MONGOLIA

MINISTRY OF DIGITAL DEVELOPMENT AND COMMUNICATIONS (MDDC),

SCHOOL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY OF THE MONGOLIA UNIVERSITY OF SCIENCE AND TECHNOLOGY (MUST-SICT),

NATIONAL ACADEMY OF GOVERNANCE (NAoG)

MONGOLIA

PROJECT FOR DEVELOPMENT OF HUMAN RESOURCES IN CYBER SECURITY (TRAIN-THE-TRAINERS/ CYBERSECURITY)

WORK COMPLETION REPORT

MAY 2023

JAPAN INTERNATIONAL COOPERATION AGENCY

TOKYO CO., Ltd.

GP
JR
23-016

Photos

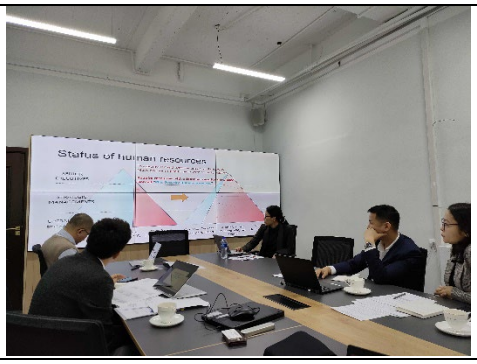
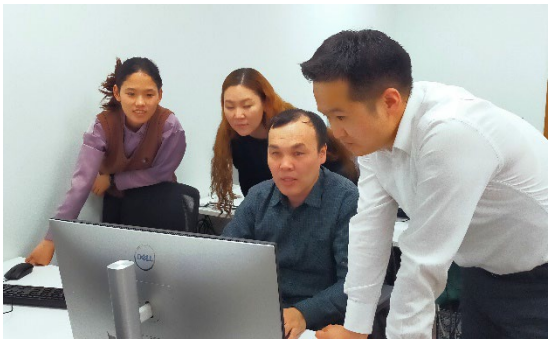
Briefing sessions with MDDC	
	
Briefing for the Cybersecurity Policy Coordination Department (MDDC, 27th Jan 2023)	Project Kickoff Meeting (MDDC, 2nd Feb 2023)
Train The Trainers	
	
Cybersecurity Awareness TTT (MUST-SICT, 6th Feb 2023)	Computer Forensic TTT (MUST-SICT, 13th Mar 2023)

Table of Contents

Appendices

List of Tables

List of Figures

Abbreviations

Abbreviations	Definitions
ACM	Association for Computing Machinery
BSSN	Badan Siber dan Sandi Negara (National Cyber and Crypto Agency)
C/P	Counterpart
CEH	Certified Ethical Hacker
CII	Critical Information Infrastructure
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CPLMs	Common Pre-Learning Materials
CS	Cyber Security
CSEC	Cybersecurity Curricular Guidelines
CSIRT	Computer Security Incident Response Team
EU	European Union
ID-SIRTII/CC	Indonesia Security Incident Response Team on Internet Infrastructure coordination center
IPA	Information-technology Promotion Agency
IT	Information Technology
JCIC	Japan Cybersecurity Innovation Committee
JICA	Japan International Cooperation Agency
KOMINFO	Kementerian Komunikasi dan Informatika (Ministry of Communication and Information Technology, Indonesia)
KSA	Knowledge, Skill, and Ability
MDDC	Ministry of Digital Development and Communications
METI	Ministry of Economy, Trade and Industry
MEXT	Ministry of Education, Culture, Sports, Science and Technology
MIC	Ministry of Internal Affairs and Communications
MUST-SICT	Mongolian University of Science and Technology- School of Information and communication Technology
NAoG	National Academy of Governance
NICE	National Initiative for Cybersecurity Education
NISC	National center of Incident readiness and Strategy for Cybersecurity

SME	Small and medium-sized enterprises
TTT	Train-the-Trainers
UI	University of Indonesia
USA	United States of America

1. Overview of the work

The “Project for Development of Human Resources in Cybersecurity” (the “Project”) was launched in Jan 2023 as a four-year project to be conducted with three counterparts (MDDC, MUST-SICT, and NAoG). The objective of the Project is to improve cybersecurity education programs in Mongolia. Three main project outputs are expected: 1) Build a collaboration network among industry, academia, and government for cybersecurity human resource development, 2) Develop and organize cybersecurity educational programs for students and working professionals, and 3) Develop and organize cybersecurity educational programs for public servants. Output 2) is closely related to another JICA cybersecurity-related project, the “Project for Human Resources Development for Cyber Security Professionals” at the University of Indonesia (UI) (the “Indonesian project”), and synergy between the two projects is expected to emerge. This Work Completion Report on the Project reports on briefings held on cybersecurity human resource development strategies, two Train-the-Trainers (TTT) classes so far conducted, and advice provided on revisions to the undergraduate cybersecurity curriculum. This content makes up parts of Outputs 1) and 2). The table below shows the project activities related to this work.

Table 1-1 Project Activities Related to This Work

Output 1)	
Activity 1-1.	Clarify the necessary CS human resources for Mongolia as a part of the formal MDDC's annual implementation plan
Output 2)	
Activity 2-1.	Study and develop up-to-date and comprehensive advanced cybersecurity curriculum
Activity 2-3.	Implement Train-the-Trainer (TTT) activities

2. Results of the work

The following outputs were developed in this work.

Table 2-1 List of Deliverables

No	Deliverables
1	Work Plan
2	Work Completion Report (this report)
3	Slides for the briefing sessions

The achievement status for each activity is described below.

2.1. Delivered two briefing sessions on human resource development strategies in other countries

The briefing sessions were held to help MDDC members understand the approaches to cybersecurity human resource development in other countries and to reflect the same in their own activity planning.

The information covered in the sessions has been shared twice with MDDC: first, with the members of the Cybersecurity Policy Coordination Department; second, with the Project Director and project managers at the Project Kickoff Meeting. After the briefing sessions, the Project and MDDC held further discussions to design cybersecurity human resource development initiatives in Mongolia. These discussions led to a decision to start cybersecurity awareness programs for citizens as an initial activity.

2.2. Conducted two Train-the-Trainer classes

Two train-the-trainer classes were conducted using cybersecurity subject materials developed in the Indonesian project. Each class had a class simulation (aka mock lesson) after five days of lecturing. Both classes were well received by the participants. The participants without teaching experience reported that they had learned a good deal from the evaluation criteria provided through the mock lessons and the teaching methods used by the actual teachers.

The participants were lecturers and engineers selected by the Project jointly with MDDC, NAoG, and MUST-SICT. Participation in the mock lessons was a mandatory step toward becoming an actual lecturer on the subject. The Project, MDDC, and NAoG decided, however, to allow the participants to choose not to participate in the mock lessons as some of the participants were in positions that did not normally involve teaching.

1) 1st TTT (Cybersecurity Awareness subject)

   This training covers two cybersecurity-awareness-related subjects from the Indonesian project in combination: “How to make top management aware of cybersecurity” and “How to make general employees aware of cybersecurity.”

Table 2-2 Results of the Cybersecurity Awareness TTT

Date	6th February 2023 – 14th February 2023
Venue	Building 6, MUST 317 Cybersecurity Lab
Participants	21 participants 8 participants from MDDC and NAoG 13 participants from MUST-SICT → 17 participants proceeded to the mock lessons
Language	Lecture: English Mock lessons: Mongolian
Pass rate (Instructor eligibility)	35 % (6 out of 17 participants) • 2 eligible to become main instructors • 4 eligible to become assistant instructors
Average attendance rate	85%
Instructors	Mr. Ruki Harwafuyu as the main instructor Ms. Mari Akiyama and Mr. Kohei Ogura as tutors

The instructor eligibility was evaluated by considering the attendance rate, post-test scores, and mock lesson scores in combination. See **Appendix 2-1 CS Awareness TTT Report** for details.

The low pass rate (35%) could be explained by the following issues.

- The backgrounds and prerequisite skills of the candidate participants, especially proficiency in English, were poorly screened in the participant selection process.
- Some participants were unable to attend the training at the scheduled times because they were added to the participant list without their consent or without prior notice from their organizations.
- Delays in the participant selection made it difficult for the participants to work on pre-assignments for the training.

- The participants experienced frequent interruptions during the classes because of network instability and interruptions in computer operation by frequent firmware updates.

2) 2nd TTT (Computer forensics subject)

This was a practical training that required deep knowledge of computer systems. Two consultants prepared the practice environment and assisted participants in the exercises. Most of the participants made thorough efforts to understand the subjects.

Table 2-3 Results of the Computer Forensics TTT

Date	13th March 2023 – 21th March 2023
Venue	Building 6, MUST 317 Cybersecurity Lab
Participants	15 participants →12 proceeded to the mock lessons
Language	Lecture: English Mock lessons: Mongolian
Pass rate (Instructor eligibility)	58 % (7 out of 12 participants) • Two eligible to become main instructors • Five eligible to become assistant instructors
Average attendance rate	90 %
Instructors	Mr. Defiana Arnaldy as the main instructor Ms. Mari Akiyama and Mr. Kohei Ogura as tutors

The instructor eligibility was evaluated based on the attendance rate, practical test scores, post-test scores, and mock lesson scores in combination. See **Appendix 2-2 Computer Forensic TTT Report** for details.

