PROJECT FOR HUMAN RESOURCES DEVELOPMENT FOR CYBER SECURITY PROFESSIONALS (A SHORT-TERM COURSE DEVELOPMENT)

WORK COMPLETION REPORT

SEPTEMBER 2021

JAPAN INTERNATIONAL COOPERATION AGENCY (JICA)

JAPAN DEVELOPMENT SERVICE CO., LTD. (JDS)

GP
JR
21-023

ABBREVIATIONS

APT	Advanced Persistent Threat
CS	Cybersecurity
CMMC	Cybersecurity Maturity Model Certification
CPSF	Cyber/Physical Security Framework
CSIRT	Computer Security Incident Response Team
C/P	Counterpart
DDoS	Distributed Denial of Service
ISO	International Organization for Standardization
IT	Information Technology
JICA	Japan International Cooperation Agency
METI	Ministry of Economy, Trade and Industry
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publications
PC	Personal Computer
TOR	Terms Of Reference
TTT	Train the Trainers
UI	Universitas Indonesia
USB	Universal Serial Bus
USD	US Dollar

TABLE OF CONTENTS

Appendix

LIST OF FIGURES AND TABLES

< Figures >

< Tables >

1. SUMMARY

The "Project for Human Resources Development for Cyber Security Professionals" was started in May 2019 as a five-year project. The objective of the Project is to establish the cybersecurity education system at Universitas Indonesia (University of Indonesia, hereafter referred to as UI). As part of this Project activity, we have been working to develop two cybersecurity professional courses named "Case Study & Practice: Supply chain cyber risk" (hereafter referred to as Supply Chain course) and "Case Study & Practice: How to make IT systems forensic-enabled" (hereafter referred to as Forensic course).

The following tables summarize the requirements for the courses.

Table 1 Summary of requirements for common contents to the 2 courses

1. **Supposed participants**

   The courses target full-time lecturers and guest lecturers at UI. Also, the targets are assumed to be senior lecturers who can communicate in English and have experience of teaching IT-related subjects at the university.

2. **Target course trainees**

   Senior IT engineers (with 3-5 years of experience) belonging to government, financial institutions, power companies and other critical infrastructure operators

3. **Other important points**

   (1) The courses will be part of future master courses in cybersecurity for working adults.
   (2) It is planned to publicly disclose the courses as open courseware.
   (3) It will be essential to subcontract assistance for the site surveys, course development and technology transfer to local consultants.
   (4) Trial lessons having the persons targeted for technology transfer as lecturers will be implemented.
   (5) Evaluation of the ability of the persons targeted for technology transfer will be implemented after the technology transfer.

Table 2 Summary of requirements for "Case Study & Practice: Supply Chain cyber risk"

1. **Course outline**

   The course should include the following contents:
   - Examples of incidents occurring in the supply chain
   - Standards and technologies (e.g. secure coding) that need to be known for mitigating supply chain cyber risk
   - Sample contract documents for procuring IT devices and services

2. **Goal for attainment after taking the course**

   The trainees will understand supply chain cyber risk and be able to take countermeasures in their respective organizations.

3. **Number of hours in the course**

   14 hours (7 hours x 2 days)
   However, in the case of remote lectures, it will be 3.5 hours x 4 days, considering the limits of sustained concentration of trainees.

4. **Important points to consider**

   (1) Since this will be a stand-alone course having no other associated courses, it shall be designed to provide broad coverage allowing the trainees to take a general view of supply chain cyber risk.

(2) Primarily classroom learning is anticipated, however, it shall be designed as a practical course that includes case studies (e.g. examples of disputes between customers and suppliers due to contractual issues) and practical exercises (e.g. how to state information security requirements in contract documents).

Table 3 Summary of requirements for “Case Study & Practice: Forensic enablement”

1. **Course outline and goals for attainment**

   The course should include the following contents:
   - Introduction to IT infrastructure design methods and examples with a view to obtaining logs for implementing forensic work
   - Forensic practice based on scenarios that integrate logs with consistency (e.g. in networks, hosts, and mobile devices)
   - Lectures on legislation and procedures that should be followed for utilizing forensic findings as evidence in a court of law[1]

2. **Goal for attainment after taking the course**

   The trainees will be able to understand and practice forensic methods in addressing incidents in IT systems.

3. **Number of hours in the course**

   35 hours (7 hours x 5 days)
   However, in the case of remote lectures, it will be 45 hours (5 hours x 9 days), considering the limits of sustained concentration of trainees and efficiency of the exercise.

4. **Important points to consider**

   (1) As a rule, practical exercises will be designed to be tackled by individual trainees rather than in teamwork.
   (2) Assuming that the trainees in this course have taken the following courses in advance, consistency with the contents of these courses shall be sought:
   - CHFI[2] (EC-Council)
   - ECIH[3] (EC-Council)
   - Mobile Forensic (to be developed by a local consultant)
   - Computer Forensic (to be developed by a local consultant)

   Note: At least CHFI course must be taken
   (3) It is assumed that the course trainees will later take part in the Cyber Range practice (practical attack and defense training in teams), and that the outputs of this course training will be utilized in the Cyber Range practice.
   (4) In the log analysis practice, logs obtained by the UI’s engineering department in monitoring of its own network will be utilized.

The target of the work is to make the course materials and to perform “Train the Trainers” (hereafter referred to as TTT) so that the counterparts have capability to teach these courses in the university.

The work started from October 2020 and ended in August 2021, achieving the target.

Following sections describe the detail of the activities.

[1] Contents equivalent to the Legal Rules of Evidence and Court Procedure defined as K0156 in NIST.SP800-181 (National Institute of Standards and Technology)

[2] CFHI: EC-Council Computer Hacking Forensic Investigator

[3] ECIH: EC Council Certified Incident Handler

2. IMPLEMENTATION METHOD AND PROGRESS OF THE WORK

2.1 POLICIES FOR ACHIEVING THE TARGET

At the beginning of the work, we set the following policies to ensure the development of the desired short-term course.

- **Policy 1: Course design**

  Considering that the intended trainees are not students but rather cybersecurity professionals who work in corporations and government agencies, the course contents will be designed to leverage the experience and knowledge of the trainees. Specifically, the ratio of classroom learning will be reduced while the ratio of case studies and practical exercises will be increased to ensure that the trainees are compelled to make full use of their own knowledge and experience. Doing so will enable the trainees to gain authentic experiences in real workplace environments and acquire the practical skills required in the "Goals for attainment after taking the course".

- **Policy 2: Experts**

  The following three experts will be assigned in consideration of the workload and aptitude.

  Expert 1: Work chief / Course development (also in charge of Supply chain course)

  This expert has experience of implementing JICA projects, in particular overseas cybersecurity projects and undertakings for developing specialized courses in universities and possesses experience and qualifications in information security management. He also has experience of working in an information systems department in the manufacturing industry, in which there is a high level of supply chain dependence, and experience of preparing contract documents with related companies and specification documents for information system equipment. Moreover, the expert has experience of implementing similar work in Indonesia and be capable of managing the smooth progress of the work.

  Expert 2: Cybersecurity & Forensic expert

  This expert has experience of CSIRT work and handling incidents in real work situations. He also has experience of not only forensic but also designing and installing Cyber Range and developing and implementing Cyber Range practical exercises.

  Expert 3: Cybersecurity & Forensic expert

  This expert has experience of system development, operation and maintenance and is endowed with sufficient knowledge and experience concerning network, server and PC management and settings.

- **Policy 3: Utilization of local consultants**

It will be essential to subcontract work to local consultants in the Project. Specifically, a contract will be signed with a local cybersecurity company to consign assistance for the surveys, course development and technology transfer necessary for implementing the work. Considering that Japanese experts cannot travel to Indonesia due to the impact of COVID-19, it is possible that these local consultants will act as classroom facilitators in remote lessons, so it will be necessary to recruit human resources who are endowed with a certain degree of skills in the specialist fields.

The contents to be consigned to the subcontracted local consultants are summarized below.

- Fact-finding survey of supply chain cyber risk in Indonesia
- Fact-finding survey of forensic work by important infrastructure operators in Indonesia
- Assistance in developing course materials
- Assistance in building the practical exercise environment (it is possible that the local consultants will be asked to perform the entire construction)
- Assistance in advancing the technology transfer (it is possible that remote lessons will be implemented)

2.2 CONTENTS OF THE WORK AND IMPLEMENTATION STEPS (PLAN AND ACTUAL)

The next table shows the planned contents of the work and implementation steps. The actual results are indicated with a right arrow symbol (→) followed by highlighted result (Yellow=Done, Grey=Not done). Note that the term "Counterpart" is abbreviated as "C/P" in the table.

Table 4 Contents of the work and implementation steps

Division	Work	Implementation Contents and Methods
First pre-preparation work in Japan	Grasping the Project progress	・ Contact the Project side, and obtain and review Project-related materials to understand the background and progress of the Project, caution points and any other details. Also obtain information on the persons targeted for technology transfer. → Done by 27 Nov. 2020 ・ Conduct TV conferences with the Project staff when necessary. → Communicated with Project staff and C/Ps using Slack and Zoom as needed
	Preparation and approval of the work plan	・ Prepare the work plan (Japanese language) and submit it to JICA headquarters and the Project side (provide explanations when necessary). → Done on 13 Nov. 2020 ・ Prepare the work plan (English language) and obtain approval from the Project side. → Done by 13 Nov. 2020
	Confirmation of related courses and the practical exercise environment	・ Confirm the contents of the ECIH and CHFI courses. → Done on 01 Nov. 2020 ・ Obtain materials and confirm contents concerning the Mobile Forensic course and Computer Forensic course developed by the local consultants. → Not done because those 2 courses were not developed at that timing.

Division	Work	Implementation Contents and Methods
		・ Confirm the quality of the network necessary for remote lessons. → Not done because no gathering session was planned due to COVID-19
	Preparation of course materials (supply chain and forensic)	・ Prepare the following course materials (all English language) for the 2 courses: - ~~Course concept~~ (Removed because not specified in TOR) - Syllabus - Texts (text for trainees and text for teachers) The texts for teachers should state the number of hours and important points to consider for each topic). - Auxiliary teaching materials (e.g. slides) → Done by 29 Jan 2021 ・ Prepare questionnaires for evaluating ability before and after the technology transfer. → Done by 29 Jan 2021
	Recruitment of the local consultants and consignment of the start of work	・ Select the local consultants and sign the contract. → Done by 28 Dec. 2020 ・ Consign survey related to supply chain and forensic. → Done on 28 Dec. 2020 ・ Obtain the findings of the supply chain survey. → Survey for supply chain cyber risk was conducted from 4 Jan 2021 until 31 Mar 2021.
First TTT (Supply Chain course)	Explanation of course materials to the C/Ps, and evaluation of the C/Ps' ability	・ Explain the course materials to the C/Ps and the Project side. → Done on 3 Feb 2021 ・ Have the C/Ps fill out the ability evaluation questionnaire. → Done on 8 Feb 2021 ・ Evaluate the ability of the C/Ps. → Done on 8 Feb 2021
	Implementation of TTT	・ Using the course materials, implement technology transfer in the form of lessons with the C/Ps. → Done from 9 Feb to 11 Feb 2021
	Implementation of trial lessons and guidance	・ Have the C/Ps implement trial lessons (partial) If possible, implement the trial lessons upon inviting the actual corporate cybersecurity staff targeted for the training. → Done on 12 and 15 Feb 2021 ・ Appropriately offer guidance on the implementation methods. → Done on 12 and 15 Feb 2021
	Post-technology transfer ability evaluation	・ Have the C/Ps fill out the ability evaluation questionnaire. → Done on 12 and 15 Feb 2021 ・ Evaluate the ability of the C/Ps. → Done on 15 and 16 Feb 2021
	Discussions about correcting the course materials	・ In light of the technology transfer results, discuss making corrections to the course materials with the C/Ps and reach conclusions. → Done on 16 Feb 2021
	Meetings with the Project	・ In light of the technology transfer results, exchange opinions on the future approach to work. → Done on 16 Feb 2021
Second preparation work in Japan	Correction and revision of the course materials (Supply Chain course)	・ Based on the results of discussing making corrections to the course materials for the Supply chain course, correct and revise the materials. → 1st: Done from 17 Feb to 22 Feb 2021 → 2nd: Done from 5 Jul to 11 Aug 2021 ・ Share the results with the C/Ps and the Project side via TV conference, etc. → Done on 13 Aug 2021

Division	Work	Implementation Contents and Methods
	Acquisition of survey findings from the local consultants (Forensic)	・ Obtain the survey findings concerning forensic. → Survey was conducted from 15 Apr 2021 until 29 Jun 2021
	Preparation of the course materials (Forensic course)	・ Prepare the following course materials (all English language) for the Forensic course: - ~~Course concept~~ (Removed because not specified in TOR) - Syllabus - Texts (text for trainees and text for teachers) The texts for teachers should state the number of hours and important points to consider for each topic). - Auxiliary teaching materials (e.g. slides) → Done by 09 Jul 2021 ・ Prepare questionnaires for evaluating ability before and after the technology transfer. → Done by 09 Jul 2021
	Implementation of trial lessons for the local consultants (forensic)	・ Conduct remote trial lessons to deepen the understanding of local consultants who undertake local lecture support. → Briefing of the contents: Done on 12 Jul 2021 ・ After the trial lessons, reflect any bugs or improvements points in the course materials. → Not done because no suggestion was given
Second TTT (Forensic course)	Explanation of course materials to the C/Ps, and evaluation of the C/Ps' ability	・ Explain the course materials to the C/Ps and the Project side. → Done by 21 Jul 2021 ・ Have the C/Ps fill out the ability evaluation questionnaire. → Done on 26 Jul 2021 ・ Evaluate the ability of the C/Ps. → Done on 26 Jul 2021
	Meeting with the local consultants	・ Hold discussions with the local consultants concerning the work implementation. → Done on 12 Jul 2021
	Implementation of TTT	・ Using the course materials, implement technology transfer in the form of lessons with the C/Ps. → Done on 26, 28, 29 Jul and 02, 04, 05, 06 Aug 2021
	Implementation of trial lessons and guidance	・ Have the C/Ps implement trial lessons (partial) If possible, implement the trial lessons upon inviting the actual corporate cybersecurity staff targeted for the training. → Done on 10 and 12 Aug 2021 ・ Appropriately offer guidance on the implementation methods. → Done on 10 and 12 Aug 2021
	Post-technology transfer ability evaluation	・ Have the C/Ps fill out the ability evaluation questionnaire. ・ Evaluate the ability of the C/Ps. → Done on 10 and 12 Aug 2021
	Discussions about correcting the course materials	・ In light of the technology transfer results, discuss making corrections to the course materials with the C/Ps and reach conclusions. → Done on 12 Aug 2021
	Meetings with the Project	・ In light of the technology transfer results, exchange opinions on the future approach to work. → Done on 10 and 12 Aug 2021
Wrap-up work in Japan	Finalization of the course materials	・ If the C/Ps and the Project side have any opinions for improving the course materials, reflect them and finalize the course materials. → Done on 13 and 16 Aug 2021 ・ Share the results with the C/Ps and the Project side via TV conference, etc. → Done on 24 Aug 2021
	Preparation of the work completion report, and reporting	・ Prepare the work completion report. ・ Report to JICA headquarters.

2.3 OVERALL WORK SCHEDULE AND THE RESULT

The overall work schedule is attached as Appendix B. It shows both plan and actual results.

The initial plan included two field works for TTT implementation, but due to the unpredictable COVID-19 situation, discussions with the Project staff and C/P was conducted at an early stage of this work, it was decided that all operations would be conducted in Japan. In this case, the TTT will be conducted online remotely, but since the Forensic course TTT is focused on practical exercises it was decided to conduct it in a group remote style that means participants gather in a physical classroom at UI. The timing of the TTT was postponed to June or later in consideration of the UI semester break. On the other hand, the Supply Chain course does not have any practical exercise, so it was held in February during the lockdown as originally planned, with participants participating remotely from their homes.

However, in June, because the situation of COVID-19 was not improved, it was judged that the gathering session is impossible, so the TTT of the Forensic course was also conducted remotely by letting participants join from their homes from 26th of July to 12th of August. The presence of local consultants was helpful in this implementation. We asked them to prepare USB memory sticks with copying the huge data for exercises and send them to the participants' homes, and also, they provided detailed follow-up services in Indonesian during the TTT. As a result, we were able to complete the Forensic course TTT without any trouble.

2.4 EXPERTS

The next table shows the experts of the work.

Table 5 List of experts

Name	Role	Major tasks
Yasumitsu ISHIKAWA	Work chief / Supply Chain course development	・ Operation and coordination of the work ・ Contact point to JICA ・ Manage local consultant ・ Support other experts ・ Make syllabus ・ Make course material ・ Create, implement, and analyze surveys ・ Perform TTT ・ Conduct trial lesson ・ Make reports
Yuta MIYAUCHI	Forensic course development	・ Make syllabus ・ Create survey and analyze ・ Make course material ・ Perform TTT ・ Conduct trial lesson
Akira HONDA	Forensic course development	・ Make course material ・ Support TTT ・ Support trial lesson

3. RESULTS OF THE WORK

3.1 PRELIMINARY SURVEYS

Preliminary surveys were conducted for both the Supply Chain course and Forensic course. The results are compiled in Appendix C and Appendix D accordingly. The purpose of the surveys was to know the actual situation in Indonesia of each field (supply chain and forensic) and the results are introduced in the course texts. If the course content needs to be adapted to the Indonesian situation, the text will need to be modified. The next table summarizes the result of the surveys.

Table 6 Summary of preliminary surveys

No.	Survey name	Summary
1	Supply chain cyber risk survey	· Survey type: Online questionnaire · Number of requested respondents: 125 · Number of visits: 59 · Number of responses: 31 · Period: From 4 Jan 2021 until 31 Mar 2021 [Summary of questions] Q1 ~Q7: Profile of individual and company Type of industry, Sales volume, Respondent's affiliated department, title, etc. Q8~Q18: Question for user (entruster) companies Issues in contractor selection, Implementing security controls, Security clauses in contract, etc. Q19~Q29: Question for contractor companies Issues in proposals, Implementing security controls, Usage of sub-contractors, Experience of cyber incident, etc. Q30: Free comment
2	Digital forensic survey	· Survey type: Online questionnaire · Number of requested respondents: 139 · Number of visits: 85 · Number of responses: 25 · Period: From 15 Apr 2021 until 29 Jun 2021 [Summary of questions] Q1 ~Q6: Profile of individual and company Type of industry, Sales volume, Respondent's affiliated department, title, etc. Q7 ~Q15: Questions for Digital forensic Presence of forensic function, forensic tools, occurrence of security incidents, training, etc.

