing
- Appendix 19 Test Cases of Mata Elang Acceptance Testing
- Appendix 20 Workshop Attendees List
- Appendix 21 Certificate of Handover

2) Appendix 3x: CS Course Development

- Appendix 31 Curriculum Revision Manual
  - 0xxx_CurriculumUpdate Manual.docx
  - Appendix A. Curriculum revision work group orgchart.svg
  - Appendix B. Curriculum revision flow.svg
  - Appendix C. Worksheet for Curriculum revision.docx
  - Appendix D Subject Structure.xlsx
  - Appendix E. Program Pathway.pptx
  - Appendix F. Specifications of Revisions.xlsx
  - Appendix G. Proposal for a new Subject_template.docx
  - Appendix H. SecBoK- idCARE program mapping.xlsx

- Appendix 32 Proposal for New Subjects
- Appendix 33 Plan of TTT (for New Subjects)

3) Appendix 5x: Instructional Design

- Appendix 51 Teaching Materials of nine CS Custom Courses (*)

  Refer to: “Teaching Materials Portable SSD Storage” or

  https://drive.google.com/drive/folders/1BJYH2EdTDMtLmEf-Pdz7aKENZkD0QNqX?usp=sharing.

  - Syllabus
  - Teaching Materials
    - Students Guide
    - Instructor Guide
    - Hands on Guide
    - Hands on Data
  - Tests
  - Template of Slides and Documents
- Appendix 52 Structure of idCARE Materials
- Appendix 53 Specifications of Teaching Material Revision
- Appendix 54 Plan of TTT
- Appendix 55 Completion Report of TTT
- Appendix 56 Proposal for Common Pre-learning Materials
- Appendix 57 Reference for Learning Assembly for Malware Analysis
- Appendix 58 Instructor Capabilities Check Sheet

4) Appendix 6x: Contract Documents

- Appendix 61 RFP “Material enhancement and Training of trainers of Cybersecurity training courses”
- Appendix 62 Service Contract of “Material enhancement and Training of trainers of Cybersecurity training courses”
- Appendix 63 Service Contract of “Additional Training of trainers of Cybersecurity

training courses"

5) Appendix 7x: Online Training at ASCCE

- Appendix 71 Module 5 of "How to Make Top Managements Aware of Cybersecurity" for ASCCE
- Appendix 72 Module 6 of "How to Make Top Managements Aware of Cybersecurity" for ASCCE
- Appendix 73 Online Training Ground Rules
- Appendix 74 Attendance List of COM0010a for ASCCE