The pass rate was higher than that in the 1st TTT in spite of the technical difficulties of the subject. Improvements in the participant selection process and the computing/network

environment contributed to this improved result.

2.3. Provided advice on two curriculum revisions

As a prelude to this activity, four lecturers from MUST-SICT participated in a curriculum development workshop implemented by the Indonesian project and consultant. The consultant therefore provided advice on the development of undergraduate and postgraduate cybersecurity curriculums at MUST-SICT, based on the methodology used in the Indonesian project. Although the postgraduate curriculum was initially considered to be outside the scope of our consultation, as it had already been drafted and discussed by the four lecturers during the curriculum development workshop, the lecturers later requested additional consultation on the topic.

1) Undergraduate curriculum

The undergraduate curriculum was drafted by a curriculum development working group from MUST-SICT. The curriculum is based on CSEC2017, a Cybersecurity Curricular Guideline published by ACM (Association for Computing Machinery), USA. The CSEC2017 supports the development of curriculums for post-secondary education. After some interviews, the consultant found that the drafted curriculum thoroughly and effectively covered the essential topics in the guideline. The advice therefore focused on the material development phase.

a. Use of free commercial courses

The drafted curriculum contained several new subjects. This presented a challenge, as MUST-SICT has insufficient human resources to develop or maintain new subjects. As a solution, the consultant suggested relying less on MUST-SICT by using up-to-date materials from the following free commercial courses.

- The Essentials series from the EC-Council (Network Defense, Ethical Hacking, Digital Forensics)
- Introduction-to-cybersecurity from Cisco

b. Use of Exemplars and learning outcomes on CSEC2017

CSEC2017 has developed a set of curricular "Exemplars" to demonstrate the ways to organize the Body of Knowledge into a complete curriculum. The Exemplars can be used for curriculum development as well as its maintenance.

CSEC2017 has also compiled several lists of topics and learning outcomes. The learning outcomes are similar to the NICE KSAs. We recommend that learning

outcomes be used to define the learning objectives on the syllabus and to develop tests linked with the objectives. (An established set of learning objectives is essential from the viewpoint of instructional design.) The learning outcomes of CSEC2017 lie within the levels of "understanding" and "applying" (levels 1 and 2 out of 6) in Bloom's Revised Taxonomy (http://ccecc.acm.org/assessment/blooms). Thus, the learning outcomes could be transformed into the learning objectives at a lower proficiency level appropriate for the undergraduate curriculum.

2) Postgraduate curriculum

The consultant pointed out that financial factors had not been duly considered in the drafted curriculum. The ensuing discussions on the consultant's questions led to two changes in the assumptions:

a. The tuition is fixed by regulation and cannot be changed.

b. To recruit more students, the target work roles defined in SecBoK as educational objectives will be expanded from three into six.

The curriculum was revised based on these two changes in the assumptions. The introduction of nine subjects developed by the Indonesian project and two new subjects for this curriculum were defined as a result, as shown in the table below. Note that further discussion in MUST-SICT must take place before the material development can proceed.

Table 2-4 Subject list in the Postgraduate Curriculum

No	Subject	Status
1	Two subjects combined: • How to make top managements aware of cybersecurity • How to make general employees aware of cybersecurity	Developed separately by UI TTT (Cybersecurity Awareness) has been delivered at MUST-SICT
2	Case Study & Practice: Malware analysis	Developed by UI
3	Cybersecurity law and regulation	Developed by UI
4	Supply-chain risk	Developed by UI
5	Case Study & Practice: How to make	Developed by UI

	IT system forensic-enabled	
6	Comprehensive exercise: CSIRT	Developed by UI
7	Computer Forensic	Developed by UI TTT has been delivered at MUST-SICT
8	Mobile device forensic	Developed by UI
9	Security operation	New*
10	Secure design & System security	New*

* The required KSAs for the two new subjects are defined in **Appendix 2-3 SecBoK-SICT Master Mapping**.

3. Content of activities

3.1. Activity schedule

Following is an overall flow chart of activities implemented in both the Mongolian and Indonesian projects. The content of the activities in Mongolia are based on discussions held during a curriculum development workshop in the Indonesian project in Oct 2022.

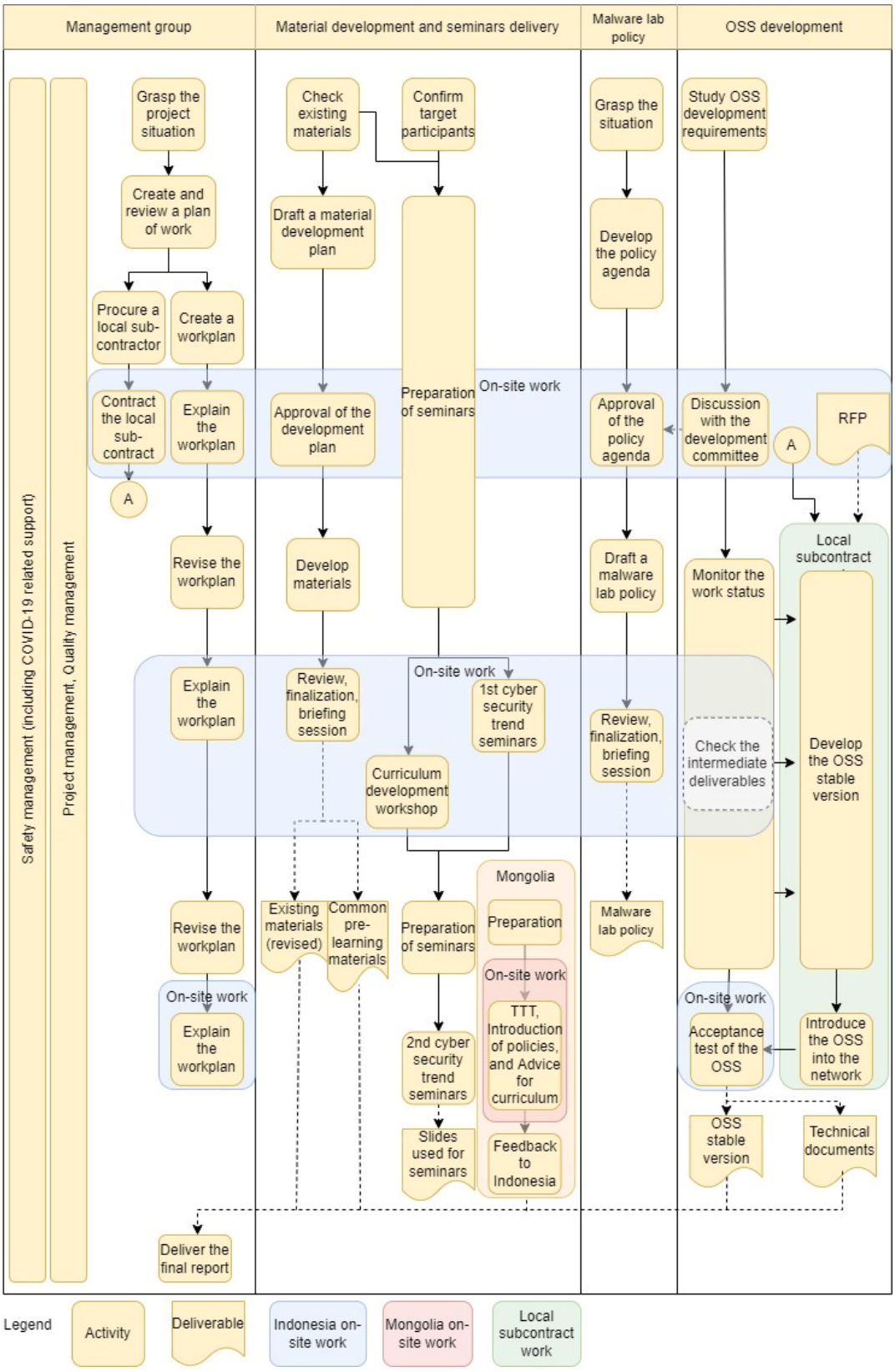
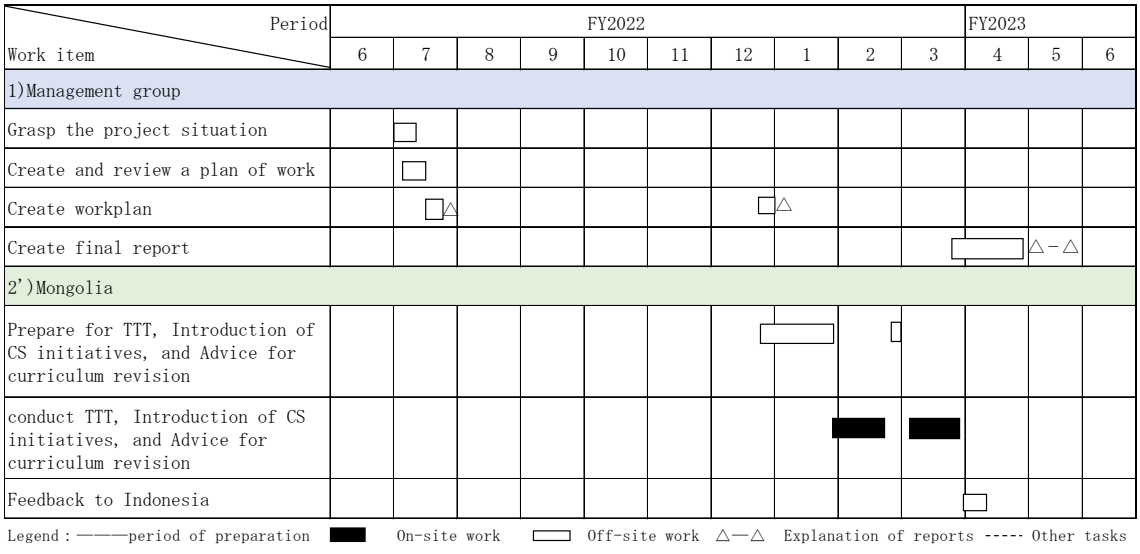


Figure 3-1 Overall Work Flow

The schedule of the work actually implemented is shown below.