3.2 MAKING COURSE MATERIALS

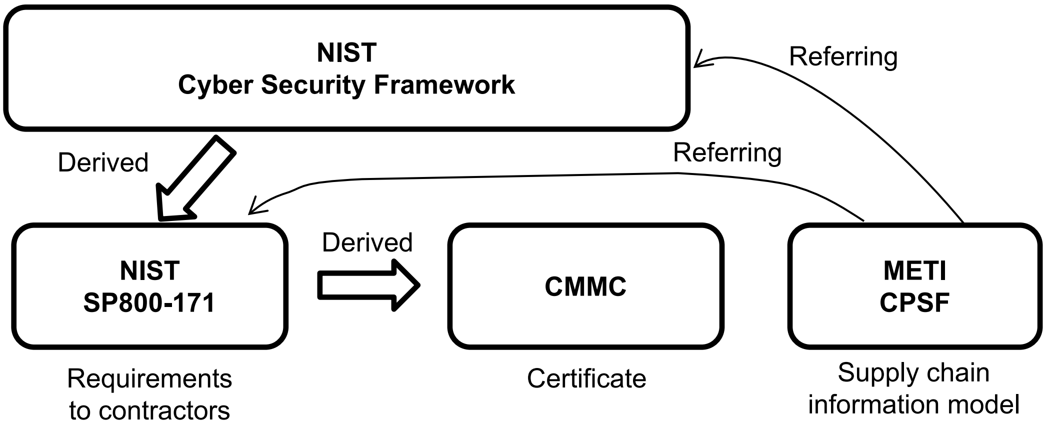
The courses was designed and implemented to fulfill the requirements described in Table 1, Table 2 and Table 3. Below are indicated the points for making the course materials.

➢ **Supply Chain course**

Although there is a lot of literature and guidelines on supply chain cyber risk management in the world, the concept is relatively new and there is no standard that companies can adopt without hesitation. Therefore, the following guidelines were set in the development of this course to ensure consistency.

- Clarify the relevance of referenced documents based on the standards, guidelines, and frameworks published by NIST[4] in the United States, which can be said to be the global standard for cyber security.
- Introduce the history and latest trends in supply chain cyber risk management standards. This makes it possible to ride the tide of the field.
- Introducing supply chain information models that can be applied in recent years to the future, which are necessary for discussing supply chain cyber risks.

As a result, the content of this course was structured as follows.



NIST Cyber Security Framework: Framework for Improving Critical Infrastructure Cybersecurity
NIST SP800-171: NIST Special Publications 800-171 “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
CMMC: Cybersecurity Maturity Model Certification”
METI CPSF: Cyber/Physical Security Framework (by Ministry of Economy, Trade and Industry, Japan)

Figure 1 Structure of Supply Chain course, Supply Chain course text

[4] NIST: National Institute of Standards and Technology

The next table lists the created course materials of Supply Chain course.

Table 7 List of course material (Supply Chain course)

No.	File name	Description
1	Syllabus_SupplyChain_rev04.docx	Syllabus
2	01_Supply_Chain Introduction Rev03.pptx	Chapter 1 Introduction
3	02_Supply_Chain Cybersecurity risks in the supply chain Rev02.pptx	Chapter 2 Cybersecurity risks in the supply chain
4	03_Supply_Chain NIST Cyber Security Framework and SP 800-171 Rev04.pptx	Chapter 3 NIST Cyber Security Framework and SP 800-171
5	04_Supply_Chain Cybersecurity Maturity Model Certification (CMMC) Rev04.pptx	Chapter 4 Cybersecurity Maturity Model Certification (CMMC)
6	05_Supply_Chain Contract Rev02.pptx	Chapter 5 Consideration for cybersecurity in contracts
7	Data-Security-Contract-Clauses-for-Service-Provider-Arrangements.pdf	Data Security Contract Clauses for Service Provider Arrangements
8	Data-Security-Contract-Clauses-for-Service-Provider-Arrangements (Indonesian).docx	Data Security Contract Clauses for Service Provider Arrangements (Indonesian version)
9	files/ folder	Several documents to be referred during the class

Every slide in the Power Point documents has notes for guiding the lecturer on how to explain the slide.

The next table is the course syllabus of Supply Chain course.

Table 8 Course syllabus (Supply Chain course)

Course Title	Case Study & Practice: Supply Chain Cyber Security Risks
Course Objective	The participants are expected to understand the supply chain cybersecurity risks and be able to take countermeasures in their respective organizations.
Participants	IT engineers (with 3-5 years of experience) who are responsible for doing one or more of followings. - Making specification document for the development of software, hardware or systems which have connection to the Internet. - Making contract document for purchasing software, hardware or services which have connection to the Internet. - Performing acceptance test or security evaluation of delivered products which have connection to the Internet. - Designing or making software, hardware or services which have connection to the Internet. - In charge of cybersecurity in the organization
Prerequisites	- The participants should have at least 3 years of working experience in IT field. - The participants should have basic cybersecurity knowledge, such as types of cyber-attacks and the mechanism.
Course goals	After completing this course, participants are: 1) Able to explain the types of cybersecurity risks from a supply chain perspective. 2) Able to take countermeasures in their respective organizations against supply chain cybersecurity risks. Especially participants know how to write the appropriate contract document to remove / mitigate cybersecurity risk. 3) Able to explain the content of international standard / framework of supply chain cybersecurity (NIST Cybersecurity framework, SP800-171, CMMC, etc.)
Course contents and schedule (1 day = 7 teaching hours)	**[Day 1]** **1. Introduction** • Cybersecurity basics - Types of cyber attacks - Today's cyber attacks - Common cybersecurity risk management in organizations

	2. Cybersecurity risks in the supply chain • Supply chain - What is supply chain? - Characteristics and examples of supply chain in each industrial sector - Cyber Physical Security Framework (CPSF) by METI Japan • Trend of cybersecurity incidents in the supply chain - Global trend - Situation in Indonesia ➢ **Exercise 1:** Identification of cybersecurity risks in the supply chain in each industrial sector. Techniques and examples of cyberattacks targeting the supply chain **3. NIST Cyber Security Framework (CSF) and SP800-171** • Overview of standards, frameworks and guidelines regarding supply chain cybersecurity • NIST Cyber Security Framework 1.1 • How to apply CSF to the organization? ➢ **Exercise 2:** Applying CSF to your organization. Make profile for your organization. • Summary of SP800-171 **[Day 2]** **1. Cybersecurity Maturity Model Certification (CMMC)** • Summary of CMMC • How to comply with CMMC ➢ **Exercise 3:** Discussion on implementing CMMC in your organization. **2. Contracts and cybersecurity risk management** • Cybersecurity risk management in work outsourcing ➢ **Exercise 4:** Practice in preparing a work outsourcing contract document. • Cybersecurity risk management in procurement of products and services ➢ **Exercise 5:** Practice in preparing a specification document for ordering products (or services) • Consideration in contract negotiation (from both the acquirer's and supplier's point of view) **3. Wrap-up**
Scheme of Instructions	Lecture 60 %, Hands-on training 40 % (Hands-on training includes exercises and case studies)
Keywords	Cybersecurity, Supply chain, Risk management, ISO 28000, NIST Cybersecurity Framework, Contract, Subcontractor
Tools (software) required for hands-on training	N. A.
Reference books	• ISO 28000 A Complete Guide - 2020 Edition [ISBN 0655916679] • Supply Chain Risk Management (Internal Audit and IT Audit) 1st Edition [ISBN 978-1138197336] • NIST Cyber Security Framework https://www.nist.gov/cyberframework/framework • NIST SP800 documents https://csrc.nist.gov/publications/sp800 • CMMC portal https://www.acq.osd.mil/cmmc/

- **Forensic course**

The Forensic course consists of 31 exercises including 6 scenario-based digital forensics practices. The scenarios contain Website defacement, Unauthorized access, DDoS attack, Ransomware attack and APT attack. The IoC (Indicator of Compromise = Evidence on devices that points out to a security breach) was created for each scenario using virtual computing / network environment shown in next diagram.

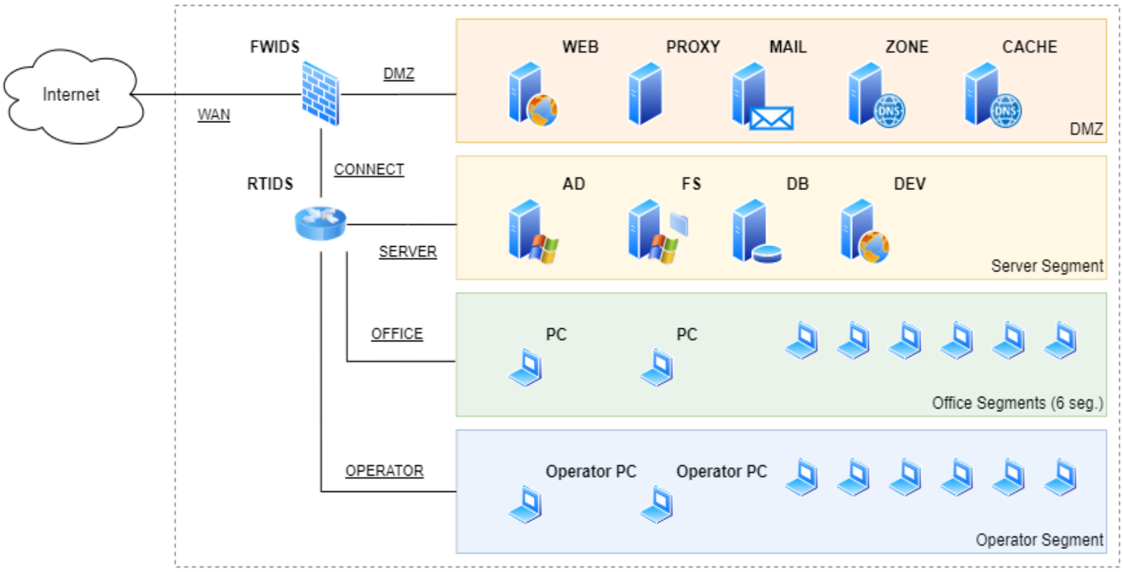


Figure 2 Virtual computing / network environment for IoC creation

Information about the configuration of servers and network devices, as well as some log files and dump files, can be given to the participants to analyze, making the exercise very realistic.

Table 9 List of course materials (Forensic course)

No.	File name	Description
1	Syllabus_Forensic_rev02.docx	Syllabus
2	INTRODUCTION_TTT.pptx	Summary of the course
3	Module0_Lecture-rev2.pptx	Module0 Introduction
4	Module0_Workbook-rev2.pptx	Workbook for Module0
5	Module1_Lecture-rev2.pptx	Module1 DFIR: Digital Forensics and Incident Response
6	Module1_Workbook-rev2.pptx	Workbook for Module1
7	Module2_Lecture-rev2.pptx	Module2 How to Design Secure IT Infrastructure
8	Module2_Workbook-rev2.pptx	Workbook for Module2
9	Module3_Lecture-rev2.pptx	Module3 Scenario-based DFIR Training
10	Module3_Workbook-rev2.pptx	Workbook for Module3
11	Module3_Worksheet-rev2.xlsx	Worksheet for Module3 Exercises
12	Module4_Lecture-rev2.pptx	Module4 Conclusions - How to make IT systems forensic enabled
13	DFIR_USB/ folder	IoC files (logs, core/disk images, etc.) used in exercises Note: The size is 155GB

Every slide in the Power Point documents has note which guides the lecturer how to explain the slide.

The next table is the course syllabus of Forensic course.

Table 10 Course syllabus (Forensic course)

Course Title	Case Study & Practice: How to Make IT Systems Forensic-enabled
Course Objective	The participants are expected to understand how to design forensic-enabled IT systems and how to investigate security incidents.
Participants	IT engineers (with 3-5 years of experience) who are responsible for doing one or more of followings. - Performing incident response if a security incident happens - Designing a secure IT system to prevent serious damage from the incidents
Prerequisites	• The participants should take following courses in advance. - CHFI (EC-Council) - ECIH (EC-Council) • The participants should have basic knowledge of cybersecurity, network and IT systems. e.g., 3-Tiers architecture, NTFS file system, TCP/IP, email protocols (SMTP, IMAP), Domain Name System, Malware types.
Course goals	After completing this course, participants are: 1) Able to understand and practice forensic method in addressing security incidents in IT systems. 2) Able to design an IT infrastructure that can record and collect logs needed for digital forensics.
Course contents and schedule (1 day = 7 teaching hours)	**[Day 1 - 2]** • **Module 0 Introduction** - Course introduction - Exercise 1: Set up your laptop • **Module 1 DFIR: Digital Forensics and Incident Response** - Security incidents in today's world - Case study 1: Common types of cyberattacks - Incident response life cycle - Digital forensics: Collection, Examination, Analysis and Reporting - Exercise 1 - 9: How to use forensics tools, investigating the incident **[Day 3]** • **Module 2 How to Design Secure IT Infrastructure** - Design secure IT infrastructure - Case study 2: Actual case of forensics and incident response - Exercise 1 - 3: Investigate typical logs and identify what happened • **Module 3 Scenario-based DFIR Training** - Scenario 1 (Exercise 1 - 4): Analysis and creating a report **[Day 4]** • **Module 3 Scenario-based DFIR Training (cont.)** - Scenario 2 - 4 (Exercise 5 - 12): Analysis and creating a report **[Day 5]** • **Module 3 Scenario-based DFIR Training (cont.)** - Exercise 5 - 6 (Exercise 13 - 19): Analysis and creating a report • **Module 4 Conclusions - How to make IT systems forensic enabled** - How to make IT systems forensic enabled
Scheme of Instructions	Lecture 25 %, Hands-on Training 75%
Keywords	Incident response life cycle, Digital forensics, Chain of Custody, Defense-in-depth
Tools (software) required for hands-on training	All tools will be installed in Exercise 1 of Module 0. - CDIR-Collector (Fast forensics tool) - Winpmem (Memory dumping tool) - FTK Imager (Disk imaging and memory dumping tool) - Autopsy (Digital forensics platform) - The Sleuth Kit (Disk image investigation tool) - log2timeline (Timeline creation tool) - Notepad++ (Text editor) - Timeline Explorer (Viewer for CSV and Excel) - Wireshark (Packet analysis tool)

	- CDIR-A (Data parser for CDIR-Collector) - WinPrefetchView (Viewer for prefetch) - Event Log Explorer (Viewer for Windows Event Log) - Autoruns (Viewer for auto-starting programs) - RegRipper (Registry investigation tool) - Registry Explorer (Viewer for registry) - The Volatility Framework (Memory dump analysis tool)
Reference books	- Incident Response & Computer Forensics, McGraw-Hill Education, ISBN 978-0071798686. - Practical Packet Analysis, No Starch Press, ISBN 1593278020. - Intelligence-Driven Incident Response, O'Reilly Media, ISBN 978-149134944

3.3 PERFORMING TTT

TTTs for 2 courses were performed in February 2021 for Supply Chain course and July to August 2021 for Forensic course. The Supply Chain course had an additional supplemental TTT on 13 August 2021 to explain modified content. The participants in TTT for the 2 courses are listed in following tables.

Table 11 List of participants (Supply Chain course TTT/ Forensic course TTT)

(Supply Chain course TTT)

No.	Mr/Ms	Name	Organization
1	Mr.	Muhammad Salman	UI
2	Mr.	I Gde Dharma Nugraha	UI
3	Mr.	Yan Maraden	UI
4	Mr.	F. Astha Ekadiyanto	UI
5	Mr.	Muhammad Rakha Rafi Baihaqi	BSSN
6	Ms.	Asriza Yolanda	BSSN
7	Ms.	Sri Chusri Haryanti	Universitas YARSI
8	Mr.	Henki Bayu Seta	Universitas Pembangunan Nasional veteran Jakarta
9	Mr.	Alfiansyah	BSSN
10	Mr.	Irmansyah	Bogor Agricultural University
11	Mr.	Nashrul Hakiem	Universitas Islam Negeri Syarif Hidayatullah Jakarta
12	Mr.	Sigit Puspito Wigati	PT. CloudTech
13	Mr.	Agus Wicaksono	iCIO Community
14	Mr.	Victor Arief Maulana	PT.Faradina
15	Mr.	Bisyron Wahyudi	CSIRT.ID

(Forensic course TTT)

No.	Mr/Ms	Name	Organization
1	Mr.	Abdul Hakim Nur Maulana	BSSN
2	Mr.	Arif Rahman Hakim	Cyber Security Department, Politeknik Siber dan Sandi Negara
3	Ms.	Diyanatul Husna (*)	
4	Mr.	Eliando	Department of Information System, Faculty of STEM, University of Matana
5	Mr.	Elvian	UI
6	Mr.	Ferry Astika Saputra	Department of Informatics and Computer Engineering Politeknik Elektronika Negeri Surabaya
7	Mr.	Hamdan Abdul Aziz	Chaosmatic (Company)
8	Mr.	I Gde Dharma Nugraha (*)	UI
9	Mr.	Ruki Harwahyu	UI
10	Mr.	Sukma Aji Triatmojo	IdNSA
11	Mr.	Yan Maraden	UI

Note: (*) denotes that he / she joins the TTT as an observer

3.4 EVALUATION OF TTT PARTICIPANTS

Each participant's ability as a teacher was measured using multiple factors such as attendance rate, evaluation of questionnaires and evaluation of trial lesson. In the Forensic course, submitted worksheets, which record the progress and result of exercises, are also be used for the evaluation. The following sections describe the method of ability measurement for each course.

➢ **Supply Chain course**

(1) Calculate the score from 0 to 5 according to the attendance result. [A]

Attendance score = Attended time slots / Total time slot * 5

Where "time slot" corresponds to morning or afternoon. (1 day = 2 time slots)

(2) Calculate the score from 1 to 5 based on the answers in the questionnaire. [B]

i.e.) For the question "Are you confident to teach chapter 1?", the score is assigned according to the answer such as "Not confident"=1, "OK but need assistance"=2, "OK but need further review"=3, "OK with little review"=4, "OK no problem"=5

(3) Rate the performance of trial lesson for each participant (0 - 5). The rating score sheet which contains the rating criteria is attached as Appendix E [C]

(4) Calculate the overall score from 0 to 10 by compiling [A] [B] and [C] with giving weight. The formula is as below.

Overall score = [A] / 5 * 3 + [B] / 5 * 2 + [C] / 5 * 5

The next table is the actual result of evaluation of Supply Chain course.

Table 12 Evaluation result of TTT participants (Supply chain)

Supply Chain Risk course eval < 1.0 < 7.5

No.	Name	Attendance score (weight=3)	Questionnaire (weight=2)	Mock class score (weight=5)	Total score (10.0)	Mock class comments
1	A	3.0	1.9	4.8	9.7	- He has very good presentation skill. He added some slides to complement the difficult content. - Excellent lecturer
2	B	3.0	1.6	3.1	7.7	- He totally changed the material, and presented different theory of incident response. - Should not deviate from the original purpose. - But his effort to improve the quality can be evaluated.
3	C	3.0	1.5	3.3	7.8	- She just read the material. - Need to review the contents
4	D	3.0	1.6	3.6	8.2	- He just read the material. - Need review before teaching
5	E	3.0	1.6	4.4	9.0	- He tried to let student understand by explaining details for each item. - Can be a good teacher.
6	F	3.0	0.7	3.6	7.3	- He just read the material. - Need review before teaching
7	G	3.0	1.3	4.5	8.8	- He has very good presentation skill. - Can be a good teacher. Students will like him.
8	H	3.0	1.0	3.3	7.3	- He just read the material and skipped few important items. - Need support to teach
9	I	3.0	1.4	3.5	7.9	- He just read the material. - Need to improve his teaching skill
10	J	3.0	1.2	3.5	7.7	- He just read the material. - Need review before teaching
11	K	3.0	1.5	4.6	9.1	- He has very good presentation skill. He reviewed the contents very well. - Can be a good teacher.
12	L	3.0	1.0	3.5	7.5	- She may need review of the material so that she can explain the content well. - Need support to teach
13	M	3.0	1.8	4.4	9.2	- He has good presentation skill. - Can be a good teacher.
14	N	3.0	1.4	4.6	9.0	- He has very good presentation skill. He prepared well for this mock class. - Can be a good teacher. Students will like him.