Table 3-1 Schedule of work actually implemented



3.2. Consultant assignments and dispatches

Table 3-2 Expert Dispatches

Name	Assignments	Dispatch period
Mari Akiyama	• Chief Consultant • Material development and seminar/workshop delivery	25th Jan – 15th Feb 2023 1st Mar – 22nd Mar 2023
Hitohiro Sakurai	• Deputy Chief Consultant	-
Kohei Ogura	• Material development and seminar/workshop delivery (deputy)	25th Jan – 15th Feb 2023 1st Mar – 22nd Mar 2023

3.3. Work content

1) Briefing session on human resource development strategies in other countries

a. Preparation

The consultant surveyed a number of cybersecurity initiatives, issues faced in cyberspace, and cybersecurity strategies adopted in the USA, EU, Australia, Indonesia, Estonia, and Japan. Human resource development initiatives for multilayered targets (i.e., citizens, CII operators, and government agencies) were also introduced.

The main sources of information were as follows:

- Japan's Cybersecurity Strategy (NISC, Japan, 2021)
- Cybersecurity Policies (METI, MEXT, MIC, Japan)
- E-gov portal (Digital Agency, Japan)
- Cybersecurity Management Guidelines and other activities (IPA, Japan)
- Shortfall of Human Resources in Information Security and its Solutions: Plus (+) Security Human Resources (JCIC, Japan, 2019)
- Cybersecurity Education & Career Development (CISA, USA)
- Cybersecurity strategy 2019-2022 (Ministry of Economic Affairs and Communications, Estonia)
- Indonesian cyber security strategy (BSSN, Indonesia)
- Digital talent / Digital leadership academy (KOMINFO, Indonesia)
- Digital literacy index (KOMINFO, Indonesia)

b. 1st briefing session

Table 3-3 1st Briefing Session

Period	Activities
10 – 11 AM 27th January 2023	**Attendees:** [MDDC] Mr. Nasanbat, Ms. Puujee, Mr. Bartan [JICA] Mr. Ide, Mr. Tsogtoo [Consultant] Ms. Akiyama, Mr. Ogura **Information shared:** Cybersecurity strategies and initiatives in Japan, the USA, Indonesia, and Estonia; in-depth explanations of initiatives in

	Japan focused on target categories such as children, the elderly, SMEs, regions, companies, CII operators, and governments.

c. 2nd briefing session

Table 3-4 2nd Briefing Session

Period	Activities
9 – 10 AM 2nd February 2023 (as part of the project kickoff)	**Attendees:** [MDDC] Mr. Erkhembaatar (Deputy Minister), Mr. Nasanbat, Mr. Bartan [NAoG] Mr. Baigal, [MUST-SICT] Mr. Chuluunbandai [JICA] Ms. Saikhantuya, Ms. Oyunbuyan, Mr. Ide, Mr. Tsogtoo [Consultant] Ms. Akiyama, Mr. Ogura **Information shared:** Issues in cyberspace; international trends in cybersecurity strategy; an introduction of human resource development initiatives in the USA, Indonesia, and Japan; an introduction to the concept of "plus cybersecurity human resources."

2) Train-the-Trainers

a. Overall preparations

The Indonesian project was consulted before the selection and assignment of the main instructors for the two TTTs, as the TTT subjects were developed under that project. Both instructors hold UI instructor certificates on the subjects and have good English proficiency.

The consultants worked to improve the quality of the training by discussing and preparing the following measures.

i. The use of common pre-learning materials

The consultants developed common pre-learning materials (CPLMs) for subjects taught in the Indonesian project. The use of CPLMs could narrow the gaps in

knowledge among participants and avoid delays in the lessons. The participants are expected to study CPLMs before the TTT as a pre-assignment.

ii. Group lecture and offline support

The consultants selected a hybrid training delivery method combining online lectures with in-person participants supported by onsite tutors (consultants), as shown below. This structure facilitates questions, discussions, and exercises and helps to minimize the disadvantages of online lectures such as machine troubles and problems in the computing/network environment or the participants' concentration.

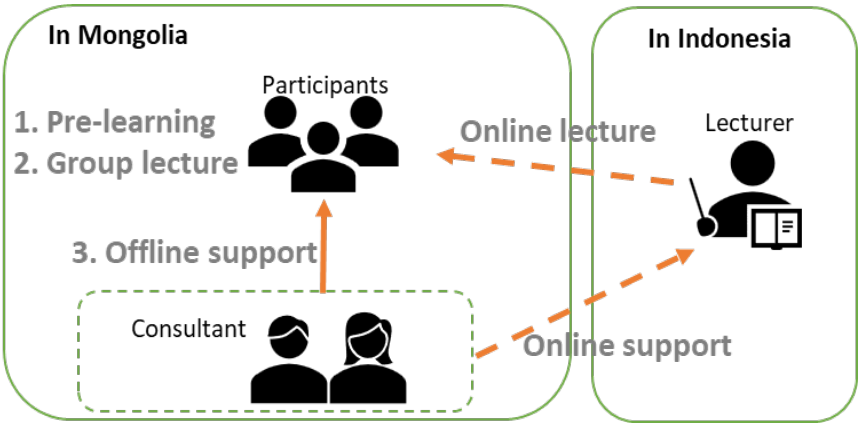


Figure 3-2 TTT Training Delivery Method

iii. Simulated lectures (mock lessons)

The consultants planned a series of mock lessons to take place after the five lecture days to enhance knowledge and skills the participants acquired. The mock lessons were to be structured according to the following rules:

- One participant acts as a lecturer while the others act as students. The lecturer role is rotated from student to student in turns. Each student has to ask at least one question per lecture.
- Use UI's materials as they are (without any modifications).
- The students evaluate the lecturers using an instructor capability check sheet (**Appendix 3-1 Instructor Capability Assessment - Mongolia**) modeled after a check sheet developed in the Indonesian project.

iv. Material modification

The consultants made several modifications to the materials while preparing and implementing the training in order to improve the trainings. The focus of most of

the modifications was to make the instructions clearer. The consultants also identify the localization needs. See **Appendix 3-2 Specifications of Revisions** for details.

b. 1st TTT (Cybersecurity Awareness subject)

Table 3-5 Activities for the Cybersecurity Awareness TTT

Period	Activities
Dec 2022 - Jan 2023	**Preparations** i. Preparations for the exercises to be conducted by the hybrid method • Discussed the time schedule and facilitation • Added instructions on the discussions to UI's materials • Modified some of the Indonesian local topics • Prepared a briefing session on the CPLMs for the participants who were unable to complete the pre-assignment themselves ii. Setup of the on-site environment MUST-SICT prepared the venue and computers. The Project prepared an internet connection and Wi-Fi router. The consultants configured the computer and router.
Jan - Feb 2023	**Participant selection / Announcement** • The consultant requested the C/Ps through the Project to select the participants two weeks before the TTT, to ensure that the participants could study the CPLMs as a pre-assignment. The participants, however, were not selected until shortly before the TTT. • The consultant announced the pre-assignment and ensuing briefing session to the participants. Because of the delay of in the participant selection, no one participated in the Zoom

	briefing session on 2nd Feb and the pre-assignment was left mostly undone.
6th - 10th Feb 2023	**Lecture** The instructor delivered the training online. The consultants supported the delivery as tutors, especially during the group discussions and presentations. Two issues were encountered in the course of the training. Both were solved after the training. • The network was unstable due to the low quality of the Wi-Fi router. • The computer operation was interrupted by frequent firmware updates.
13th, 14th Feb 2023	**Mock lessons** The consultant organized a series of mock lessons. Every participant acted as a lecturer and evaluated the other participants as lecturers.
14th Feb 2023	**Preliminary report** The consultant reported the preliminary results of the training, the issues encountered, and recommendations to the vice project manager.
16th - 22nd Feb 2023	**Evaluation** The instructor and consultants finalized the evaluation by determining the theoretical and practical skills of the participants.
9th Mar 2023	**Evaluation report** The consultants reported the evaluation results to the Project.

c. 2nd TTT (Computer forensics subject)

Table 3-6 Activities for the Computer Forensics TTT

Period	Activities
Dec 2022- Feb 2023	**Preparations** i. Preparations for the exercises to be conducted by the hybrid method • Discussed the time schedule and facilitation • Added instructions on the discussions to UI's materials • Prepared virtual machines with the latest versions of the tools required for hands-on practice • Prepared a briefing session on the CPLMs for participants who could not complete the pre-assignment themselves ii. Onsite environment setup MUST-SICT prepared the venue and computers. The Project prepared an internet connection and Wi-Fi router. The consultants configured the computer and router. To solve the network stability problem encountered in the previous TTT, the Project used another type of Wi-Fi router and the consultants prepared several mobile internet lines as backups.
Feb – Mar 2023	**Participant selection / Announcement** • The consultants set stricter prerequisites for the participants in view of the technically demanding subject: ➢ Listening and reading skills in English (Equivalent: IELTS 6.0, TOEFL550, TOIEC 860) ➢ Knowledge of OSs, file systems, data structures (Windows, Unix), OSI & TCP/IP models, and e-mail protocols ➢ Basic knowledge of computer architecture/systems,

	digital storage media (volatile, non-volatile) ➢ Basic knowledge of SQL (SQLite) • The consultants requested the C/Ps through the Project to select the participants two weeks before the TTT, and the participants were selected a week before as result. The participant selection process went faster than in the 1st TTT, but there was still room for improvement. • The consultant announced the pre-assignment and ensuing briefing session to the participants. Every participant completed the pre-assignment before the TTT. No one needed to take part in the ensuing briefing on the CPLMs planned for the 10th.
13th - 17th Mar 2023	**Lecture** The instructor delivered the training online. The consultants supported the delivery as tutors, especially the exercises.
20th, 21st Mar 2023	**Mock lessons** The consultant organized mock lessons. Every participant acted as a lecturer, demonstrated the exercises, and evaluated the performance of the other participants by the same approach used in the 1st TTT.
21st Mar 2023	**Preliminary report** The consultant reported the preliminary results of the training, the issues encountered, and recommendations to the vice project manager.
21st - 28th Mar 2023	**Evaluation** The instructor and consultants finalized the evaluation by determining the theoretical and practical skills of the participants.
10th Apr 2023	**Evaluation report**

	The consultants reported the evaluation results to the Project.

3) Advice on curriculum revisions

a. Undergraduate curriculum

Table 3-7 Advisory Activities for the Undergraduate Curriculum

Period	Activities
26th Jan 2023	1st meeting The curriculum development working group provided the consultant with an explanation of the drafted undergraduate curriculum, which is based on CSEC2017, ACM.
3rd Feb 2023	2nd meeting The consultant requested the working group to do the following. **Knowledge covered** Create a map detailing the alignment between the subjects and the topics covered in the framework by 3rd March 2023. **Subject** Decide whether to introduce the commercial courses into the curriculum by 3rd March 2023. This request was based on the conflict between ideas for introducing commercial courses and the regulatory limits set on tuition.
3rd Mar 2023	3rd meeting The working group reported the results of the internal discussion to the consultant together with a map of the subjects and the topics covered in the framework. **Knowledge covered** The consultants requested the map to confirm the coverage of the subjects in the CSEC2017 framework and found that the subjects covered almost all of the essential topics. No advice was required in terms of the coverage. **Subject**

	The working group decided not to introduce commercial courses and reported that the institution had too few human resources to develop new subjects for the time being. The consultant therefore recommended that the institution use free, entry-level materials provided by commercial vendors. **Other matters** The consultant suggested that the institution use curricular exemplars of CSEC2017 and create learning objectives and tests using the learning outcomes of CSEC2017.

b. Postgraduate curriculum

Table 3-8 Advisory Activities for the Postgraduate Curriculum

Period	Activities
26th Jan 2023	1st meeting The curriculum development working group explained the current status of the postgraduate curriculum to the consultant and requested advice. The meeting participants discussed two questions from the consultant and project chief advisor and decided to revise two of the prerequisites in response to each question. i. How will the tuition be priced to cover the necessary expenses? →Prerequisite revision: Tuition is fixed by government regulation and cannot be changed. A tuition increase to cover the cost of the commercial courses listed in the drafted curriculum was expected. This turned out not to be the case, however, as the regulation set on the tuition was not duly considered. It was decided, through discussion, that only a few commercial courses could be introduced in the MUST-SICT postgraduate curriculum, if any. ii. What will be the strategy for student recruitment? →Prerequisite revision: To recruit more students, the work roles

	targeted as educational objectives (defined in SecBoK) will be expanded from three into six. The target work roles were narrowed down to three in the curriculum development workshop to complete the exercises in time. Hence, the market demands were discussed and six target work roles were set in total. Two revisions in the prerequisites were necessary, as explained above. The consultant requested the working group to reach decisions on the following and revise the curriculum accordingly. i. Decide whether or not to introduce the commercial courses into the curriculum ii. Finalize the target work roles discussed in the meeting
3rd Mar 2023	2nd meeting The working group reported the results of the internal discussion to the consultant. It was decided that commercial courses would not be introduced into the curriculum, and that six work roles would be introduced (CISO, forensic engineer, vulnerability diagnostic consultant, incident manager/handler, self-assessment/solution analyst, information security auditor). The working group and consultant revised the curriculum together during the meeting. The results of the revisions are shown in **Table 2-4 Subject list in the Postgraduate Curriculum**.

4. Lessons learned and suggestions

1) Train-the-Trainers

- We recommend that the institution ensure that the candidate lecturers have basic knowledge of cybersecurity. For instance, a CEH or Security+ level certificate could be used for qualification.
- English proficiency was clearly found to be a key prerequisite for studying

cybersecurity using Indonesian materials and instructors in English. Some of the participants struggled to keep up with the class because of the language barrier.

- Online training can only succeed if tutors are on hand to perform the training effectively, especially on subjects with numerous exercises and discussions. Support for group discussions and support for individual participants who are having trouble with the machines and exercises are essential for interactive learning.

2) Material localization

Several topics introduced information specific to Indonesia, as stated in **2.2 Conducted two Train-the-Trainer**. We recommend that the following topics be localized.

i. "How to make top management aware of cybersecurity"

One of the discussions in the instructor guide / student guide in Module 3 refers to the ID-SIRTII report, an annual national internet traffic monitoring report published by ID-SIRTII/CC, the Indonesian national CSIRT. A comparable report in Mongolia should be discussed instead. If no such report is available, a substitute report, "apac-state-of-incident-response-2022," could be used. This substitute report was introduced during the TTT.

ii. "How to make general employees aware of cybersecurity"

A number of case studies localized in Indonesia are covered in the hands-on-exercises in Module 4. These should be replaced with comparable cases in Mongolia. One TTT participant suggested a case involving a data breach at the Khan Bank.

iii. "Computer Forensics"

Several pages in the instructor guide / student guide in Module 1 explain cyber laws in Indonesia. These explanations should be replaced by comparable explanations of the Mongolian cyber laws.

3) Curriculum revisions

Each step of the curriculum development and revision should be documented for cross check and review.

A number of prerequisites had to be revised after the curriculum development because of a lack of documentation. The working group checked the regulations before

designing the curriculum. Their approach was in line with the method used in the Indonesian project. The issue of tuition pricing, however, was left unaddressed in the requirement clarifications. This concern was not documented or carried over to the next phase of curriculum development.

Appendices

Report of Train The Trainer

Date: 28th Feb 2023

TOKYO Co., Ltd.

1. General information

Training: Train-the-Trainer (TTT) on "CyberSecurity Awareness"

Duration: From 6th Feb To 14th Feb

Subject: Cybersecurity Awareness
(How to make general employees aware of cybersecurity,
How to make top management aware of cybersecurity)

Delivery method: Hybrid (Online + Onsite training room @ MUST-SICT)

Instructor: Dr. Ruki Harwahyu (Online)

Tutors: Ms. Mari Akiyama, Mr. Kohei Ogura (Onsite)

2. Activity record

Activity	Period
Preparation Material modifications for Mongolia Preparation for exercises in the Hybrid manner Onsite environment setup	Dec 2022- Jan 2023
Lecture	6-10 Feb 2023
Mock lessons	13, 14 Feb 2023
Evaluation Discussions between the Main instructor and tutors	16- 22 Feb 2023

3. Evaluation result

Instructor Eligibility	Number of participants
Main Instructor Level	2
Assistant Level	4
Not Eligible	14*

(*Seven of them are not evaluated due to poor attendance rate or not willing to be an instructor)

Instructor eligibility is evaluated with a combination of attendance rate, post-test scores, and mock lesson scores. Four participants are evaluated as assistants of the two main instructors. If the main instructor assumes that they get sufficient experience and skill

to teach this subject, they may be promoted to a main instructor.

See Appendix A, "Evaluation of participants_CS Awareness" for details.

4. Lesson learned, Suggestions and Concerns

1) Participants
   - ✓ Participant selection criteria should be improved related to the issues below;
     - ➢ Haven't had enough management background and cybersecurity background to follow the training and to be a lecturer
     - ➢ Experiences are not sufficient, hence couldn't give examples related to their work/organization
     - ➢ Busy working on other things
     - ➢ Language barriers
     - ➢ Low motivation. Too many participants hesitate to present or ask questions. We assume that depends on their daily role and the predicted benefit that they can personally earn from the TTT.
   - ✓ Many participants did not utilize the pre-learning materials as intended. Participants shall get at least 2 weeks to study it.
   - ✓ It is suggested to set minimum scores on module tests. Participants were actively asking questions regarding the test. Using it for triggering engagement may yield a good result.