➢ Forensic course

(1) Calculate the score from 0 to 5 according to the attendance result. [A]

$$\textit{Attendance score} = \textit{Attended time slots} / \textit{Total time slot} * 5$$

Where "time slot" corresponds to morning or afternoon. (1 day = 2 time slots)

(2) Calculate the score from 1 to 5 based on the answers in the questionnaire. [B]

i.e.) For the question "Are you confident to teach chapter 1?", the score is assigned according to the answer such as "Not confident"=1, "OK but need assistance"=2, "OK but need further review"=3, "OK with little review"=4, "OK no problem"=5

(3) Rate the performance of trial lesson for each participant (0 - 5). The rating score sheet which contains the rating criteria is attached as Appendix E. [C]

(4) Evaluate the performance of exercise based on the worksheets submitted by participants (0 - 5). The worksheet contains the record of the progress and result of participant's exercise. [D]

(5) Calculate the overall score from 0 to 10 by compiling [A] [B] [C]and [D] with giving weight. The formula is as below.

$$\textit{Overall score} = [A] / 5 * 2 + [B] / 5 * 2 + [C] / 5 * 3 + [D] / 5 * 3$$

The next table is the actual result of evaluation of Forensic course.

Table 13 Evaluation result of TTT participants (Forensic)

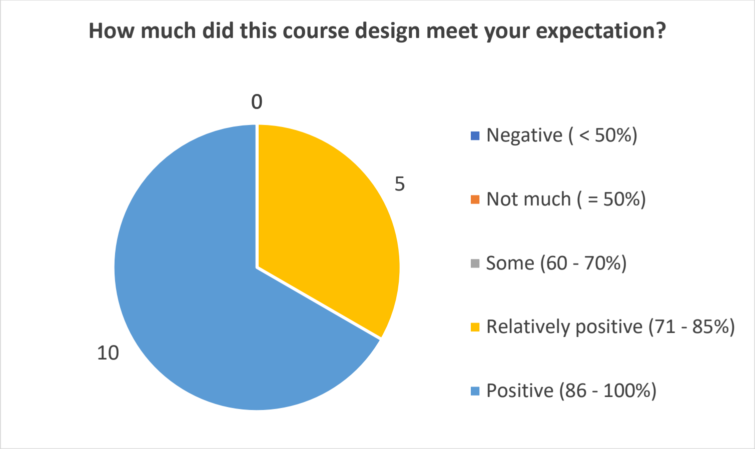
Forensic Enablement course evaluation

No.	Name	Attendance score (weight=2)	Questionnaire (weight=2)	Exercise score (weight=3)	Mock class score (weight=3)	Total score (10.0)	Exercise comments (About submitted worksheet)	Mock class comments
1	**A**	**2.0**	**2.0**	**1.2**	**2.5**	**7.7**	- Most of contents are copied from text material (-) - He may not understand well (-) - Seems limited technical knowledge in countermeasure columns (-)	- He skipped few items (-) - He prepared online quiz to attract students (+)
2	**B**	**1.9**	**1.7**	**3.0**	**2.6**	**9.2**	- He filled timelines and IoC by his own effort, but seems copied in other part (+) - The countermeasures he filled in are appropriate and well considered (+)	- He basically read the contents (-) - He prepared online quize.9 questions to attract students (+)
3	**C**	**1.8**	**1.5**	**1.8**	**2.6**	**7.7**	- Most of contents are copied from text material (-) - The cause analysis is appropriate (+) - Countermeasures are biased to narrow idea (-)	- He prepared a video lecture by himself (0) - The explanation is very clear and understandable (+) - Q&A is appropriate (+) - Took longer time than expected (-)
4	**D**	**2.0**	**1.6**	**3.0**	**2.5**	**9.1**	- He copied timelines and IoC but did analysis by his own effort (+) - The countermeasures he filled in are appropriate and well considered (based on his wide knowledge) (+)	- Skipped page 127 - 129 (-) - The time per slide is longer more than expected (-) - He understands the contents (+)
5	**E**	**1.8**	**1.6**	**3.0**	**2.6**	**8.9**	- He filled timelines and IoC by his own effort. But some other parts are copied. (+) - The analysis he added are appropriate (+) - The countermeasures he filled in are appropriate and well considered (+)	- He understands the contents well (+)
6	**F**	**1.9**	**1.5**	**1.8**	**2.5**	**7.7**	- Timeline is not sorted by time. Not well compiled (-) - About 70% of contents are copied from others, therefore unable to evaluate (-)	- He understands the contents well (+) - Time allocation is good. (+)
7	**G**	**2.0**	**1.4**	**3.0**	**2.7**	**9.1**	- He copied timelines and IoC but did analysis by his own effort (+) - The countermeasures he filled in are appropriate and well considered (based on his wide knowledge) (+)	- He took 10 min for his introduction. Should be OK in actual class but not in mock class (0) - He used highlighter to explain. It's effective (+) - He understand the contents well (+)
8	**H**	**1.9**	**1.1**	**1.8**	**2.6**	**7.3**	- Timeline is not sorted by time. Not well compiled (-) - About 70% of contents are copied from others, therefore unable to evaluate (-)	- He explained with concrete examples (+) - Time allocation is good (+)
9	**I**	**2.0**	**1.2**	**3.0**	**2.8**	**9.0**	- He solved all exercises by his own effort (+) - The cause analysis and countermeasures are well described and appropriate (+)	- He explained with concrete examples (+) - He try to keep student being concentrated (+) - His explanation is very clear and understandable (+) - His teaching skill and technique are good (+)

3.5 EVALUATION OF COURSE MATERIALS AND EXPERTS

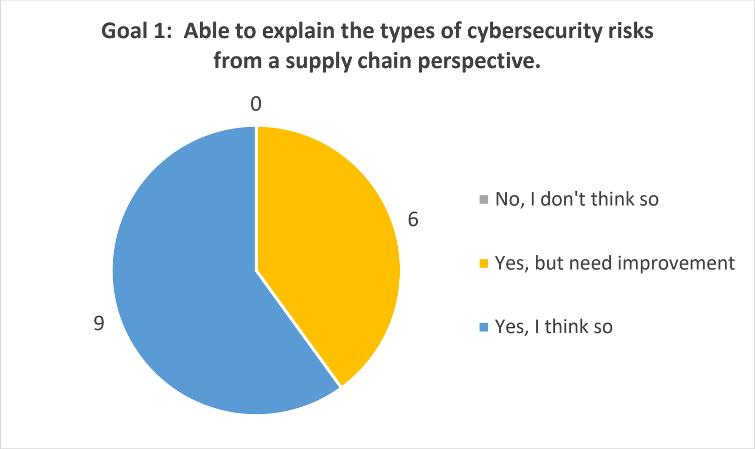
The design of the courses, course materials and experts who conducted the TTTs are evaluated by participants using online questionnaire. The results are shown as follows.

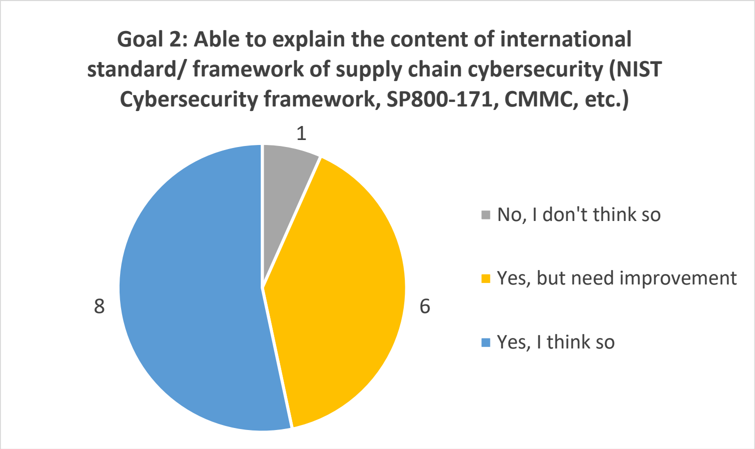
- **Supply Chain course**



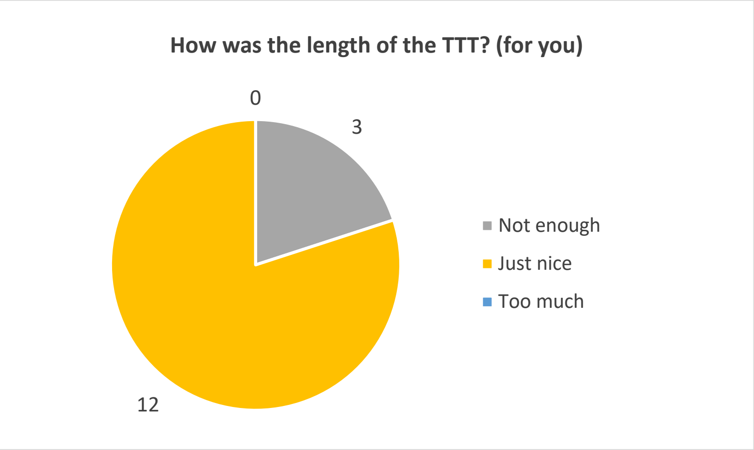
All participants responded positively.

[Question] Do you think the course goals can be achieved with this design? Please select the respective answer for each goal.

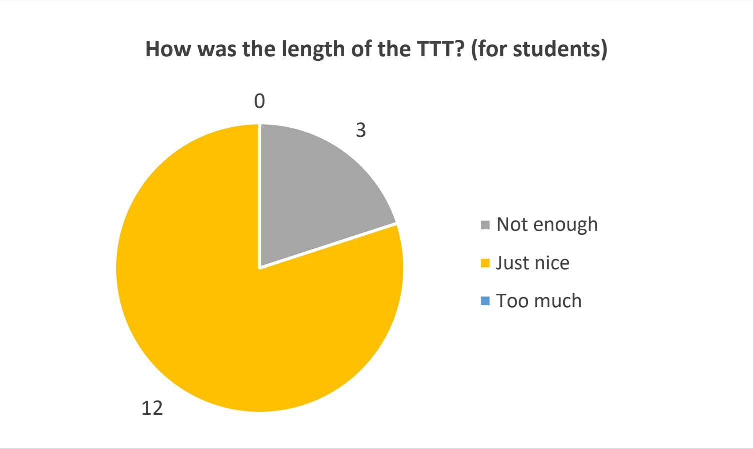




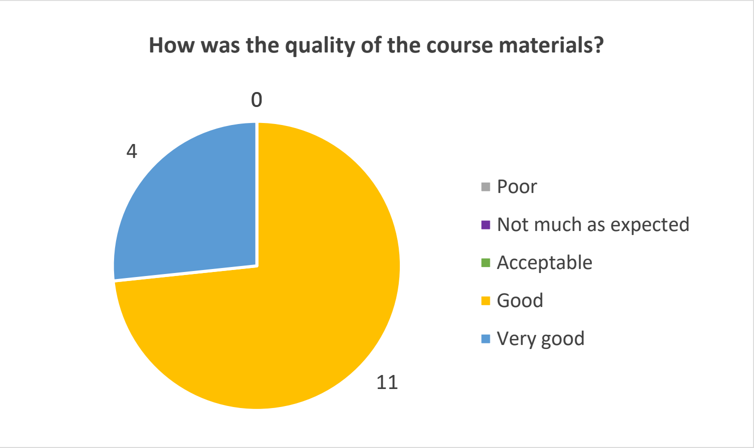
There are 2 negative answers “No I don’t think so” in Goal 2. The reasons for the answers are unknown because the respondents said “Why i chose the answer”. It might be a sinple mistake.



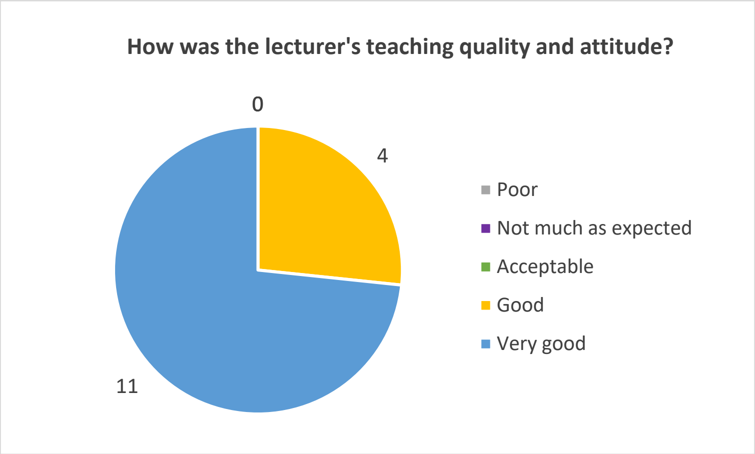
The length of the TTT should be OK.



The length of the course should be OK.

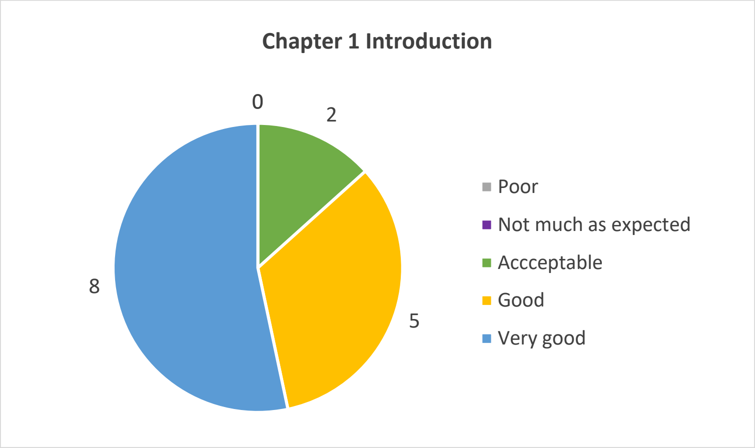


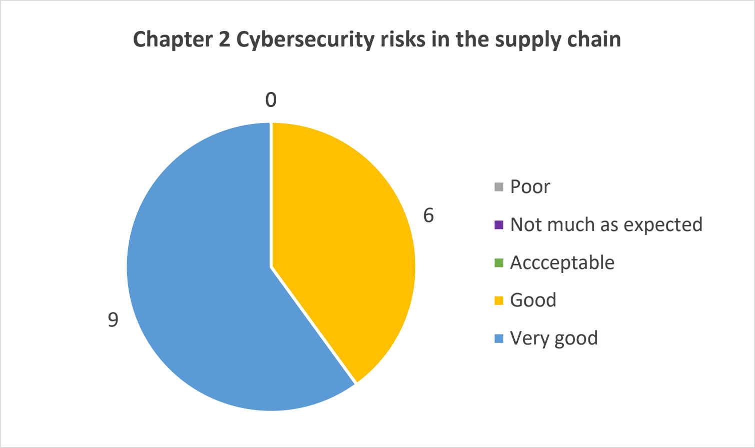
The quality of the course materials is OK.

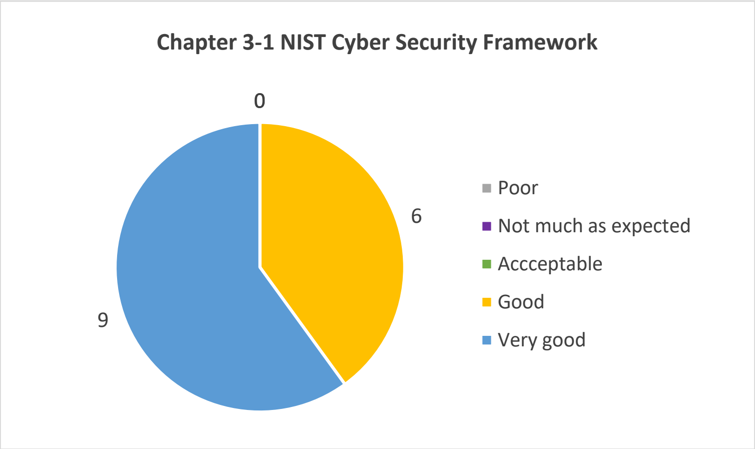


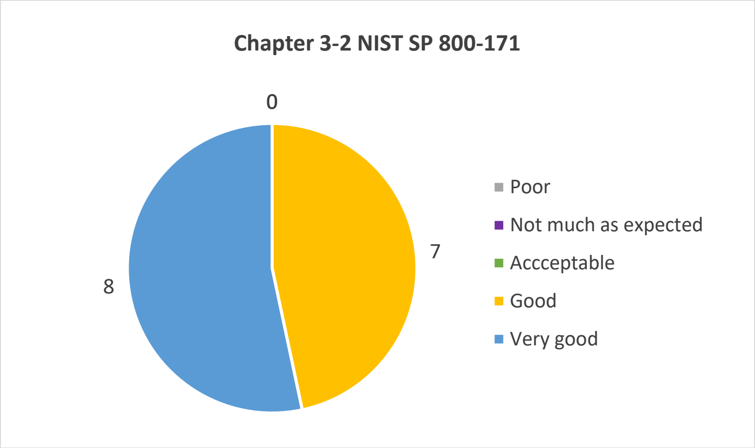
The quality and attitude of the TTT lecturer were OK.

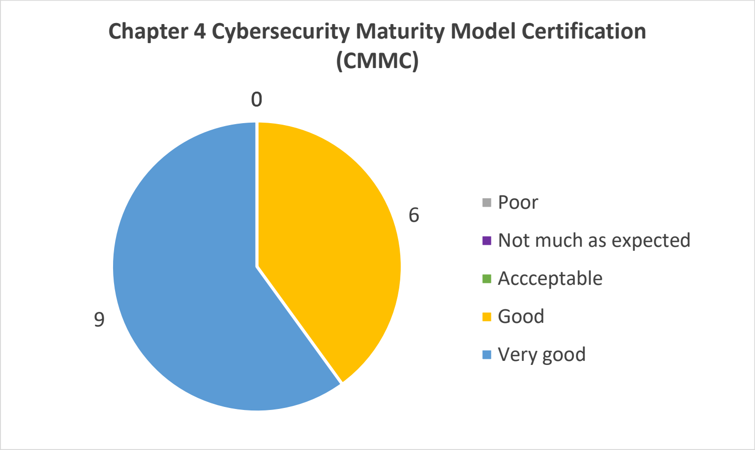
[Question] How was the quality of the course contents?