2) Materials
   - ✓ It is suggested to separate the training into the original 2 subjects and has another TTT for "How to make top management aware of cybersecurity" with participants who have management background.
   - ✓ It is better to collect local cases which is more related/relevant to their organization. It can help participants and motivate them more.
   - ✓ Many participants tried to cheat on tests. It is suggested to update the tests periodically and strictly monitor the tests physically and technically. If they use google or ChatGPT, we cannot evaluate their true achievement from the learning/training process they took.

3) Environment
   - ✓ Internet connection was not stable enough. In future training with the Hybrid delivery method, it is suggested to have more than one active device on both

sides with different internet connections, as a backup.

- ✓ Audio management should be improved. Especially the mobile microphone. It went loose and unclear sometimes. This makes the instructor difficult to understand the participant's words in addition to different English pronunciations.
- ✓ Webcam in the training room was clear enough, but the location should be changed to cover a wider area of the venue.

5. General feedback

- ✓ In discussions that do not require prior experience in middle-level management, most of the groups did their tasks rather well.
- ✓ It was good that older participants tend to include a little bit of their background experience during the presentation.
- ✓ Hybrid delivery went well with the onsite tutor's feedback to the online instructor regarding the class's condition, and participants' reactions.

END

Report of Train The Trainer

Date: 28th Mar 2023

TOKYO Co., Ltd.

1. General information

Training: Train-the-Trainer (TTT) on "Computer Forensics"

Duration: From 13th Mar To 21st Mar

Subject: FOR0040a Computer Forensics

Delivery method: Hybrid (Online + Onsite training room @ MUST-SICT)

Instructor: Mr. Defiana Arnaldy (Online)

Tutors: Ms. Mari Akiyama, Mr. Kohei Ogura (Onsite)

2. Activity record

Activity	Period
Preparation Material modifications for Mongolia Preparation for exercises in the Hybrid manner Onsite environment setup	Dec 2022 - Feb 2023
Lecture	13-17 Mar 2023 (5 days)
Mock lessons	20, 21 Mar 2023 (2 days)
Preliminary report Temporal training results were reported to Mr.Uuganbayar. Control of a Google account for training was transferred to Mr.Uuganbayar.	21 Mar 2023
Evaluation and Report Discussions between the Main instructors and tutors	22-28 Mar 2023

3. Evaluation result

Instructor Eligibility	Number of participants
Main Instructor Level	2
Assistant Level	5
Not Eligible	8*

(*Four of them is not evaluated due to poor attendance or not willing to be an instructor)

Instructor eligibility is evaluated with a combination of attendance rate, practical skills,

post-test scores, and mock lesson scores. Five participants are evaluated as assistants of the two main instructors. If the main instructor assumes that they get sufficient experience and skill to teach this subject, they may be promoted to a main instructor. Mr. Purevbat and Mr.Sandagsuren need only a few steps to reach the main instructor level.

See Appendix A, "Evaluation of participants_Computer Forensic" for details.

4. Lessons learned, Suggestions, and Concerns

1) Participants

Participant selection was delayed and excluded MUST lecturers at the beginning.

- ✓ It is suggested to build a structure and flow of participant selection to enhance the process.
  - ➢ At first, MUST shall have an administrative leader who can manage
    - ✧ Lecture schedule of participant's lecturers
    - ✧ Venue and environment preparation
    - ✧ Participant criteria adjustment
    - ✧ Teaching materials
  - ➢ Participants should be decided 2 weeks before the training
- ✓ MUST could have a human resource pool like CAMP program at the University of Indonesia. It is suggested to set a baseline of pre-requisite knowledge and skills for the potential lecturers
- ✓ Participant attendance should be carefully controlled. If a participant skipped classes for more than a half day, he/she would remain behind, especially in advanced subjects.

2) Others

- ✓ Onsite training, Hybrid training with clearer captions, or slide note enhancement may improve the issue of language.
- ✓ DELL update at the Lab computer should be controlled to prevent disturbances in the class activities

5. General feedback

- ✓ Venue environment has been improved compared to the CS Awareness TTT, hence the class activities went smoothly.
- ✓ Participants' selection criteria have been improved compared to the CS Awareness TTT, hence most of the participants had enough background and language proficiency.
- ✓ Every participant could access Zoom with an auto caption. It improved the participant's understanding.
- ✓ Mock lessons got favorable reputations, especially from non-MUST participants for them

to gain lecture skills.

END

Appendix 2-3 SecBoK-SICT Master Mapping

Security knowledge field (SecBoK) Human resources skill map 2021 edition Overall arrangement table

* Created by the Information Security Knowledge Item (SecBoK) Revision Committee, Education Subcommittee, Japan Network Secur

Required knowledge and skills for each role

1	Prerequisite skills (Knowledge / skills to be possessed as a premise
2	Required skills (Knowledge / skills required to carry out job perform
0.5	Reference skills (Not required for job performance but desirable kno

※Relationship between"Prerequisite skills" and "Required skills"
If you secure human resources with prerequisite skills and provide education and training on required skills to the person, he/she will be able to take the job.

<Level of knowledge and skills>

L	Low(less than 3 years experience)
M	Medium (more than 3 years of experience or related exercises / training participants can cope)
H	High (10 or more years of experience or experienced professional who assumed advanced training or "prominent personnel" can cope)
P	Pending (related to information gathering and intelligence. It is not a subject to leveling this time)

									Supply Chain	CSIRT	Aware CEO	Aware General Employees	Computer Forensic	Mobile Forensic	CS Law	Malware Analysis	Forensic Enable	Introduction to Cybersecurity	Security operation	Secure degisn & System security	Remaining for other Custom Courses	CISO	Incident manager,Incident handler	Self assessment,Solution analyst	Vulnerability diagnostic consultant	Forensic engineer	Information security auditor
									157	830	247	215	457	453	198	475	562										
2021ID	OLD 2019I	KSA -ID	Old / New	Field	Category	Subcategory	Leve	KSA (knowledge, Skill, Ability) Description																			
1	1	K0052	Similar Term exists in Old NICE	00 Basis	1 Mathematical and Physical Informatics		L	Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).													for Bachelor course			0.5			
3	3	K0036	Same term as Old NICE	00 Basis	2 Computer/Com		L	Knowledge of human-computer interaction principles.													for Bachelor course			1			
15	15	K0556	New Term	00 Basis	2 Computer/Com		L	Knowledge of telecommunications fundamentals.													for Bachelor course		1	1	1	1	1
16	16	K0015	Same term as Old	00 Basis	3 Software		L	Knowledge of computer algorithms.													for Bachelor course			1	1	1	
17	17	K0016	Similar Term exists	00 Basis	3 Software		L	Knowledge of computer programming principles													for Bachelor course			1	1	1	
19	19	K0068	Same term as Old	00 Basis	3 Software		L	Knowledge of programming language structures and logic.													for Bachelor course			1	1	1	
20	20	K0069	Almost same Term	00 Basis	3 Software		L	Knowledge of query languages such as SQL (structured query language)													for Bachelor course		1	1	1	1	
21	21	K0082	Same term as Old	00 Basis	3 Software		L	Knowledge of software engineering.													for Bachelor course			1	1	1	
26	26	K0080	Same term as Old	00 Basis	3 Software		L	Knowledge of software design tools, methods, and techniques.													for Bachelor course			1	1	1	
28	28	K0420	Same term as Old	00 Basis	4 Data		L	Knowledge of database theory.													for Bachelor course				0.5		
41	994		Added by SecBok	01 IT/Security	1 ICT	2 ICT Literacy	L	Fundamental IT literacy at level 2 of ITSS										x				1	1	1	1	1	1
59	52	K0203	New Term	01 IT/Security Basics	2 Security Basics	2 Model	M	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).												x		0.5		0.5	0.5		
67	1091		Added by SecBok	02 IT Human Skill	1 Communication		L	Ability to read and understand English documents promptly													Pre-requisite						1
68	1092		Added by SecBok	02 IT Human Skill	1 Communication		L	Ability to read and understand English documents appropriately													Pre-requisite						1
83	1107		Added by SecBok	02 IT Human Skills	2 Thinking and Judgment		M	Ability to determine information appropriately										x				1	1	1			2
84	1108	A0070	New Term	02 IT Human Skills	2 Thinking and Judgment		M	Ability to apply critical reading/thinking skills.										x				1					
98	67	K0293	New Term	03 Security Governance	2 Organizational Architecture		M	Knowledge of integrating the organization's goals and objectives into the architecture.												x		2		2			
233	202	K0104	Same term as Old NICE	05 Network Security	6 VPN		L	Knowledge of Virtual Private Network (VPN) security.													for Bachelor course	0.5	0.5	0.5	0.5		0.5
234	203	S0059	Same term as Old NICE	05 Network Security	6 VPN		M	Skill in using Virtual Private Network (VPN) devices and encryption.													for Bachelor course		0.5				
246	215	K0294	New Term	06 System Security	0 General remarks		L	Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.												x		2	1	2	1	1	1
248	217	K0167	Similar Term exists in Old NICE	06 System Security	0 General remarks		M	Knowledge of system administration, network, and operating system hardening techniques.												x		0.5	0.5	0.5	0.5	0.5	0.5
257	226	K0212	New Term	06 System Security	3 Application		L	Knowledge of cybersecurity-enabled software products.												x						2	
271	240	K0275	New Term	06 System Security	6 Security Functions		L	Knowledge of configuration management techniques.												x				1			
288	257	S0139	New Term	07 Secure design and Development	2 Security Requirement Definition		M	Skill in applying security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).												x				2			1

Appendix 2-3 SecBoK-SICT Master Mapping

Required knowledge and skills for each role

1	Prerequisite skills (Knowledge / skills to be possessed as a premise
2	Required skills (Knowledge / skills required to carry out job perform
0.5	Reference skills (Not required for job performance but desirable kno

※Relationship between"Prerequisite skills" and "Required skills"
If you secure human resources with prerequisite skills and provide education and training on required skills to the person, he/she will be able to take the job.

<Level of knowledge and skills>

L	Low(less than 3 years experience)
M	Medium (more than 3 years of experience or related exercises / training participants can cope)
H	High (10 or more years of experience or experienced professional who assumed advanced training or "prominent personnel" can cope)
P	Pending (related to information gathering and intelligence. It is not a subject to leveling this time)

2021ID	OLD 2019I	KSA –ID	Old / New	Field	Category	Subcategory	Level	KSA (knowledge, Skill, Ability) Description	Supply Chain	CSIRT	Aware CEO	Aware General Employees	Computer Forensic	Mobile Forensic	CS Law	Malware Analysis	Forensic Enable	Introduction to Cybersecurity	Security operation	Secure degsn & System security	Remaining for other Custom Courses	CISO	Incident manager,Incident handler	Self assessment,Solution analyst	Vulnerability diagnostic consultant	Forensic engineer	Information security auditor
290	259	K0073	Similar Term exists in Old NICE	07 Secure design and Development	3 Secure Design		L	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).												x				2			1
295	264	S0036	Same term as Old NICE	07 Secure design and Development	3 Secure Design		H	Skill in evaluating the adequacy of security designs.												x					2		
297	266	K0140	Same term as Old NICE	07 Secure design and Development	4 Secure Programming		L	Knowledge of secure coding techniques.												x					0.5		
344	313	A0155	New Term	08 Security Operations	4 Trouble Shooting		H	Ability to provide an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation and recommend corrective actions to address identified vulnerabilities.											x				2		2		
753	722	A0077	New Term	11 Intellligence	9 Other		P	Ability to coordinate cyber operations with other organization functions or support activities.											x			0.5					
756	725	A0085	New Term	11 Intellligence	9 Other		P	Ability to exercise judgment when policies are not well-defined.											x			0.5					
759	728	A0104	New Term	11 Intellligence	9 Other		P	Ability to select the appropriate implant to achieve operational goals.											x			2					
760	729	A0107	New Term	11 Intellligence	9 Other		P	Ability to think like threat actors.											x				0.5	0.5			

Instructor capabilities check sheet

	Evaluation criteria	Status (Good/Fair/Poor)
Personality (3point x3)	Enthusiastic（Motivated, Energetic）: Walking around the class to see students' progress. Talking or giving feedback to each person. Taking initiatives in class control (for work instruction, time management, and etc.)	
	Honesty & Confidence : Not changing or deleting the provided materials. Not giving wrong information to questions. Having enough knowledge and confidence to deliver the content.	
	Positive : Actively promoting mutual respect and interaction. For example, remembering the students' name and talking to them.	
Presentation skill (3point x8)	Nonverbal behavior	
	Vocal ・Loudness of the voice can be heard up to the last row of the classroom ・Understandable speaking speed ・Changing pitch and tone of voice for better stress and intonation ・Not using filler words or verbal habit such as "well", "like", "you know" ,and etc.)	
	Body language and Posture ・Keeping the face relax and expressive ・Using hands and other gestures to add clarity, emphasis, and energy ・Not making unnatural movement	
	Eye contact ・Holding eye contact on one person while speaking one sentence ・Giving eye contact to everyone fairly ・Not keeping eyes too long on a white board or a screen (Looking at audience) ・Looking at the camera for online lectures.	
	Verbal behavior	
	・Using instructor's own experience and episodes, examples of real world, knowledge associated with other topics (parables, paraphrases) to increase students' knowledge retention	
	・Making one sentence short and concise	
	・Instructions for exercises and tasks are clear and specific ・Not using pronouns(this, that, those, etc.) too much ・Repeating instructions. Making sure each student understands the instructions.	
	・Not just explaining to students but questioning to each person or to the whole class for confirming comprehension ・Planning out the questions well. For example, questioning twice with a combination of open-ended and closed-ended questions.	
	Media utilization	

	・Trying to keep students interested by using media (handouts, whiteboard, actual machines) ・Content on whiteboard or handouts are appropriate(Content of the media is correct, providing the media at the right timing, no typo)	
Instructional design（Gagne's Nine events of instruction）	1 Gaining attention of the students. Students are watching and listening while instructor presents the contents.	
	2 Informing students of the objectives and explain what they are expected to learn today to reach the objectives Explaining the objectives without using the word "Understand"	
	3 Confirming students if they have pre-requisite knowledge or skills	
	4 Clearly presenting the content to reach the objectives	
	5 Providing new topics in an easy-to-understand manner, such as parables and exercises to remember the topics. Trying to keep students' interest with variety of learning methods such as group work and gamification.	
	6 Providing opportunity to practice	
	7 Providing feedback on individualized tasks or practices	
	8 Utilizing a variety of assessment methods such as exams and wrap-up quizzes, and to see if the students reach the objectives	
	9 Wrap-up the learning contents and enhance retention. Promoting further study.	

Any other feedback to the instructor：

Total score____/60

*Pass rate is 60%.