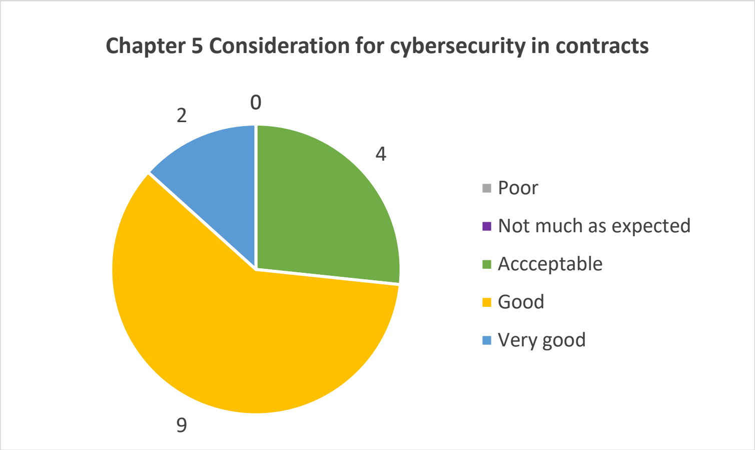





Chapter 3-1 NIST Cyber Security Framework
0
6
9
Poor
Not much as expected
Accceptable
Good
Very good

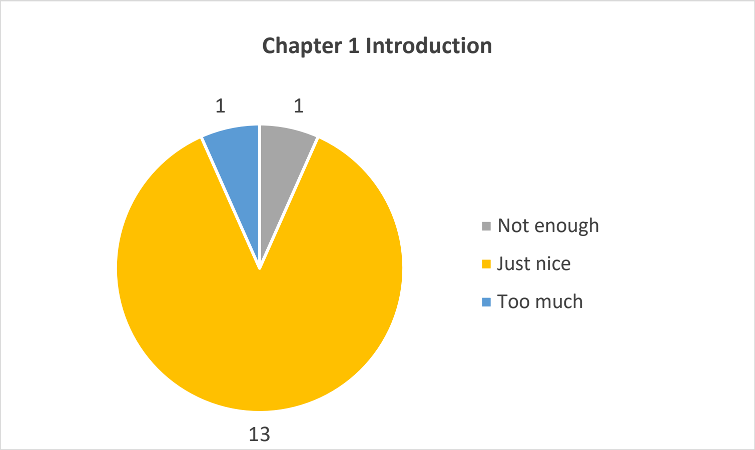

Chapter 3-2 NIST SP 800-171
0
7
8
Poor
Not much as expected
Accceptable
Good
Very good

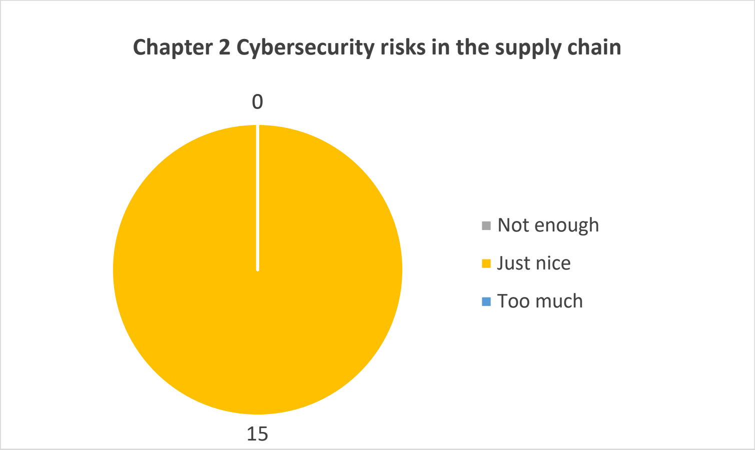

Chapter 4 Cybersecurity Maturity Model Certification (CMMC)
0
6
9
Poor
Not much as expected
Accceptable
Good
Very good

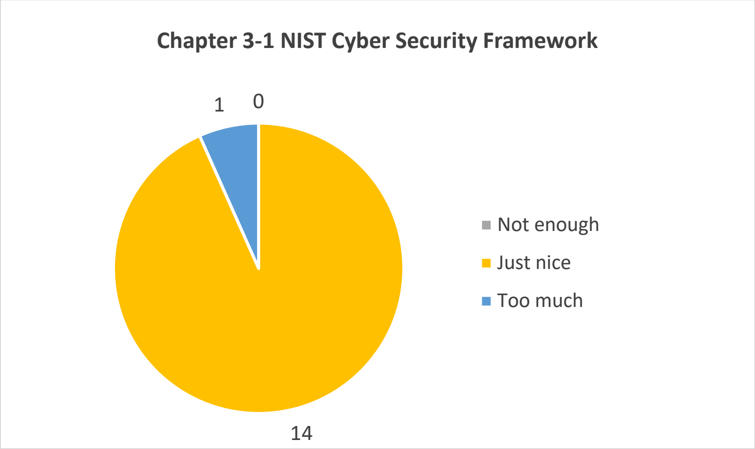

Chapter 5 Consideration for cybersecurity in contracts
2
0
4
9
Poor
Not much as expected
Accceptable
Good
Very good

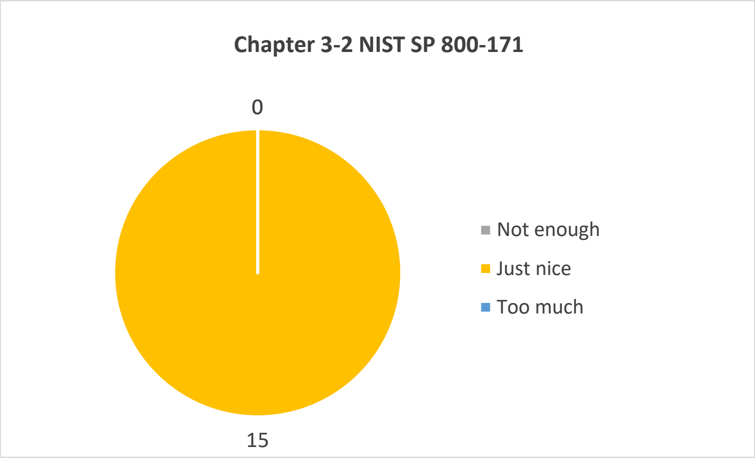
The quality of each content is OK.

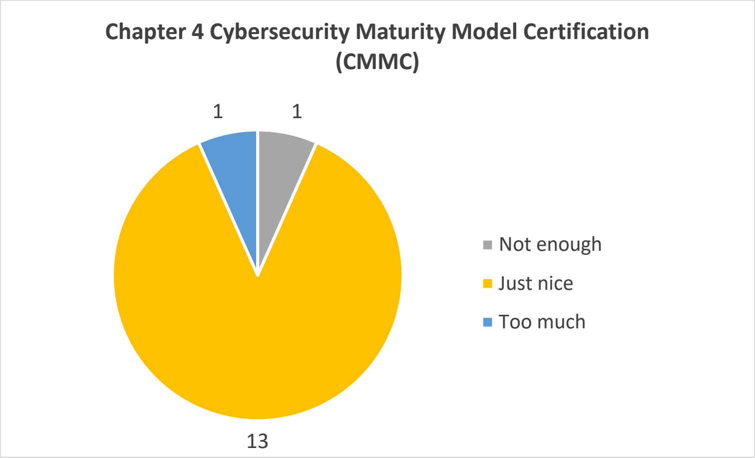
[Question] How was the volume of the course contents?

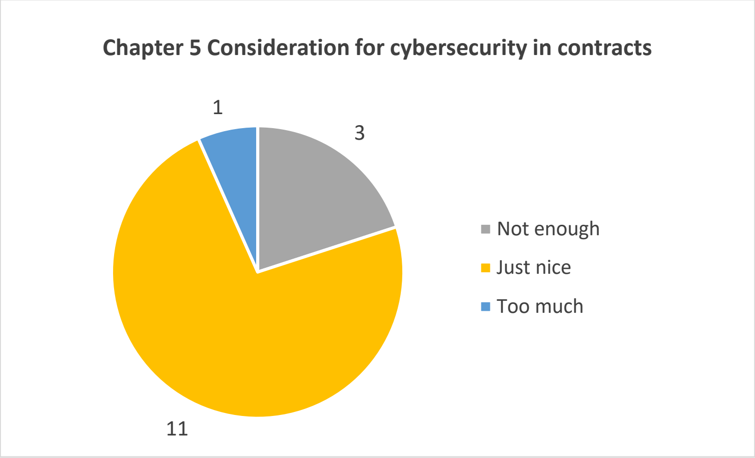






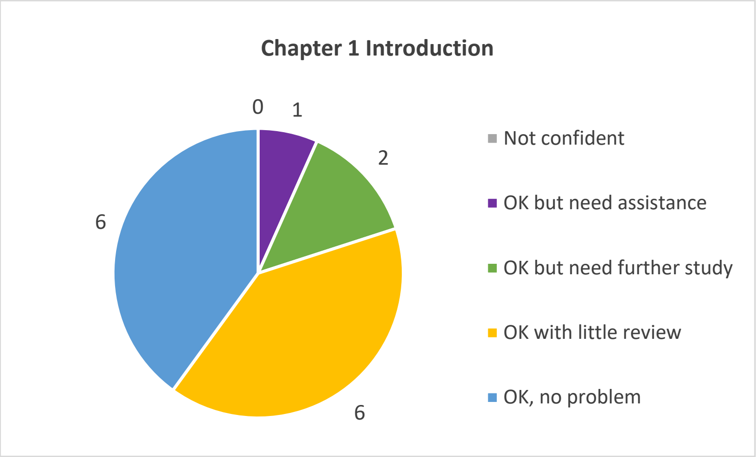


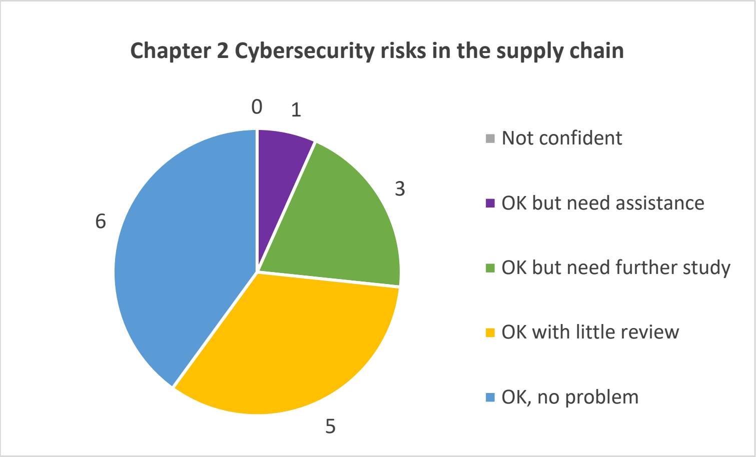


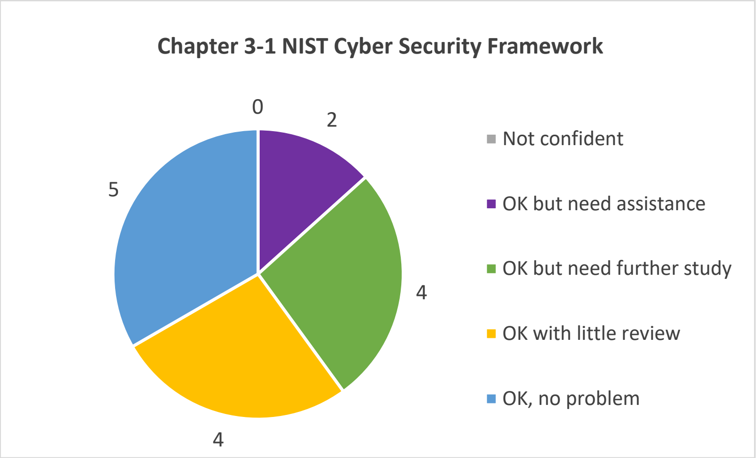


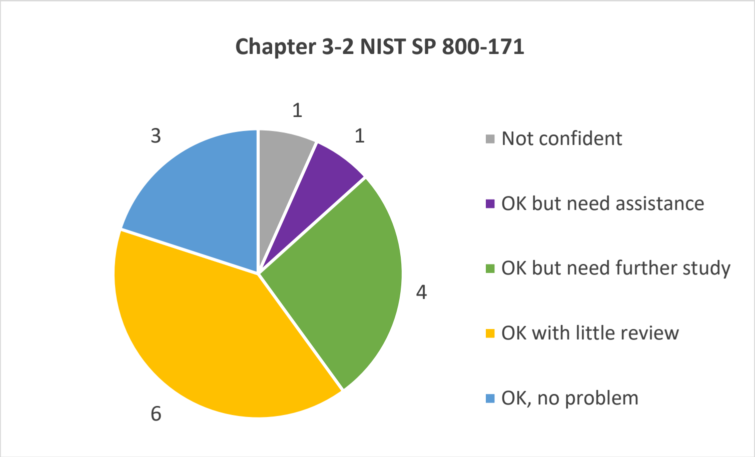
The volume of Chapter 1, Chapter 4 and Chaper 5 is evaluated as “Not enough” by 1 or 2 participants. The volume has been increased after this survey and shared among the participants.

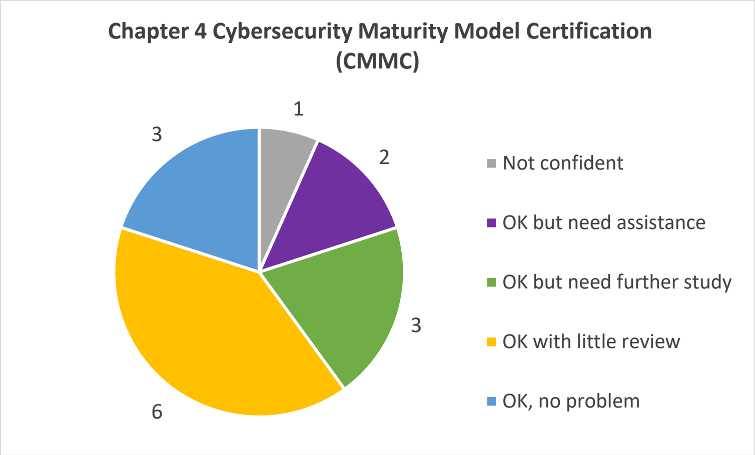
[Question] Are you confident in teaching the topic?

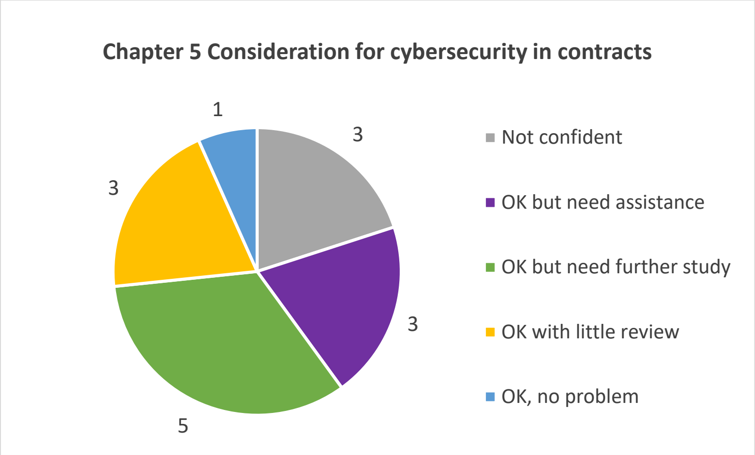




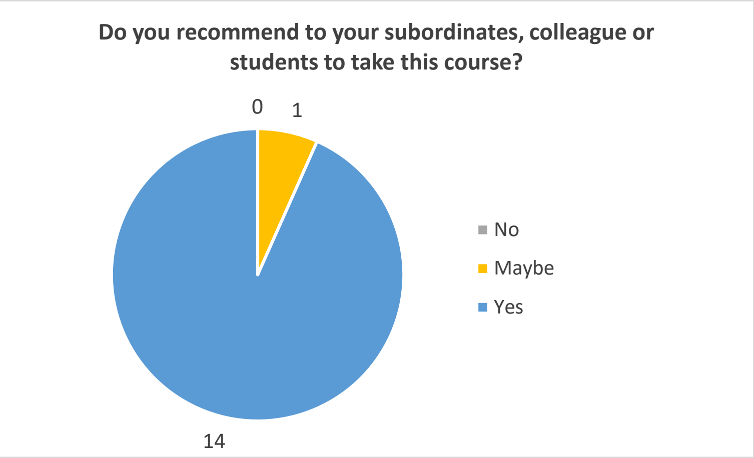






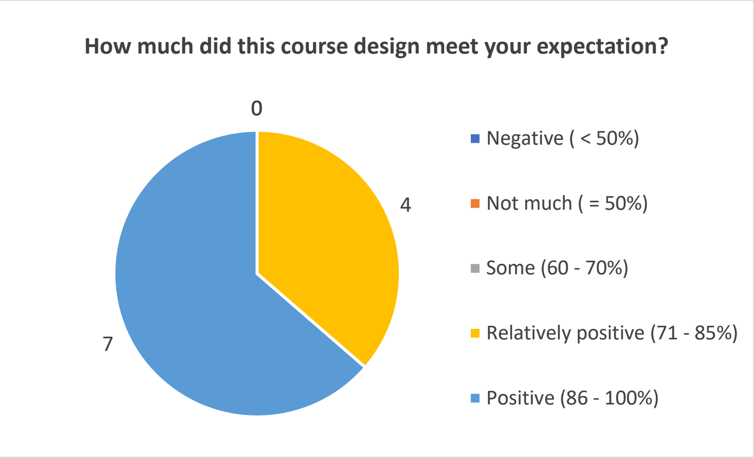


One participant answered "not confident" on important topics (SP 800-171, CMMC and contracts). This is considered to be a problem of the participants' comprehension. As for the topic "Consideration for cybersecurity in contracts", it seems relatively difficult because it contains a lot of legal jargon.



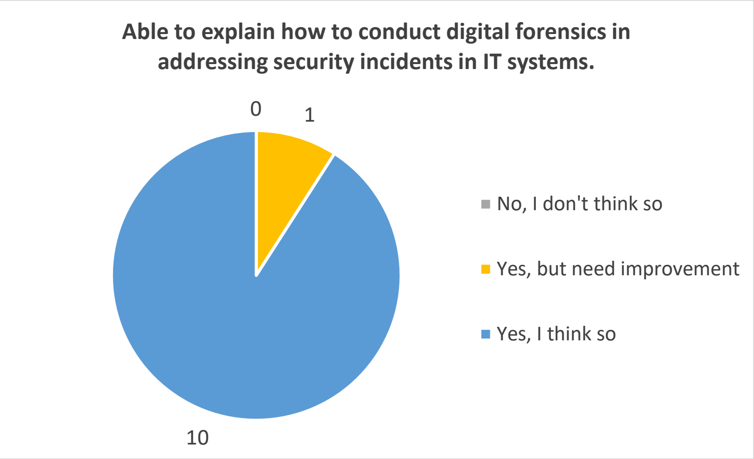
It is good to be recommended.