Good : 3 points
Fair : 2 points
Poor :1 point

Appendix 3-2 Specifications of Revisions

How to make top managements aware of CS

No	Revision status	Priorities (High-Law)	Type of actions	Materials	Topics / Modul	Modification ID	Directions of Revision	Reason of the Revision	Applied framework/theories	Issued by	Date of iss	Received b	Date of received	Actions taken	Date of Submission	Date of Acceptance
1	Accepted	High	Modify	Mapping Table COM0010a	All modules		Modified time allocation from 2days to 3days.	Too short duration for the subject.	-	Ogura	01-Mar-23			Expand time allocation especially for exercise and discussion.	01-Mar-23	02-Apr-23
2	Accepted	High	Modify	Instructor guide, Student guide	Module2		Practical test could be a proposal of an appropriate response to a certain cyber incident.	Not clear direction for discussion.	-	Ogura	01-Mar-23			Added explanation for discussion on instructor guide p.24.	01-Mar-23	02-Apr-23
3	Accepted	High	Modify	Instructor guide, Student guide	Module2		Statement on slide p.16 are not correct. - "CIO got angry" should be "CEO got angry" - "CIO doesn't calm" should be "CEO doesn't calm"	For consistency between video and slides.	-	Ogura	01-Mar-23			Revised p.16	01-Mar-23	02-Apr-23
4	Accepted	High	Modify	Instructor guide, Student guide	Module3		"Explain by ID-SIRT report" (p.36); Due to ID-SIRT report only in Bahasa, prepared an alternative report in English for Mongolia TTT. "apac-state-of-incident-response-2022.pdf" in https://drive.google.com/drive/folders/1WmnxT4hQoBiYcDQ9QQ3r5MUt3ysY48-s?usp=sharing	For other language than Bahasa	-	Ogura	01-Mar-23			The template file has already been located in "Hands on Data"	01-Mar-23	02-Apr-23
5	Accepted	High	Modify	Instructor guide, Student guide	Module3		Change "Group discussion" to "Exercise with Statistic Report" (p.37) and add detail instructions	For help on instruction	-	Ogura	01-Mar-23			Revised p.37	01-Mar-23	02-Apr-23
6	Accepted	High	Modify	Mapping Table COM0010a	Module3		"Exercise with Statistic Report" (instructor guide p.37); On mapping table, no time is allocated for discussion.	For availability of subject	-	Ogura	01-Mar-23			Allocated 65min for this exercise	01-Mar-23	02-Apr-23
7	Accepted	High	Modify	Instructor guide, Student guide	Module3		Hide slide p.38, instead of the exercise on p.37.	The exercise on p.38 is very similar to an exercise at the end of Module 2.	-	Ogura	01-Mar-23			Hided p.38	01-Mar-23	02-Apr-23
8	Accepted	High	Modify	Module 3 test	Module3		Module3 test Question5: the answer seems not correct, should be "All of the above statements."	For correct answer	-	Ogura	01-Mar-23			Changed the answer	01-Mar-23	02-Apr-23
9	Accepted	High	Modify	Instructor guide, Student guide	Module4		"Exercise and Discussion" (p.32); No direction for discussion was showed.	For help on instruction	-	Ogura	01-Mar-23			Added instructions on note area. - Please identify and discuss the challenges in your organization to implement cybersecurity risk assessment. - Give short analysis what are things to be improved to tackle those challenges.	01-Mar-23	02-Apr-23
10	Accepted	High	Modify	Instructor guide, Student guide	Module4		"Exercise and Discussion" (p.54); Recommended to provide a template file. Sample in Mongolia TTT is "ASSET RISK IDENTIFICATION.docx" in https://drive.google.com/drive/folders/16oUSYkRZh9PpWo1goBH6SY8A22rfSv8z?usp=sharing	For help on understanding	-	Ogura	01-Mar-23			The template file has already been located in "Hands on Data"	01-Mar-23	02-Apr-23
11	Accepted	High	Modify	Instructor guide, Student guide	Module5		"Exercise: Quantitative Risk Assessment" (p.21); To clarify the question, revised the slide and note.	For help on understanding	-	Ogura	01-Mar-23			Revised p.21. (Words are added, "weekly" to slide and "700%" to note.)	01-Mar-23	02-Apr-23
12	Accepted	High	Modify	Instructor guide, Student guide	Module5		"Sample Scenario on Profit/Loss" (p.23); There was an incorrect number on the table. The cost -60 of "COGS- labor / manufacturing" on the column "Indirect 5% future loss" is not correct, -75 is correct.	For help on instruction	-	Ogura	01-Mar-23			Changed the number "-60" to "-75"	01-Mar-23	02-Apr-23
13	Accepted	High	Modify	Instructor guide, Student guide	Module5		"Exercise1" (p.40); Recommended to provide a template file. Sample in Mongolia TTT is "Exercise Impact calculation.xlsx" in https://drive.google.com/drive/folders/1WmnxT4hQoBiYcDQ9QQ3r5MUt3ysY48-s?usp=sharing	For help on understanding	-	Ogura	01-Mar-23			The template file has already been located in "Hands on Data"	01-Mar-23	02-Apr-23
14	Accepted	High	Modify	Module 5 test	Module5		Module5 test Question3: the answer seems not correct, should be "Qualitative Risk Assessment"	For correct answer	-	Ogura	01-Mar-23			Changed the answer	01-Mar-23	02-Apr-23
15	Accepted	High	Modify	Instructor guide, Student guide	Module6		Change the title "6.2.Exercise and discussion" to "Appendix: Guideline for Exercises"	The title "6.2.Exercise and discussion" is not appropriate with its contents.	-	Ogura	01-Mar-23			Changed the title	01-Mar-23	02-Apr-23
16	Accepted	High	Modify	Module 6 test	Module6		Module6 test Question3; The allocated score was incorrectly "0", should be "10".	For correct scoring	-	Ogura	01-Mar-23			Changed the score	01-Mar-23	02-Apr-23
17	Accepte	High	Modify	Mapping Table	Module1~7		Time allocation needs to be revised based on actual time used in the TTT in	For appropreate time allocaton	-	Ogura	01-Mar-23			Changed time allocation	01-Mar-23	02-Apr-23
18	Accepted	Middle	Modify	Post test	Post test		Replace following questions with other questions. 2. Investments in cyber security technologies should be based on: 9. A successful cyber security management program should use which of the following to determine the amount of resources devoted to mitigating exposures? 10. Which of the following will BEST protect an organization from internal security attacks? 14. When the computer incident response team (CIRT) finds clear evidence that a hacker has penetrated the corporate network and modified customer information, an information security manager should FIRST notify: 17. A common concern with poorly written web applications is that they can allow an attacker to:	The questions are less relative to the material content, too technical or too similar to other questions.		Akiyama	21-Mar-23			Replaced with following questions. Module1 related: 1 What is not the benefit of adopting a risk management approach to cybersecurity? a.Corporate decision making is improved through the high visibility of risk exposure b.Reduced of losses and improved "Value for Money" potential (correct)c. Employees are not leaving the organizations d. Being assured of adequate contingency plans Module 2 related: 2 Which response activity is NOT appropriate when an incident happens and grows bigger ? a.Identify the attack and understand the severity	21-Mar-23	02-Apr-23
19	Issued	Low	Modify	(Hands on Data) Cyber Security Awarness Movie.mp4	Module2		According to ending credit of video material, COO doesn't appear in the video. The credit on video should be changed.	For consistency between video and slides.	-	Ogura	01-Mar-23					
20	Issued	Low	Modify	(Hands on Data) Cyber Security Awarness Movie.mp4	Module2		Caption on video scene 5 (9:00) is not correct. - "CIO got angry on IT team" should be "CEO got angry on IT team"	For consistency between video and slides.	-	Ogura	01-Mar-23					
21	Issued	Low	Modify	Instructor guide, Student guide	Module3		Needs detail direction or sample of "Show some leaked data" (p.16) and "Dark web" (p.23) for instructors. Example in Mongolia TTT is "sample of 'Show some leaked data' and 'Dark web'.mp4" in https://drive.google.com/drive/folders/1umDqghw9MuQwE4W0McjR2UFGVXQu9Ywl?usp=sharing	For help on instruction	-	Ogura	01-Mar-23					
22	Issued	Low	Modify	Instructor guide, Student guide	Module5		"Exercise: How to prioritize actions" (p.25); There's the same slide on p.55. Thus, just provide introduction on p.25, do exercise on p.55.	For correct information	-	Ogura	01-Mar-23					
23	Issued	Low	Modify	Instructor guide, Student guide	Module5		In COM0010a Module5 "THREAT * VULNERABILITY = RISK" should be explicitly explained in earlier stage. At least early in Module4	For help on understanding	-	Ogura	01-Mar-23					

Appendix 3-2 Specifications of Revisions

24	Issued	Low	Modify	Post test	Post test		Modify following questions. 5. Which of the following would be MOST effective in successfully implementing restrictive password policies? 7. The MOST important characteristic of good security policies is that they: 8. A risk management program should reduce risk to: 11. Which of the following risks would BEST be assessed using qualitative risk assessment techniques? 12. Quantitative risk analysis is MOST appropriate when assessment data: 13. A successful risk management program should lead to: 15. Which of the following attacks is BEST mitigated by utilizing strong passwords? 20. Senior management commitment and support for cyber security can BEST be obtained through presentations that:	The questions are copies of CISM online quizlet.		Akiyama	21-Mar-23					
25																
26																
27																
28																
29																
30																

Appendix 3-2 Specifications of Revisions

How to make general employees aware of CS

No	Revision status	Priorities (High-Law)	Type of actions	Materials	Topics / Module	Modification ID	Directions of Revision	Reason of the Revision	Applied framework/theories	Issued by	Date of iss	Received by	Date of received	Actions taken	Date of Submission	Date of Acceptance
1	Accepted	High	Modify	(Hands on data) Studi Kasus Ilham Bintang.docx, Studi Kasus Tokopedia.docx	Module4		Input files for discussion were only in Bahasa.	For using in other countries	-	Ogura	01-Mar-23			Added description in English to the end of files.	01-Mar-23	02-Apr-23
2	Accepted	High	Modify	Module test	Module5		Module5 test Question4; invalid question, there were several correct answers.	For correct answer	-	Ogura	01-Mar-23			Changed options of the question.	01-Mar-23	02-Apr-23
3	Accepted	High	Modify	Instructor guide, Student guide, (Hands on data) template for designing and evaluating awareness program.xlsx	Module6		Instructor guide p.43: Added a page that instructs to fill in "template for designing and evaluating awareness program.xlsx"	For help on instruction	-	Ogura	01-Mar-23			Instructor guide p.43: Added a page that instructs to fill in "template for designing and evaluating awareness program.xlsx"	01-Mar-23	02-Apr-23
4	Accepted	High	Modify	Instructor guide, Student guide	Module7		"Discussion" (Instructor guide p.20); To clarify what to discuss, use the template file same as module6 ("template for designing and evaluating awareness program.xlsx"). Participants update the "Programs" sheet based on module7 lesson.	For help on instruction	-	Ogura	01-Mar-23			"Discussion" (Instructor guide p.20); Changed the instruction sentense.	01-Mar-23	02-Apr-23
5	Accepted	High	Modify	Instructor guide, Student guide	Module8		Instructor guide p.25: Added a page that instructs to fill in "template for designing and evaluating awareness program.xlsx"	For help on instruction	-	Ogura	01-Mar-23			Instructor guide p.25: Added a page that instructs to fill in "template for designing and evaluating awareness program.xlsx"	01-Mar-23	02-Apr-23
6	Accepted	High	Modify	Mapping Table COM0020a	Module1~8		Time allocation needs to be revised based on actual time used in the TTT in Mongolia.	For appropreate time allocaton	-	Ogura	01-Mar-23			Changed time allocation	01-Mar-23	02-Apr-23
7	Accepted	Middle	Modify	Post test	Post test		Replace following questions with other questions: 2. Who has the primary responsibility of determining the classification level for information? 3. Which of the following is not addressed by the data retention policy? 4. A preferred technique of attackers is to become “normal” privileged users of the systems they compromise as soon as possible. This can normally be accomplished in all the following ways except which one? 5. It is important that organizations ensure that their security efforts are effective and measurable. Which of the following is not a common method used to track the effectiveness of security efforts? 6. What is the main concern with single sign-on? 7. When is it acceptable to not take action on an identified risk? 12. What is called an event or activity that has the potential to cause harm to the information systems or networks? 13. What is called the probability that a threat to an information system will materialize? 18. Which of the following is the most effective, positive method to promote security awareness? 19. Security awareness training includes: 8. How do you calculate residual risk? 17. Which of the following is considered the weakest link in a security system? 20. When speaking to an organization's human resources department	The questions are less relative to the material content, too technical or too similar to other questions.		Akiyama	21-Mar-23			Replaced with following questions: Module 1: 1. As an information security measure, Information on computers can only be accessed by authorized persons. This is an example of: a.Integrity (correct)b.Confidentiality c.Availability d.Traceability 2. Classify confidentiality of company regulations. a.Confidential b.Public (correct)c.Internal d.White Module 2: 3 What are the differences between information security and cybersecurity? a.Cybersecurity is a broader term that encompasses all data, both physical and digital. (correct)b. Information security is a broader term that encompasses all data, both physical and digital. c Common attacks in cybersecurity include illegal access, modification disclosure, alteration, and disruption. d.There is no differences 4. Basic principles of cybersecurity consist of followings except: (correct)a. Removing all threats b. Protecting information c. Enabling risk management	21-Mar-23	02-Apr-23
8	Issued	Low	Modify	Post test	Post test		Modify following questions. 1. Information classification is most closely related to which of the following? 9. The term used to denote a potential cause of an unwanted incident, which may result in harm to a system or organization is .....? 10. Which of the following term best describes a weakness that could potentially be exploited? 11. Which answer best describes a computer software attack that takes advantage of a previously unpublished vulnerability? 14. In terms or Risk Analysis and dealing with risk, which of the four common ways listed below seek to eliminate involvement with the risk being evaluated? 15. Another example of Computer Incident Response Team (CIRT) activities is:	The questions are copies of CISSP or CISM online quizlet.		Akiyama	21-Mar-23					
9																
10																
11																
12																
13																
14																
15																
16																
17																
18																
19																
20																