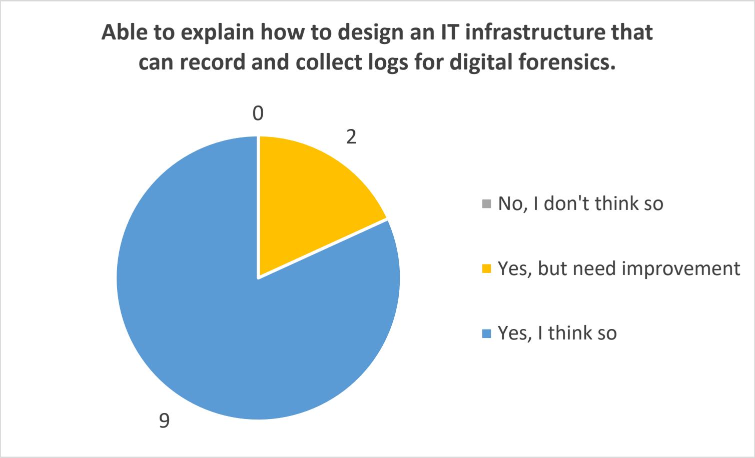
- **Forensic course**



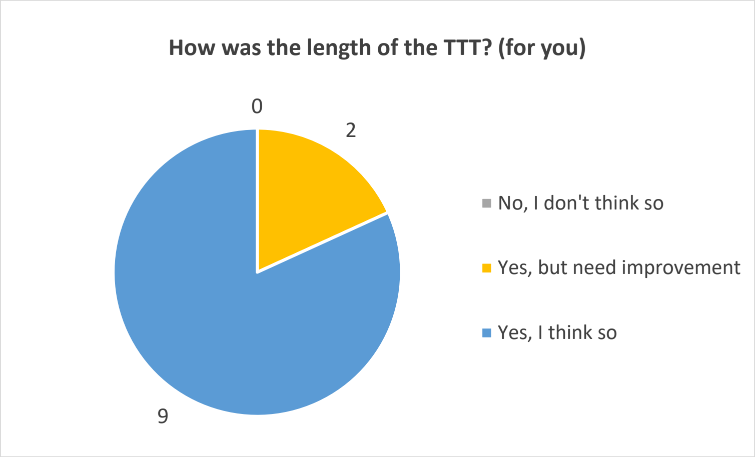
All participants responded positively.

[Question] Do you think the course goals can be achieved with this design? Please select the respective answer for each goal.

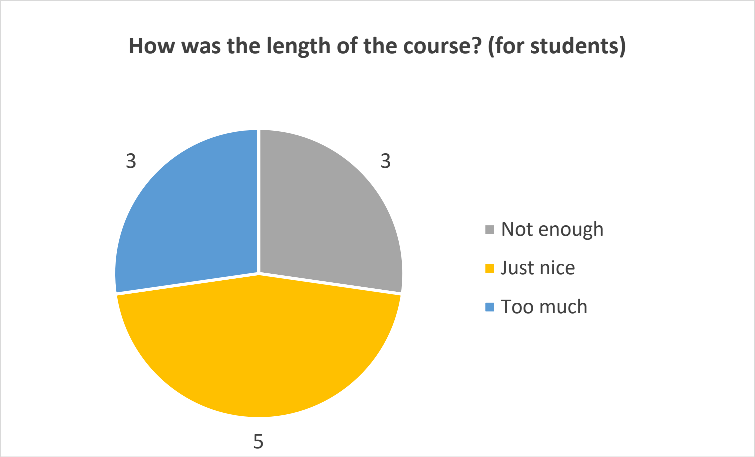




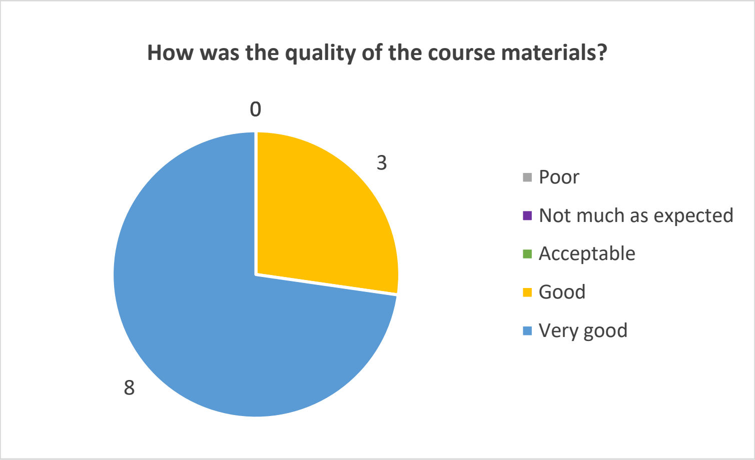
They think the course goals can be achieved.



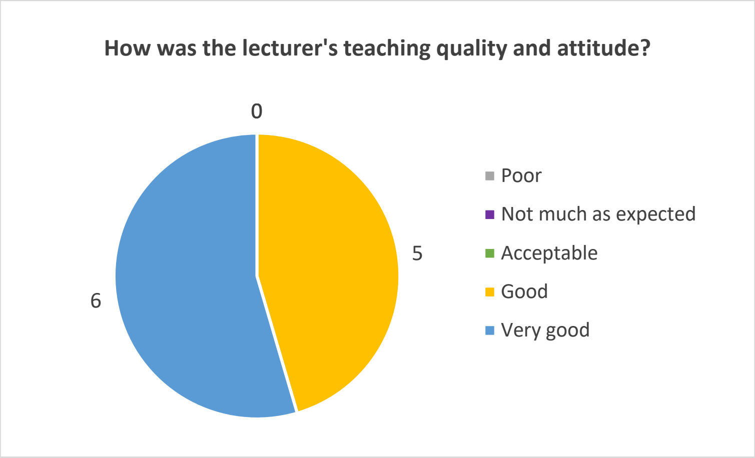
The TTT length should be OK.



The course length should be OK.

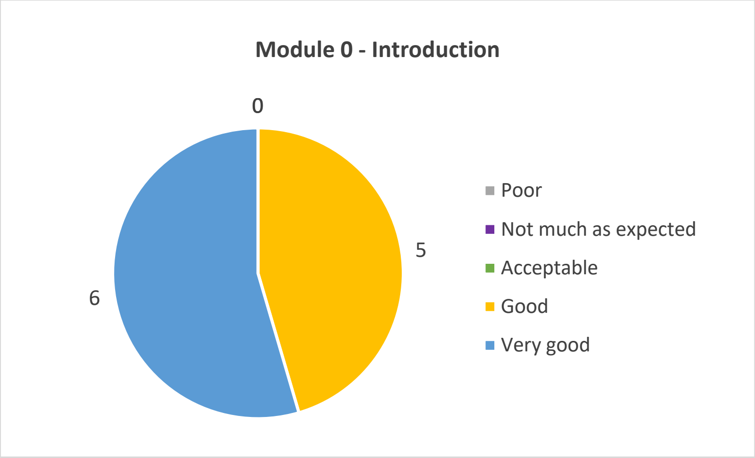


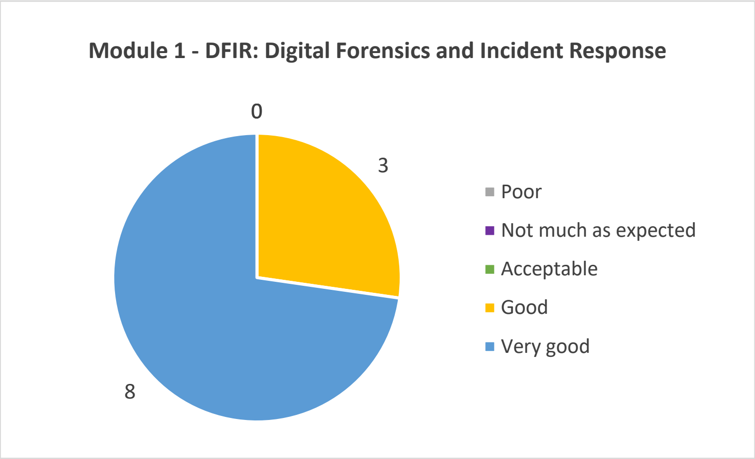
The quality of course material is OK.

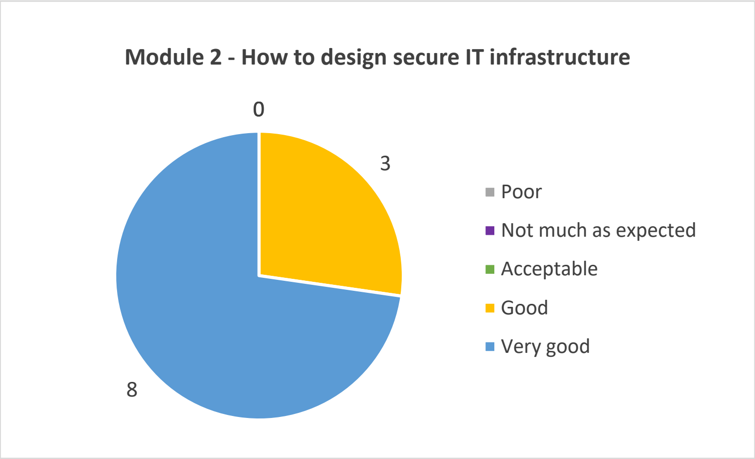


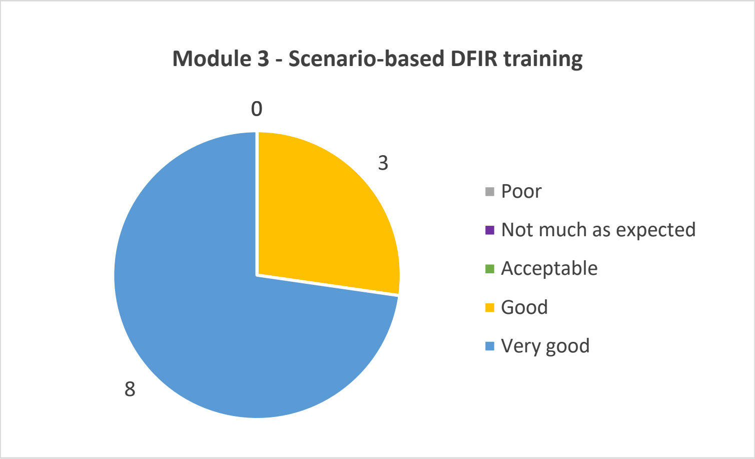
The quality and attitude of the TTT lecturer were OK.

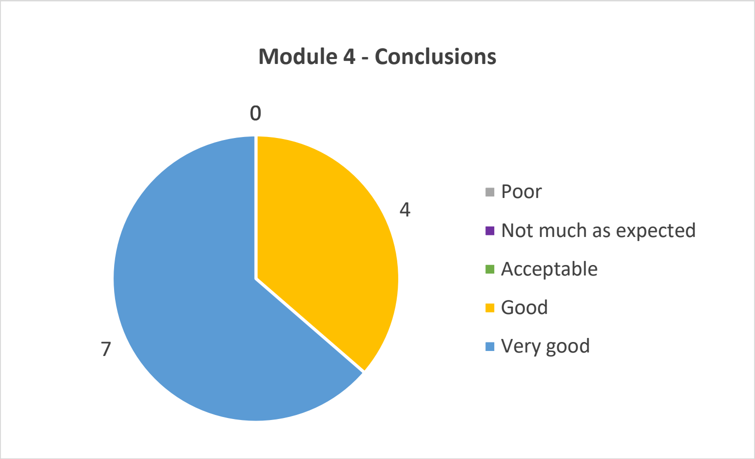
[Question] How was the quality of the course contents?




Module 1 - DFIR: Digital Forensics and Incident Response
0
3
8
Poor
Not much as expected
Acceptable
Good
Very good

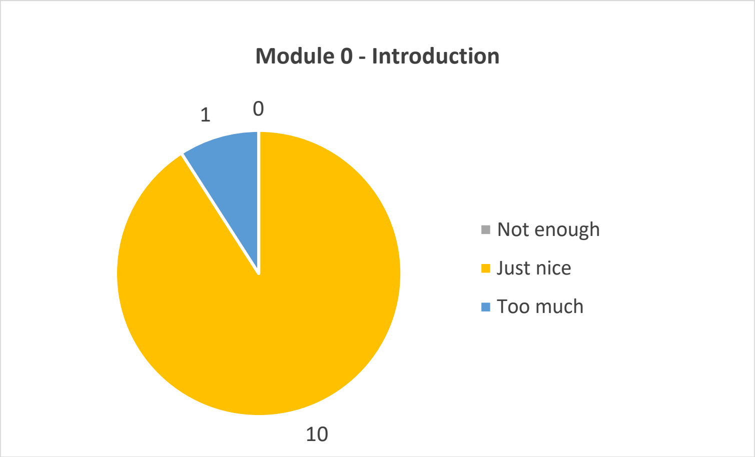

Module 2 - How to design secure IT infrastructure
0
3
8
Poor
Not much as expected
Acceptable
Good
Very good

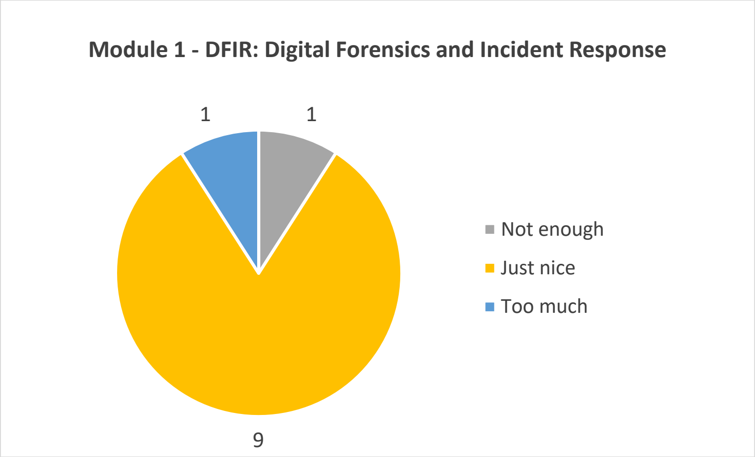

Module 3 - Scenario-based DFIR training
0
3
8
Poor
Not much as expected
Acceptable
Good
Very good

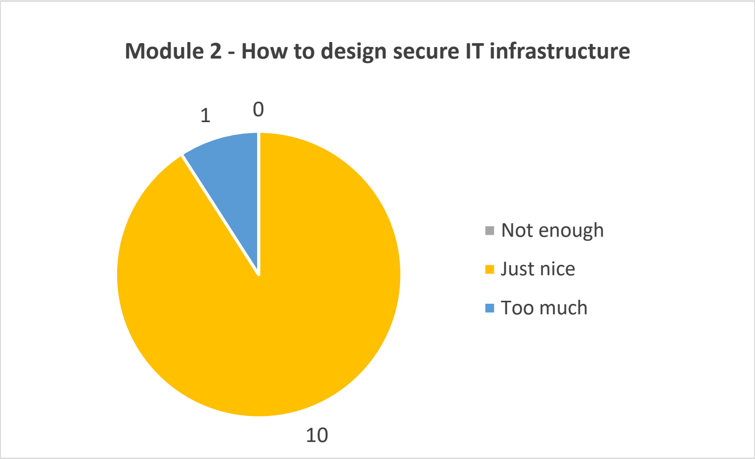


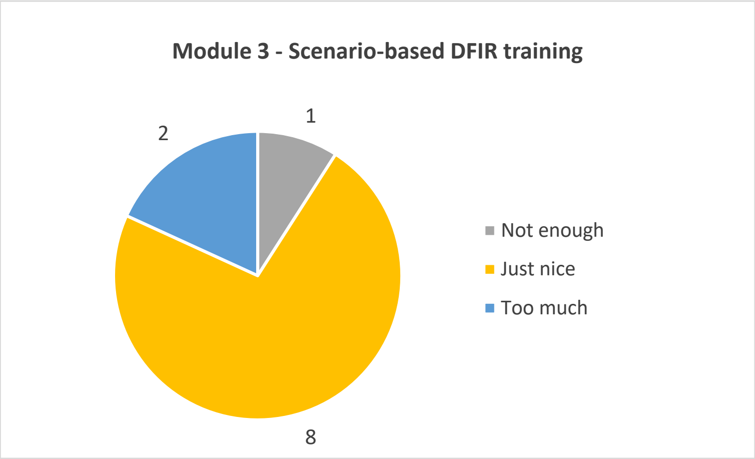
The quality of every content is OK.

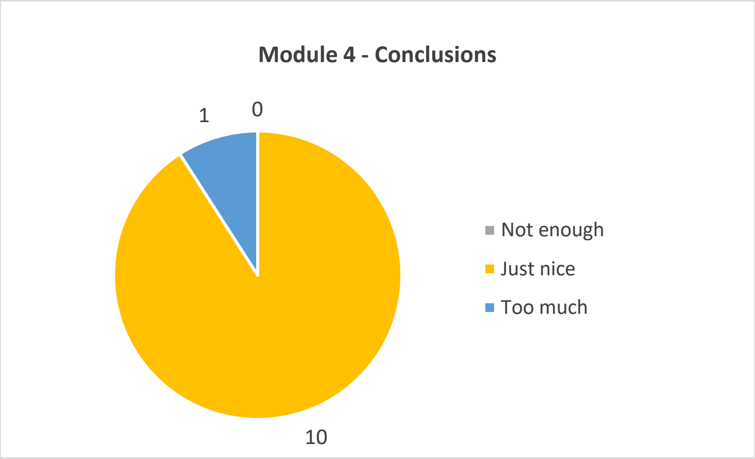
[Question]　How was the volume of the course contents?





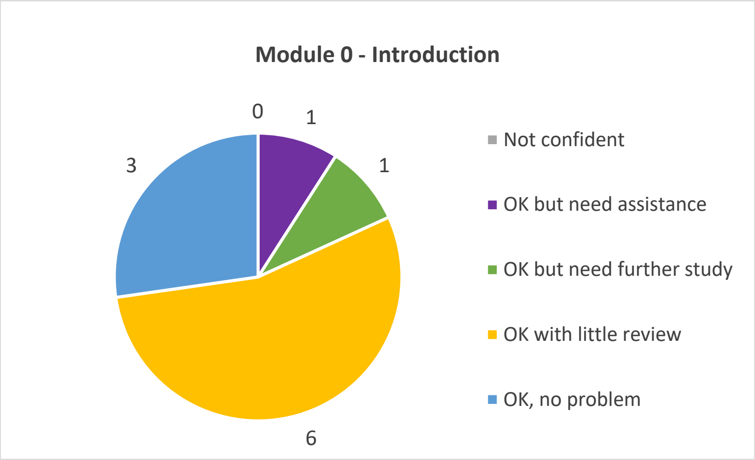


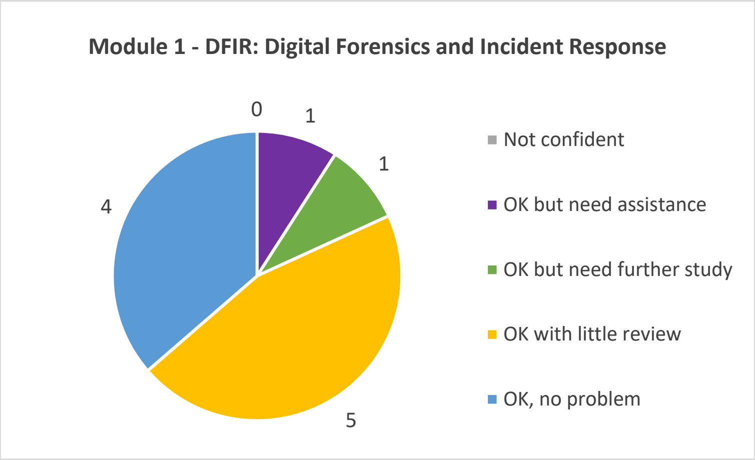


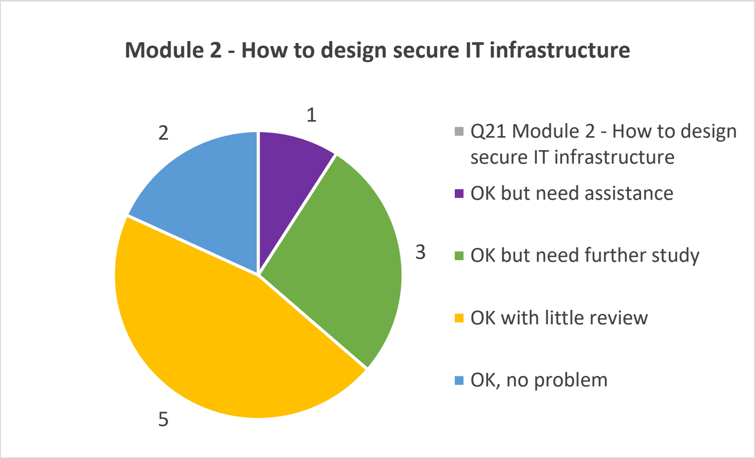


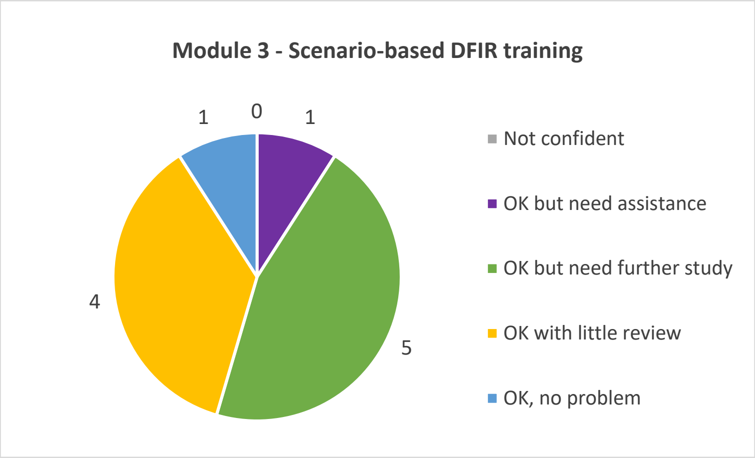
The volume of every Module should be OK.

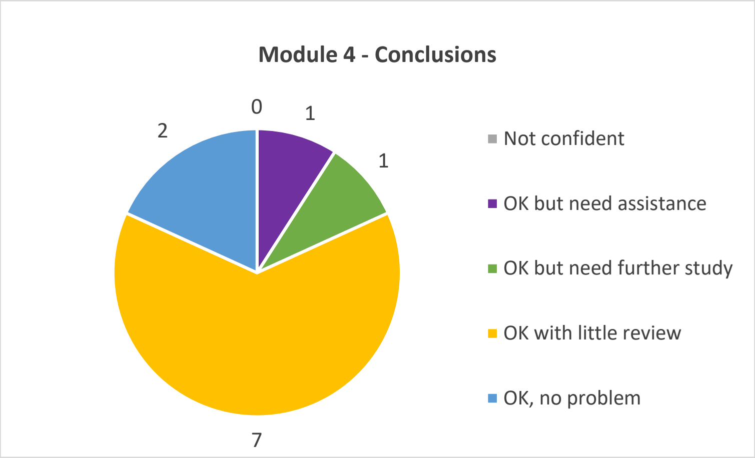
[Question]   Are you confident in teaching the topic?



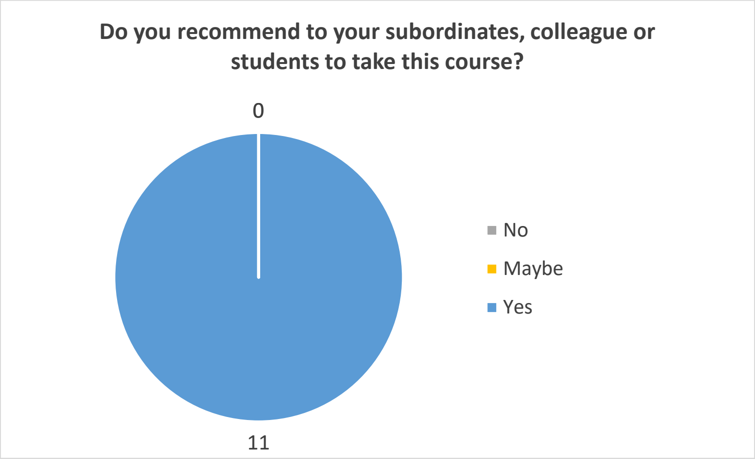








Every participant has confidence for teaching.



It is good to be recommended.

4. SUGGESTIONS

(1) Since the course materials contain a certain amount of information on today's state and trends of cybersecurity, it is necessary to constantly update such information. It is advised to review those parts at least once a year and keep the contents of the course materials up to date.

(2) It is recommended to consider developing another practical training course such as “How to build Cyber Range for cyber-attack and defense exercises”. Because having and operating a Cyber Range will be essential for future Cybersecurity organizations. For the UI, Cyber Range will also be needed to update the exercises in this Forensic course.

(3) The course materials are not specific to Indonesia except few parts (i.e., Summary of Supply Chain Survey) and can be used in other countries. For this reason, it is recommended to use it for similar educational purposes in other countries.

(4) When planning similar TTT in the future, it will be necessary to take care that it is not performed in the semester. Otherwise, sufficient attendance of the counterparts cannot be expected.

(5) It is not clear whether this is a problem peculiar to Indonesia, but it seems necessary to prepare reward to increase the response rate and quality level of the questionnaire. This is a piece of advice from one of the counterparts and it would be useful.

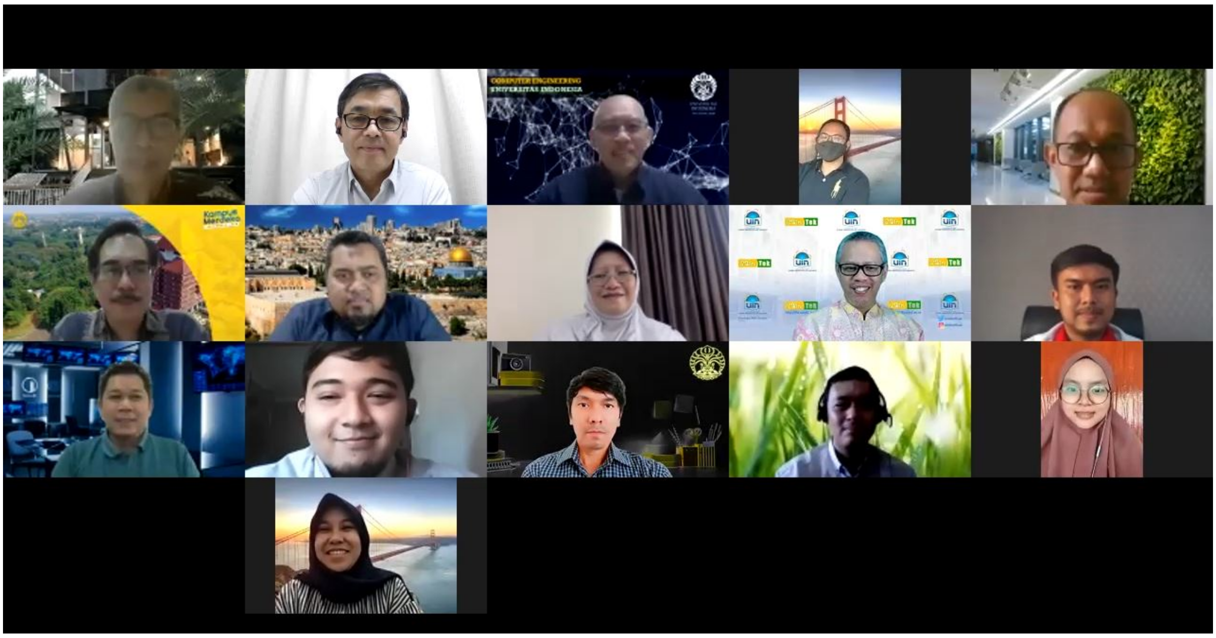
5. CONCLUSION

We have successfully completed making the materials and performed TTT for the cybersecurity courses “Case Study & Practice: Supply chain cybersecurity risks” and “Case Study & Practice: How to make IT systems forensic-enabled”. We hope that these achievements will contribute to the cybersecurity human resource development in Indonesia, which is the major purpose of the Project.

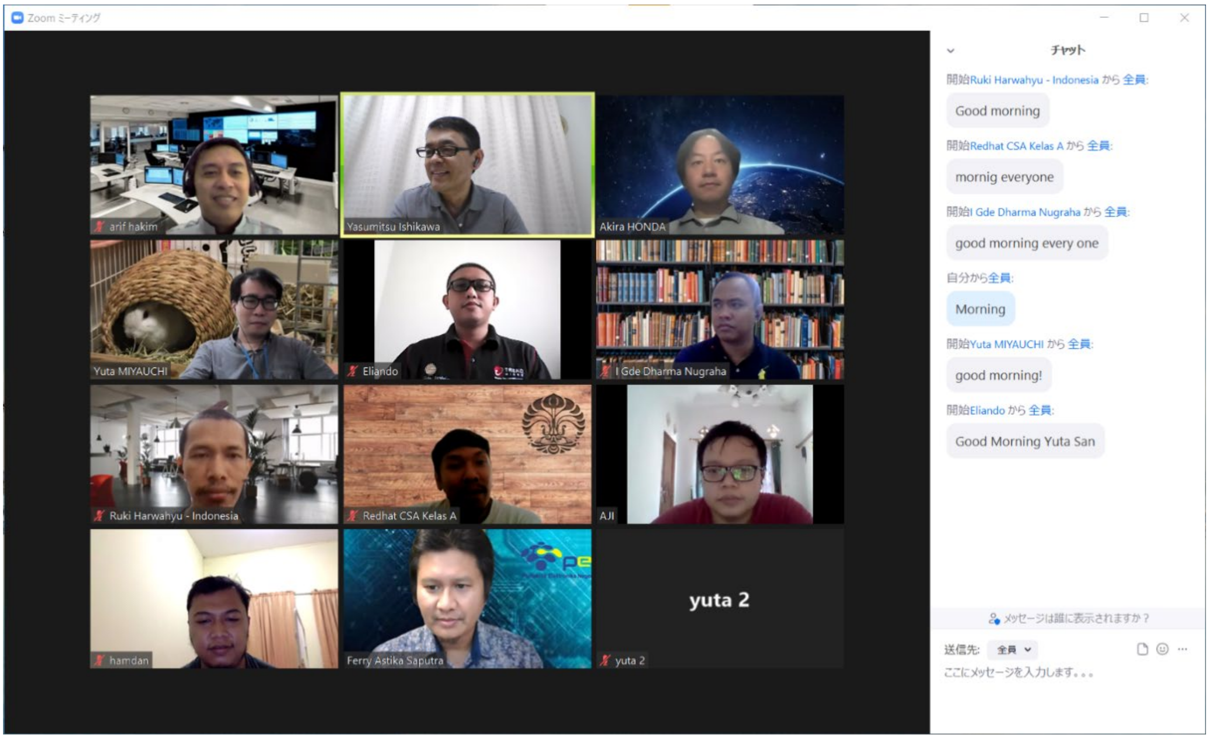
APPENDIX

APPENDIX A　PHOTO

■　TTT for Supply Chain course (from 9 Feb to 11 Feb 2021)



■　TTT for Forensic course (Done on 26, 28, 29 Jul and 02, 04, 05, 06 Aug 2021)



開始Ruki Harwahyu - Indonesia から 全員:

Good morning

開始Redhat CSA Kelas A から 全員:

mornig everyone

開始I Gde Dharma Nugraha から 全員:

good morning every one

自分から全員:

Morning

開始Yuta MIYAUCHI から 全員:

good morning!

開始Eliando から 全員:

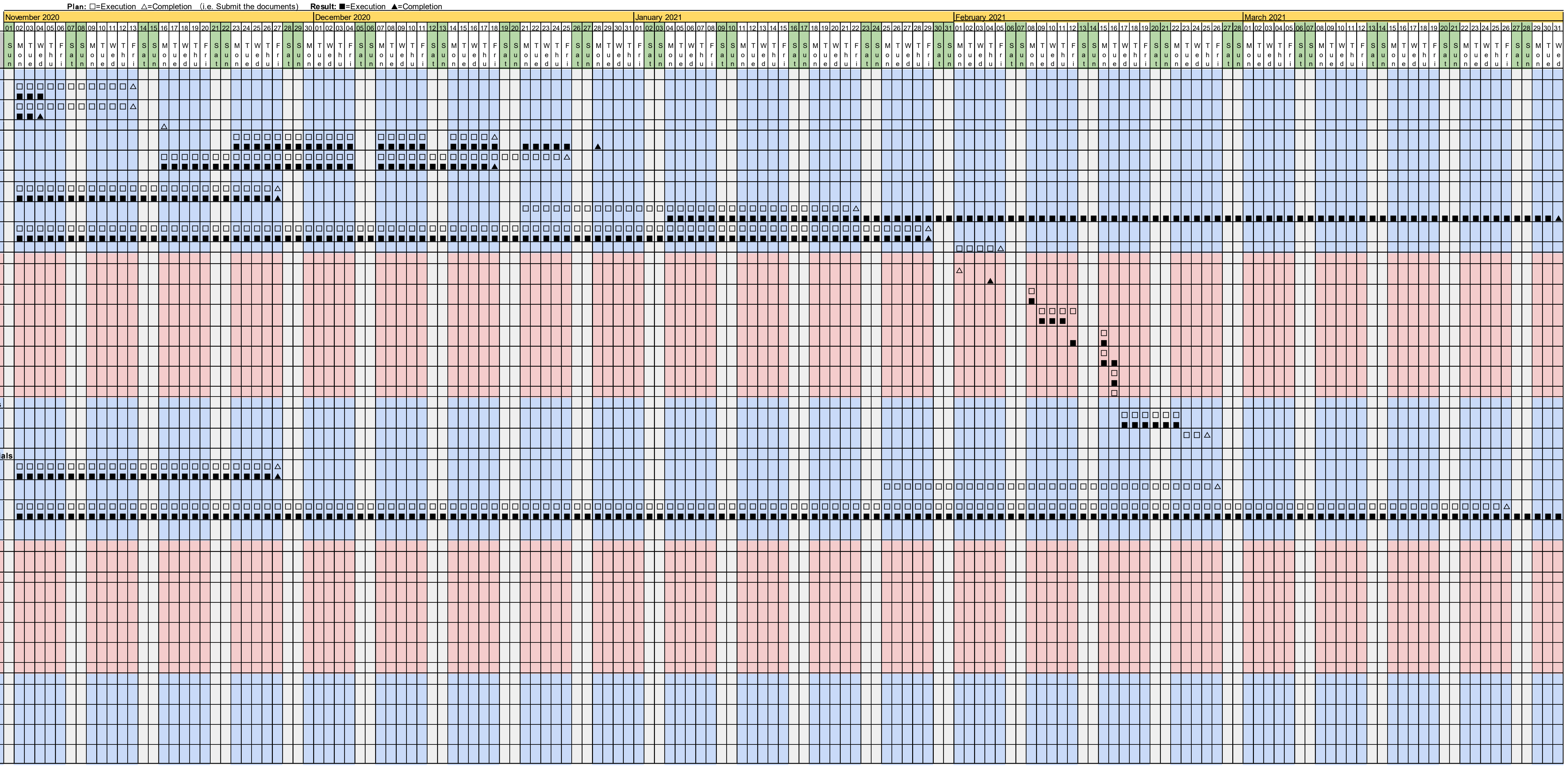
Good Morning Yuta San

メッセージは誰に表示されますか？
送信先: 全員
ここにメッセージを入力します。。。

APPENDIX B　OVERALL WORK SCHEDULE (PLAN AND ACTUAL)

November 2020 – March 2021

Plan: □=Execution △=Completion （i.e. Submit the documents） **Result:** ■=Execution ▲=Completion



No	Japan/ On-site	Action item
1	Japan	◆**Common work**
2	Japan	(1)Make Work plan (Japanese)
3	Japan	(2)Make Work plan (English)
4	Japan	(3)Explain Work plan to JICA HQ
5	Japan	(4)Engage contract with local consultant
6	Japan	(4)Procure equipment and books
7	Japan	◆**Develop Supply chain risk course**
8	Japan	(1)Collect information and conduct research
9	Japan	(2)Survey conducted by local consultant
10	Japan	(3)Make course materials
11	Japan	(4)Material review with local consultant
12	Japan	◆**1st TTT (Individual remote lecture)**
13	Japan	(1)Explain plan & course contents to C/P and project staff
14	Japan	(2)Evaluate C/P's capacity (Pre)
15	Japan	(3)Conduct TTT (3.5 hours/day)
16	Japan	(4)Perform trial lesson (partial)
17	Japan	(5)Evaluate C/P's capacity（Post）
18	Japan	(6)Discuss for material correction with C/Ps
19	Japan	(7)Meeting with project staff
20	Japan	◆**Modify Supply chain risk course materials**
21	Japan	(1)Do modification
22	Japan	(2)Share and approval
23	Japan	◆**Develop Forensics exercise course materials**
24	Japan	(1)Collect information and conduct research
25	Japan	(2)Survey conducted by local consultant
26	Japan	(3)Make course materials
27	Japan	(4)Material review with local consultant
28	Japan	◆**2nd TTT (Group remote lecture)**
29	Japan	(1)Explain plan & course contents to C/P and project staff
30	Japan	(2)Evaluate C/P's capacity (Pre)
31	Japan	(3)Conduct TTT (7 hours/day)
32	Japan	(4)Perform trial lesson (partial)
33	Japan	(5)Evaluate C/P's capacity（Post）
34	Japan	(6)Discuss for material correction with C/Ps
35	Japan	(7)Meeting with project staff
36	Japan	◆**Wrap-up work**
37	Japan	(1)Finalize course materials
38	Japan	(2)Share and approval
39	Japan	(3)Make work completion report
40	Japan	(4)Explain the result & conclusion to JICA HQ