Appendix 3-2 Specifications of Revisions

Computer Forensic

No	Revision status	Priorities (High-Law)	Type of actions	Materials	Topics / Modules	Modification ID	Directions of Revision	Reason of the Revision	Applied framework/theories	Issued by	Date of issue	Received by	Date of received	Actions taken	Date of Submission	Date of Acceptance
1	Submitted	High	Modify	Module1 test	Module1		Module1 test Q2, the question and answer don't match. The question should be changed as: From: "The following are Processes of Digital Evidence, Except:" To: "Which of the following is types of Digital Evidence?"	To make questions clear	-	Ogura	04-Mar-23			Changed the question sentense	04-Mar-23	
2	Submitted	High	Modify	Hands On Guide	Module1~3		Add a document that describes facilities to be prepared for training.	For proper preparation of exercises	-	Ogura	04-Mar-23			Added a document "Preparation for FOR0040a exercises.docx".	04-Mar-23	
3	Submitted	High	Modify	Hands On Guide	Module1~3		Change using software-tools to the updated version which is compatible with Windows11.	For feasibility of exercises	-	Ogura	04-Mar-23			Updated software-tools	04-Mar-23	
4	Submitted	High	Modify	Hands On Guide	Module1~3		Prepare data which are required for practices.	For feasibility of exercises	-	Ogura	04-Mar-23			Prepared data which are required for practices.	04-Mar-23	
5	Submitted	High	Modify	All of tests	Module1~4		Add an item of "Name" into the test form to identify who responder is.	For proper management of test results	-	Ogura	04-Mar-23			Added an item of "Name" into the test form to identify who responder is.	04-Mar-23	
6	Submitted	High	Modify	All of tests	Module1~4		Change the setting of test form "Send responders a copy of their response" From: "Off" To: "Always" "Missed questions" From: "Off" To: "On" (Exclude of post-test) "Correct answers" From: "Off" To: "On" (Exclude of post-test) "Point values" From: "Off" To: "On"	For responders checking their answers	-	Ogura	04-Mar-23			Changed the setting of test form	04-Mar-23	
7	Submitted	High	Modify	Practical Test Module 1, Practical Test Module 3, WU-practical test.docx, Assessment of practical skill.xlsx	Module1, 3		Add sample image to Module1 Q1 Module3 Q1	To make questions clear	-	Ogura	04-Mar-23			Added sample image to Module1 Q1 Module3 Q1	04-Mar-23	
8	Submitted	High	Modify	Instructor guide,Student guide	Module2		Slide p.35, there's a typo. "Reconstruct fragments of deleted f" should be "Reconstruct fragments of deleted file" Slide p.39, there's a typo. "e tool dependencies" should be "The tool dependencies". Slide p.84. On the slide, there are words in Bahasa, "layanan yang berfungsi untuk menerima e-mail". It should be in English to keep consistency. Slide p.85. Bubbles for the previous updating work are remaining on the slide p.85. The bubbles should be removed.	To correct mistakes	-	Ogura	04-Mar-23			Revised as pointed	04-Mar-23	
9	Submitted	High	Modify	Hands On Module 2.docx	Module2		2.2. Image Mounting For Windows11, FTK imager 4.7 is available, but FTK imager 4.7 shows an error when mounting image. Alternatively, using OSFMount is available.	For feasibility of exercises	-	Ogura	04-Mar-23			Added an option to use OSFMount instead of FTK imager.	04-Mar-23	
10	Submitted	High	Modify	Practical Test Module 2, WU-practical test.docx, Assessment of practical skill.xlsx	Module2		Questions and answers of practical test need to be changed as below. Question1-3 From:/test/photo.jpg To:tes.jpg Answer1 From:Bogor To:Bogor or West Java or Indonesia Question4 Change source: From:tes.html To:File Signature.rar Question5 From:recovery.dd To:ez-recovery	For feasibility of practical test	-	Ogura	04-Mar-23			Changed questions	04-Mar-23	
11	Submitted	High	Modify	Module2 test	Module2		Module2 test Question4 seems invalid. Question: Which of the following is a form of attack via email? Answer: Brute Force password and Social Engineering	To make questions clear	-	Ogura	04-Mar-23			Changed question as "Which of the following is a form of attack on an email?"	04-Mar-23	
12	Submitted	High	Modify	Instructor guide, Student guide, mapping table, Syllabus FOR0040a Computer Forensic V1.2.docx	Module2, 3		On module2 and 3, module tests are placed before practices. Module tests should be at the end of each module.	For proper evaluation	-	Ogura	04-Mar-23			Changed the order of contents so that module tests are placed in the end of each module.	04-Mar-23	
13	Submitted	High	Modify	Hands On Module 3.docx	Module3		For case study 2, there were unclear questions and answers. Especially step6 (finding pdf and office files in a .mp4 file as steganography), a correct procedure is missing.	For feasibility of exercises	-	Ogura	04-Mar-23			Revised sentences to be clear and skipped some steps.	04-Mar-23	

Appendix 3-2 Specifications of Revisions

14	Submitted	High	Modify	WU-practical test.docx, Assessment of practical skill.xlsx	Module3		Practical test module 3 question 4 The answer seems not correct. From: "[66.68.99.53], [198.82.59.65], [65.14.7.224]; Alternative :[213.66.32.81], [65.34.1.56]" To: "[213.66.32.81], [65.34.1.56]" On FOR0040a WU-practical test.docx, added a procedure to get the answer.	For feasibility of exercises	-	Ogura	04-Mar-23			Revised answers to be correct.	04-Mar-23	
15	Submitted	High	Modify	Hands On Module 3.docx	Module3		Module3 Case study2, there's a question that participants submit a report of case study2, but no format for the report.	For feasibility of exercises	-	Ogura	04-Mar-23			Provided a format of report, that is "blank-chain-of-custody-form.pdf", in Hands on Data > USB-FOR0040 > Data for Case Study > module3 > case study	04-Mar-23	
16	Submitted	High	Modify	Instructor guide,Student guide	Module3		Slide p.47, there's a typo. "TCP/OP Model" should be "TCP/IP Model"	To correct mistakes	-	Ogura	04-Mar-23			Revised as pointed	04-Mar-23	
17	Submitted	High	Modify	Module4 test	Module4		For questions which need multiple choices (Q3, Q9), put a note of "select all of correct options" explicitly.	To make questions clear	-	Ogura	04-Mar-23			Put a note of "Select all of correct options." to each question.	04-Mar-23	
18	Submitted	High	Modify	Post test	Module4		Change the title on the top of Post test form. From: POST TEST digital forensic - JICA To: FOR0040a POST TEST	For consistency	-	Ogura	04-Mar-23			Changed the title on the top of Post test form.	04-Mar-23	
19	Submitted	High	Modify	Post test	Module4		Post test Q18, the answer is not correct. It should be changed as From: Physical To: Data Link	To correct mistakes	-	Ogura	04-Mar-23			Changed the answer.	04-Mar-23	
20	Submitted	High	Modify	Hands on Guide	Module4		P.4 Mbox viewer to EML viewer	For the feasibility of exercises. MBox viewer is old version of viewer and it doesn't work with Catalina	-	Akiyama	21-Mar-23			Changed the text and link for MBox viewer to EML viewer.	21-Mar-23	
21	Issued	Low	Modify	Instructor guide,Student guide	Module1		Slides p.74-81, 85. These slides are discussing cyber law in Indonesia. When the material is used in other countries, it's recommended to adjust contents with the country.	For open courseware	-	Ogura	04-Mar-23					
22	Issued	Low	Modify	Module1 test	Module1		Module1 test Q4, the question is about Indonesian local law. When using materials in other countries, it should be changed.	For open courseware	-	Ogura	04-Mar-23					
23	Issued	Low	Modify	Practical Test Module 2, Hands On Module 3	Module2, 3		Module2 practical test Q3 is the exactly same activity with Case study on Module3. Used file is same jpg file. At least, the jpg file should be changed on Module2 practical test.	For effectiveness of practice	-	Ogura	04-Mar-23					