June 2021 – September 2021

No	Japan/ On-site	Action item	June 2021																													
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
			Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed
1	Japan	◆Common work																														
2	Japan	(1)Make Work plan (Japanese)																														
3	Japan	(2)Make Work plan (English)																														
4	Japan	(3)Explain Work plan to JICA HQ																														
5	Japan	(4)Engage contract with local consultant																														
6	Japan	(4)Procure equipment and books																														
7	Japan	◆Develop Supply chain risk course																														
8	Japan	(1)Collect information and conduct research																														
9	Japan	(2)Survey conducted by local consultant																														
10	Japan	(3)Make course materials																														
11	Japan	(4)Material review with local consultant																														
12	Japan	◆1st TTT (Individual remote lecture)																														
13	Japan	(1)Explain plan & course contents to C/P and project staff																														
14	Japan	(2)Evaluate C/P's capacity (Pre)																														
15	Japan	(3)Conduct TTT (3.5 hours/day)																														
16	Japan	(4)Perform trial lesson (partial)																														
17	Japan	(5)Evaluate C/P's capacity（Post）																														
18	Japan	(6)Discuss for material correction with C/Ps																														
19	Japan	(7)Meeting with project staff																														
20	Japan	◆Modify Supply chain risk course materials																														
21	Japan	(1)Do modification																														
22	Japan	(2)Share and approval																														
23	Japan	◆Develop Forensics exercise course materials																														
24	Japan	(1)Collect information and conduct research																														
25	Japan	(2)Survey conducted by local consultant	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	▲
26	Japan	(3)Make course materials	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
27	Japan	(4)Material review with local consultant																														
28	Japan	◆2nd TTT (Group remote lecture)																														
29	Japan	(1)Explain plan & course contents to C/P and project staff																														
30	Japan	(2)Evaluate C/P's capacity (Pre)																														
31	Japan	(3)Conduct TTT (7 hours/day)																														
32	Japan	(4)Perform trial lesson (partial)																														
33	Japan	(5)Evaluate C/P's capacity（Post）																														
34	Japan	(6)Discuss for material correction with C/Ps																														
35	Japan	(7)Meeting with project staff																														
36	Japan	◆Wrap-up work																														
37	Japan	(1)Finalize course materials																														
38	Japan	(2)Share and approval																														
39	Japan	(3)Make work completion report																														
40	Japan	(4)Explain the result & conclusion to JICA HQ																														

No	Japan/ On-site	Action item	July 2021																														
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
			Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	Japan	◆Common work																															
2	Japan	(1)Make Work plan (Japanese)																															
3	Japan	(2)Make Work plan (English)																															
4	Japan	(3)Explain Work plan to JICA HQ																															
5	Japan	(4)Engage contract with local consultant																															
6	Japan	(4)Procure equipment and books																															
7	Japan	◆Develop Supply chain risk course																															
8	Japan	(1)Collect information and conduct research																															
9	Japan	(2)Survey conducted by local consultant																															
10	Japan	(3)Make course materials																															
11	Japan	(4)Material review with local consultant																															
12	Japan	◆1st TTT (Individual remote lecture)																															
13	Japan	(1)Explain plan & course contents to C/P and project staff																															
14	Japan	(2)Evaluate C/P's capacity (Pre)																															
15	Japan	(3)Conduct TTT (3.5 hours/day)																															
16	Japan	(4)Perform trial lesson (partial)																															
17	Japan	(5)Evaluate C/P's capacity（Post）																															
18	Japan	(6)Discuss for material correction with C/Ps																															
19	Japan	(7)Meeting with project staff																															
20	Japan	◆Modify Supply chain risk course materials																															
21	Japan	(1)Do modification					■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
22	Japan	(2)Share and approval																															
23	Japan	◆Develop Forensics exercise course materials																															
24	Japan	(1)Collect information and conduct research																															
25	Japan	(2)Survey conducted by local consultant																															
26	Japan	(3)Make course materials	■	■	■	■	■	■	■	■	▲																						
27	Japan	(4)Material review with local consultant												□ ▲	□	□	□	△															
28	Japan	◆2nd TTT (Group remote lecture)																															
29	Japan	(1)Explain plan & course contents to C/P and project staff																			△ TE		▲										
30	Japan	(2)Evaluate C/P's capacity (Pre)																										□					
31	Japan	(3)Conduct TTT (7 hours/day)																										□ ■		□ ■	□ ■		
32	Japan	(4)Perform trial lesson (partial)																															
33	Japan	(5)Evaluate C/P's capacity（Post）																															
34	Japan	(6)Discuss for material correction with C/Ps																															
35	Japan	(7)Meeting with project staff																															
36	Japan	◆Wrap-up work																															
37	Japan	(1)Finalize course materials																															
38	Japan	(2)Share and approval																															
39	Japan	(3)Make work completion report																															
40	Japan	(4)Explain the result & conclusion to JICA HQ																															

No	Japan/ On-site	Action item	August 2021																														
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
			Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue
1	Japan	◆Common work																															
2	Japan	(1)Make Work plan (Japanese)																															
3	Japan	(2)Make Work plan (English)																															
4	Japan	(3)Explain Work plan to JICA HQ																															
5	Japan	(4)Engage contract with local consultant																															
6	Japan	(4)Procure equipment and books																															
7	Japan	◆Develop Supply chain risk course																															
8	Japan	(1)Collect information and conduct research																															
9	Japan	(2)Survey conducted by local consultant																															
10	Japan	(3)Make course materials																															
11	Japan	(4)Material review with local consultant																															
12	Japan	◆1st TTT (Individual remote lecture)																															
13	Japan	(1)Explain plan & course contents to C/P and project staff																															
14	Japan	(2)Evaluate C/P's capacity (Pre)																															
15	Japan	(3)Conduct TTT (3.5 hours/day)												■Supplementary class																			
16	Japan	(4)Perform trial lesson (partial)																															
17	Japan	(5)Evaluate C/P's capacity（Post）																															
18	Japan	(6)Discuss for material correction with C/Ps												■																			
19	Japan	(7)Meeting with project staff																															
20	Japan	◆Modify Supply chain risk course materials																															
21	Japan	(1)Do modification	■	■	■	■	■	■	■	■	■	■	■	■																			
22	Japan	(2)Share and approval												▲																			
23	Japan	◆Develop Forensics exercise course materials																															
24	Japan	(1)Collect information and conduct research																															
25	Japan	(2)Survey conducted by local consultant																															
26	Japan	(3)Make course materials																															
27	Japan	(4)Material review with local consultant																															
28	Japan	◆2nd TTT (Group remote lecture)																															
29	Japan	(1)Explain plan & course contents to C/P and project staff																															
30	Japan	(2)Evaluate C/P's capacity (Pre)																															
31	Japan	(3)Conduct TTT (7 hours/day)		□ ■		□ ■	□ ■	□ ■																									
32	Japan	(4)Perform trial lesson (partial)										□ ■	□	□ ■																			
33	Japan	(5)Evaluate C/P's capacity（Post）										□ ■	□	□ ■																			
34	Japan	(6)Discuss for material correction with C/Ps												□ ■																			
35	Japan	(7)Meeting with project staff												□																			
36	Japan	◆Wrap-up work																															
37	Japan	(1)Finalize course materials													□ ■			□ ▲	□	□	□	□	□	□	△								
38	Japan	(2)Share and approval																								□ ▲	□	□	△				
39	Japan	(3)Make work completion report													□ ■			□ ■	□ ■	□ ■	□ ■	□ ■	□ ■	□ ■	□ ■	□ ■	□ ■	□ ■	□ ■	□ ■	□ ■	□ ■	△ ▲
40	Japan	(4)Explain the result & conclusion to JICA HQ																															

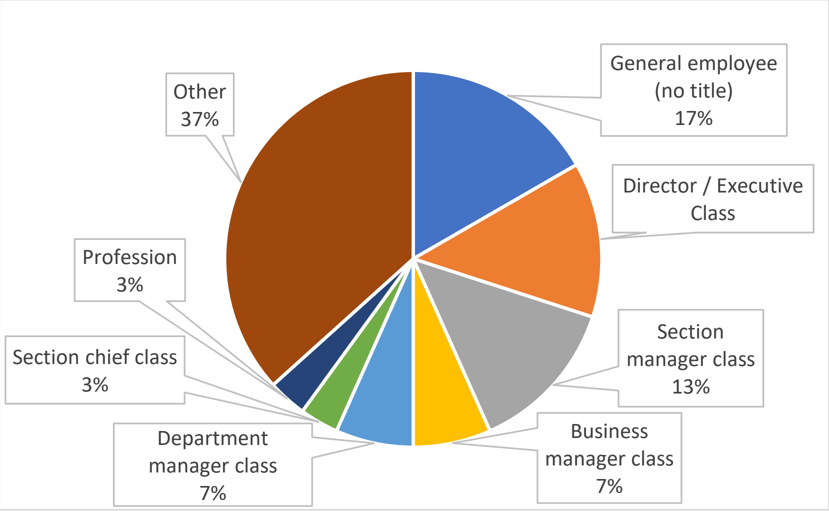
No	Japan/ On-site	Action item	September 2021																													
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
			Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu
1	Japan	◆Common work																														
2	Japan	(1)Make Work plan (Japanese)																														
3	Japan	(2)Make Work plan (English)																														
4	Japan	(3)Explain Work plan to JICA HQ																														
5	Japan	(4)Engage contract with local consultant																														
6	Japan	(4)Procure equipment and books																														
7	Japan	◆Develop Supply chain risk course																														
8	Japan	(1)Collect information and conduct research																														
9	Japan	(2)Survey conducted by local consultant																														
10	Japan	(3)Make course materials																														
11	Japan	(4)Material review with local consultant																														
12	Japan	◆1st TTT (Individual remote lecture)																														
13	Japan	(1)Explain plan & course contents to C/P and project staff																														
14	Japan	(2)Evaluate C/P's capacity (Pre)																														
15	Japan	(3)Conduct TTT (3.5 hours/day)																														
16	Japan	(4)Perform trial lesson (partial)																														
17	Japan	(5)Evaluate C/P's capacity（Post）																														
18	Japan	(6)Discuss for material correction with C/Ps																														
19	Japan	(7)Meeting with project staff																														
20	Japan	◆Modify Supply chain risk course materials																														
21	Japan	(1)Do modification																														
22	Japan	(2)Share and approval																														
23	Japan	◆Develop Forensics exercise course materials																														
24	Japan	(1)Collect information and conduct research																														
25	Japan	(2)Survey conducted by local consultant																														
26	Japan	(3)Make course materials																														
27	Japan	(4)Material review with local consultant																														
28	Japan	◆2nd TTT (Group remote lecture)																														
29	Japan	(1)Explain plan & course contents to C/P and project staff																														
30	Japan	(2)Evaluate C/P's capacity (Pre)																														
31	Japan	(3)Conduct TTT (7 hours/day)																														
32	Japan	(4)Perform trial lesson (partial)																														
33	Japan	(5)Evaluate C/P's capacity（Post）																														
34	Japan	(6)Discuss for material correction with C/Ps																														
35	Japan	(7)Meeting with project staff																														
36	Japan	◆Wrap-up work																														
37	Japan	(1)Finalize course materials																														
38	Japan	(2)Share and approval																														
39	Japan	(3)Make work completion report																														
40	Japan	(4)Explain the result & conclusion to JICA HQ	△																													

APPENDIX C　RESULTS OF PRELIMINARY SURVEY (SUPPLY CHAIN)

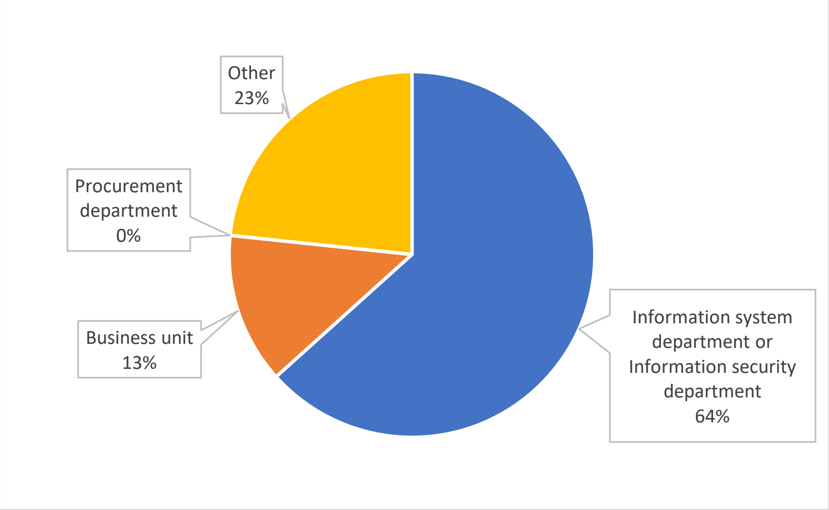
Q1　First Name, Last Name, Company / Organization, Company Address, City, Zip Code, Country, State, Phone, Email

<This response result is not disclosed because the responses include privacy information.>

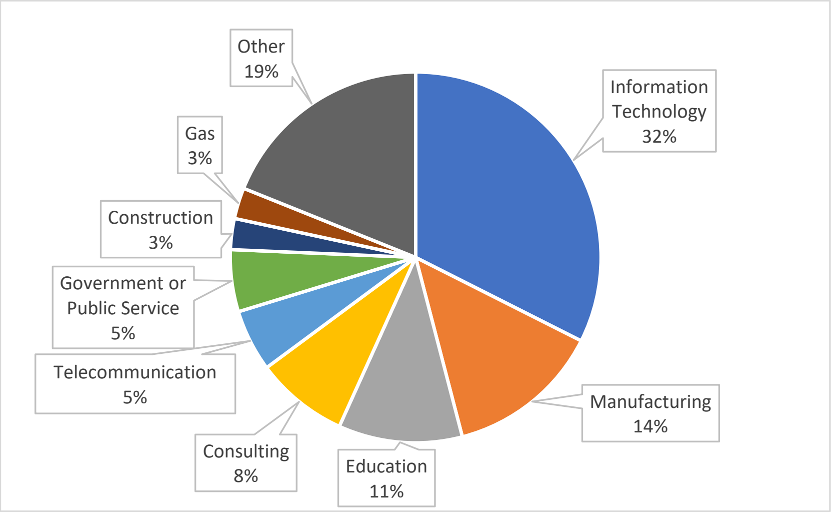
Q2　Please select your title



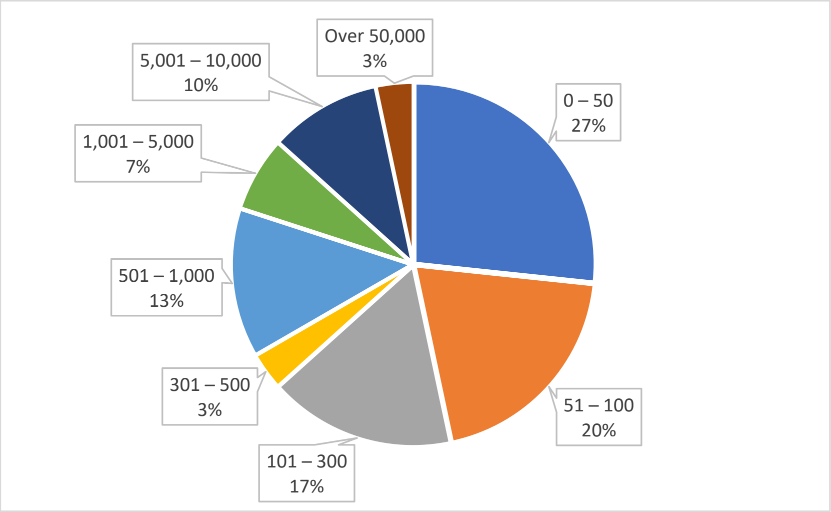
Q3　Please select your department / division



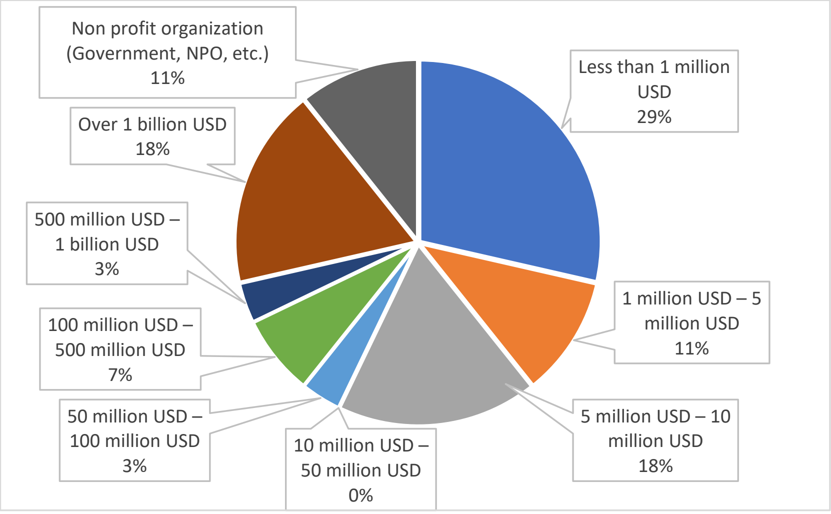
Q4 What industry is your company categorized to?



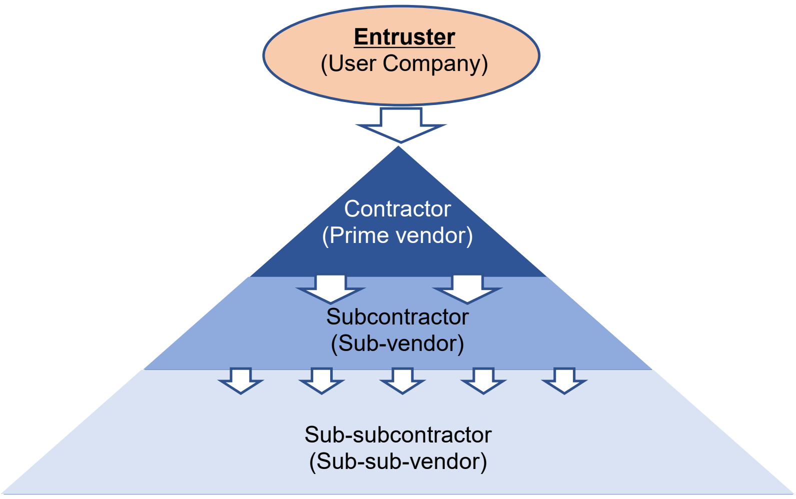
Q5 Please select the total number of employees at your company (including full-time and part-time employees).

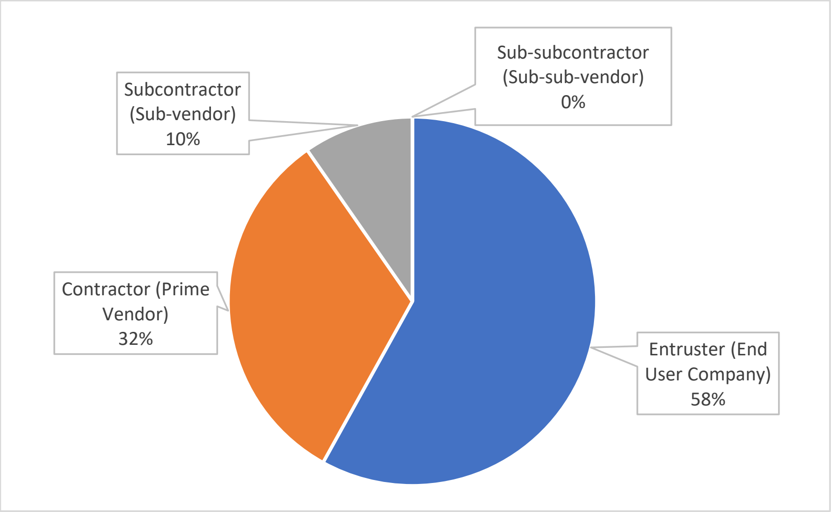


Q6 Please select the estimated sales of your company



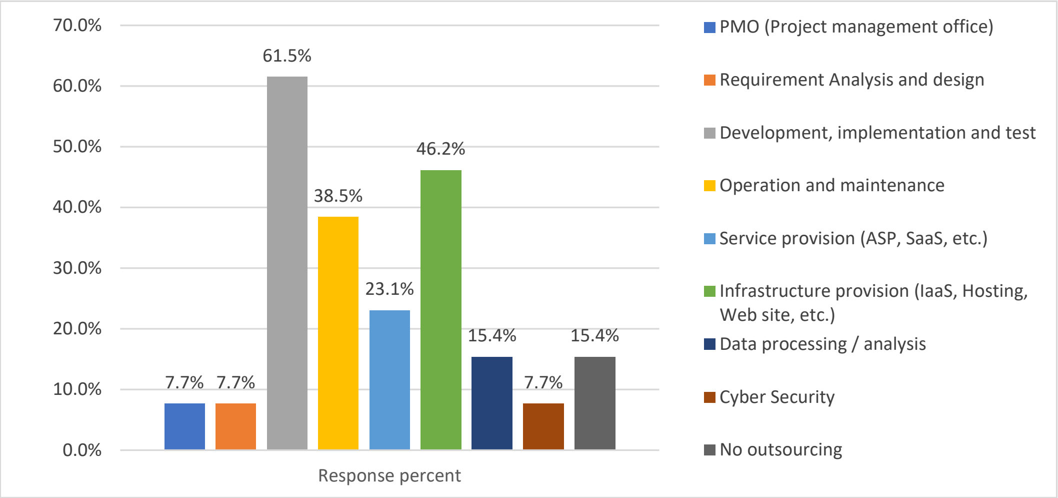
Q7 What kind of Company / Organization that you are working on, in the IT Supply Chain above ?



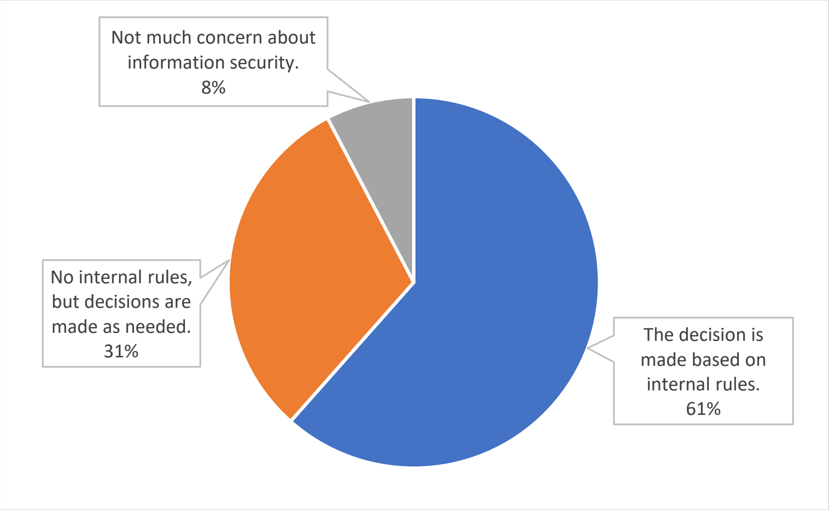


From Q8 to Q18 were responded by Entrust (User) companies

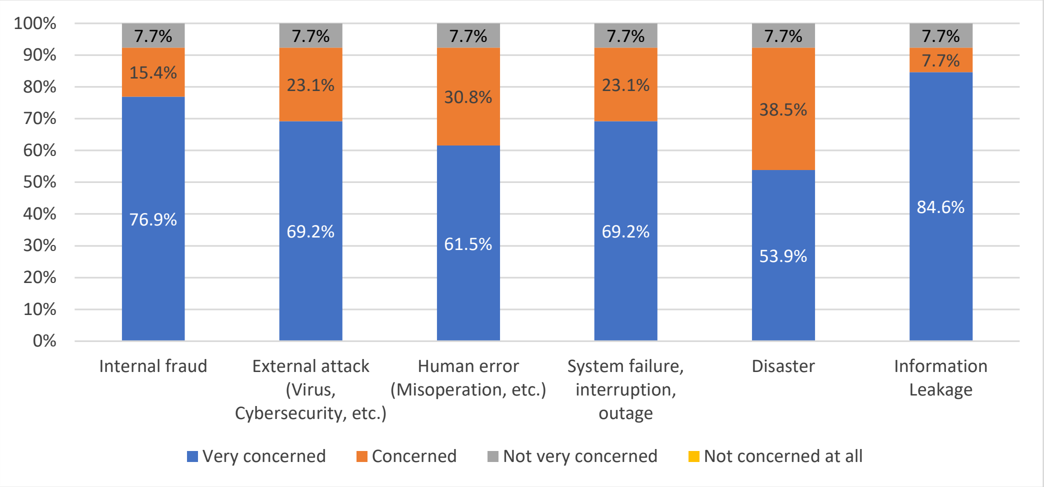
Q8 What IT system services that your company outsources ? (Multiple option)



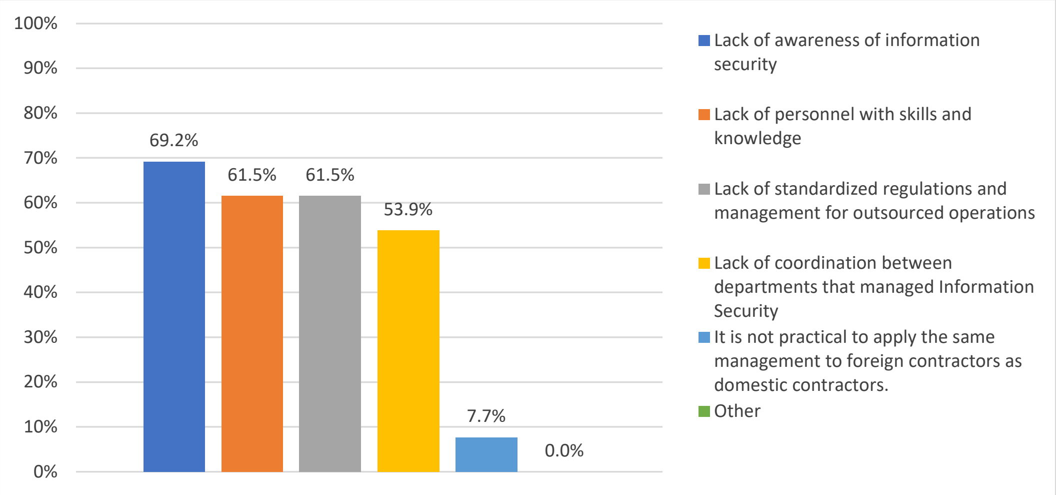
Q9 What basis does your company decide whether or not to outsource information security ?



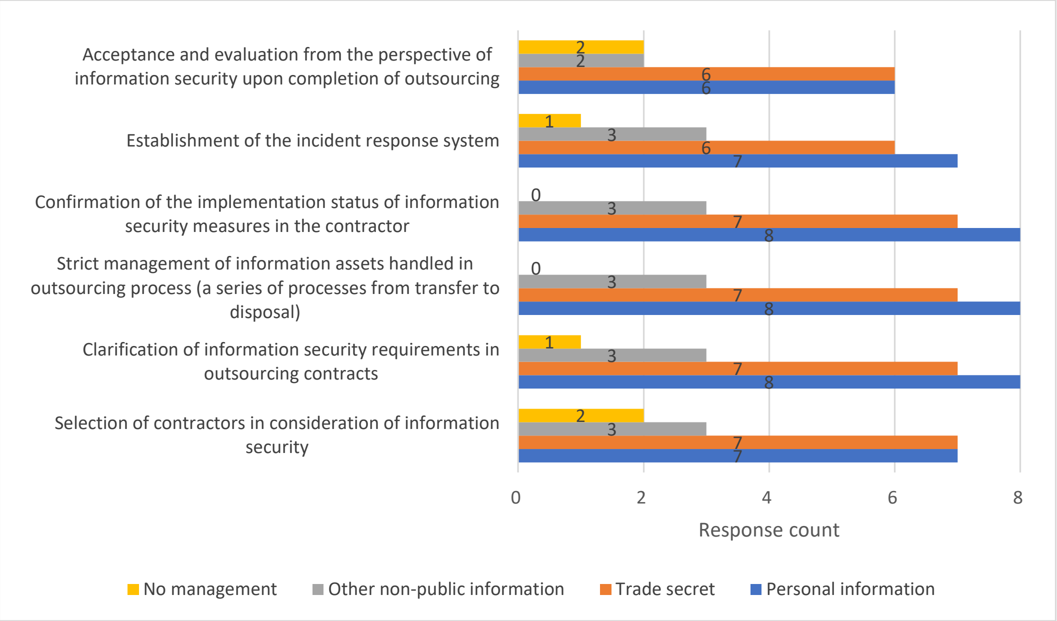
Q10 How concerned are you about the information security risks associated with outsourced assets?



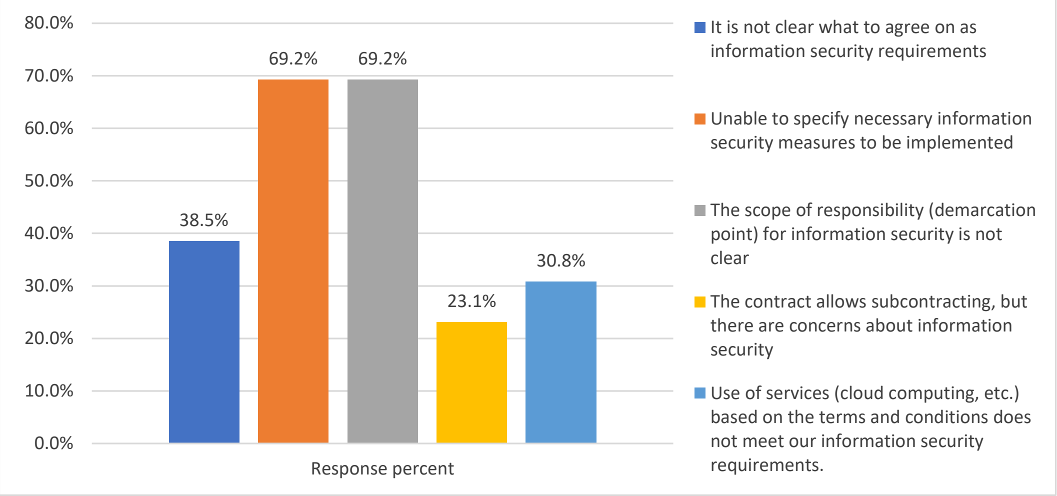
Q11 What do you consider to be the issues in managing the information security of contractors? Choose up to 3 ONLY



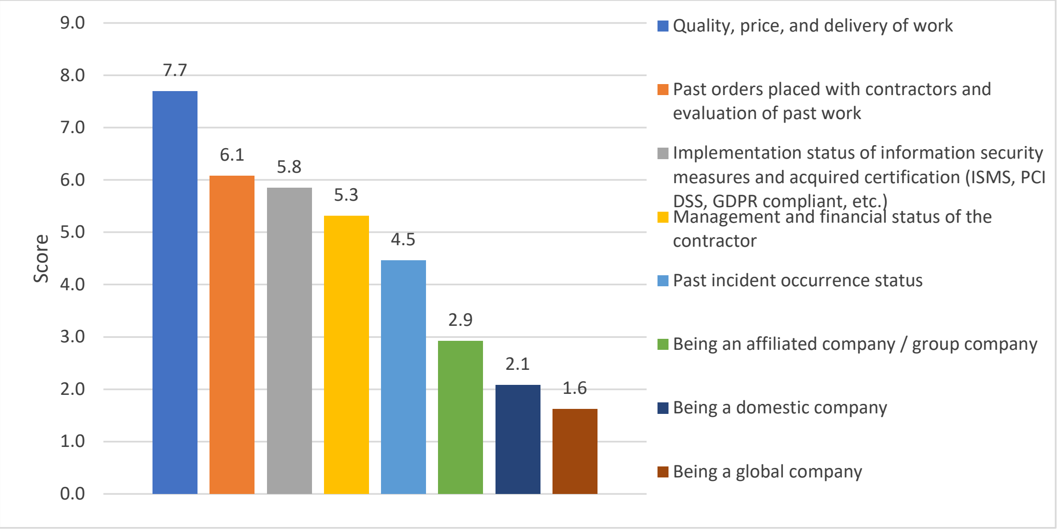
Q12 Please select which Information Security control that you already have in place during the process o f managing contractors.



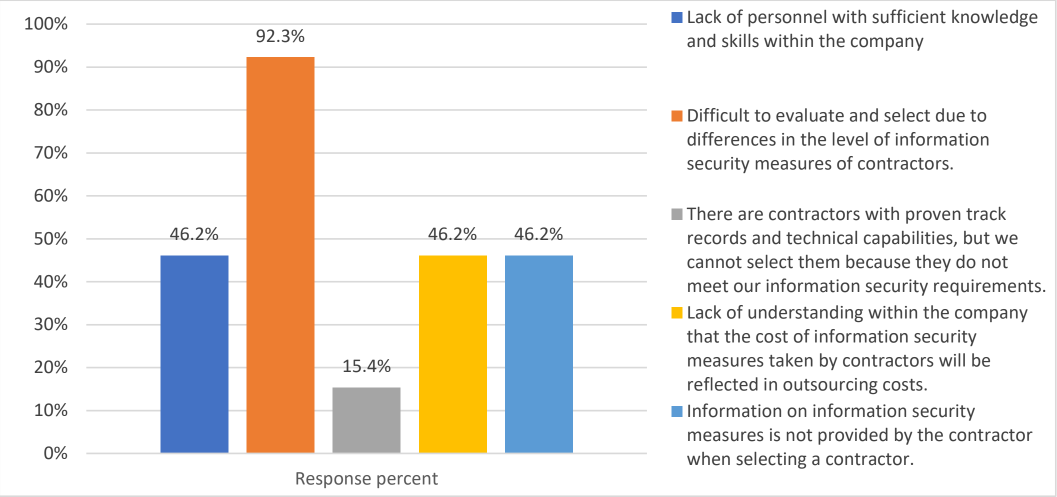
Q13 What do you consider to be the most important information security issues that needs to be described in the contracts with contractors? (Multiple choice up to 3)



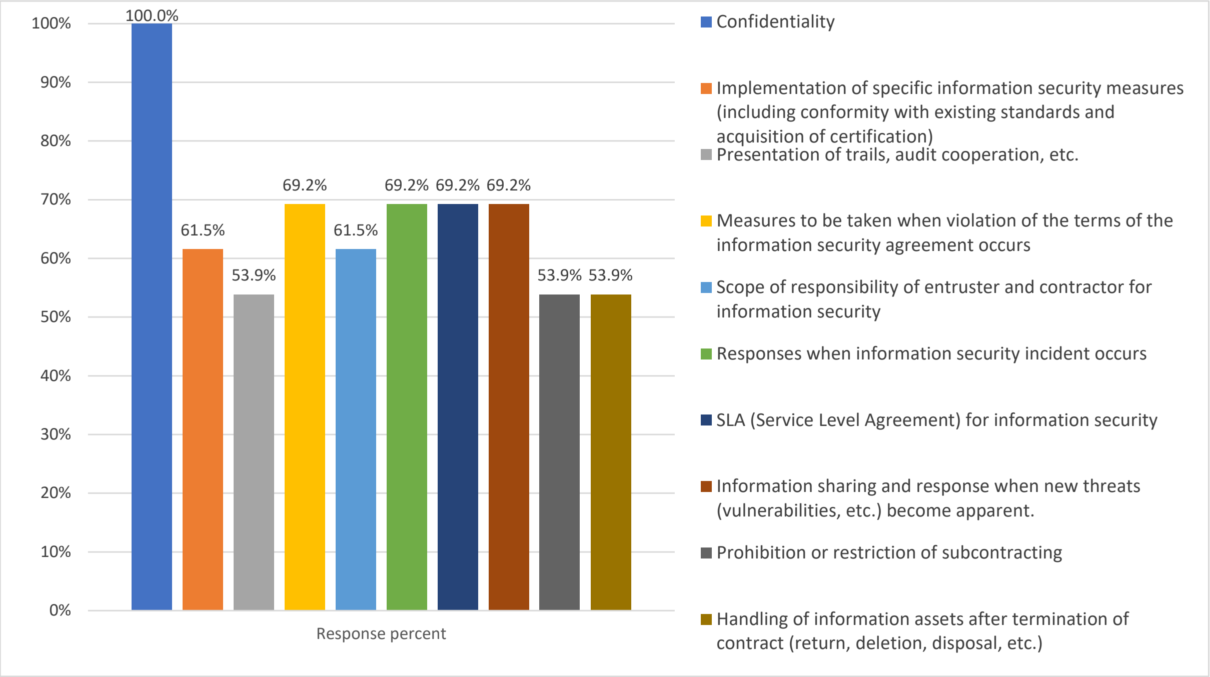
Q14 What points do you place importance on when selecting contractors? Please choose the four most important items in order of priority.



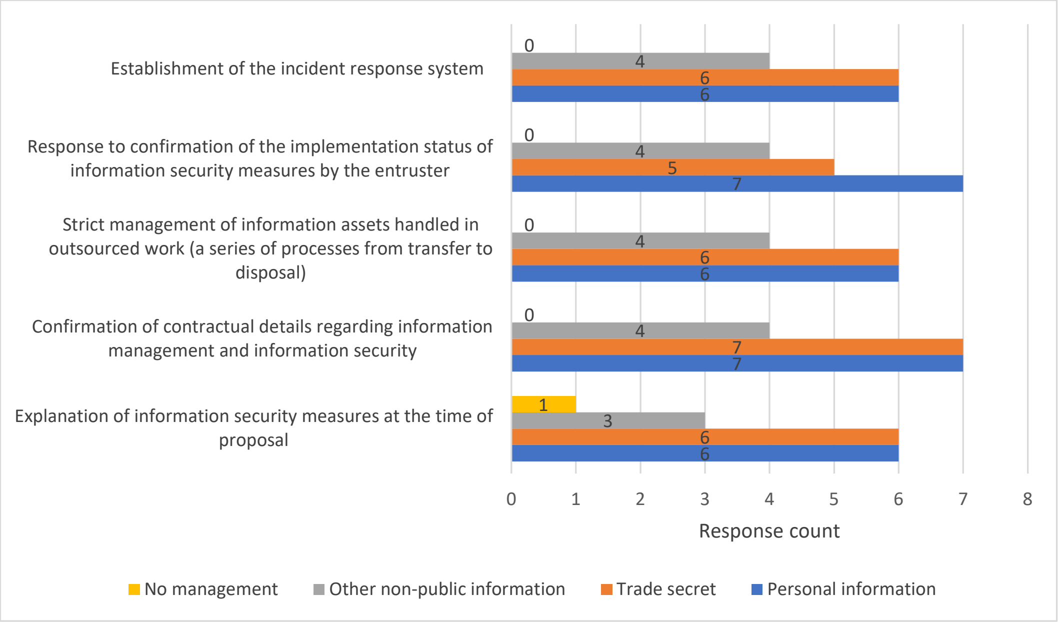
Q15 From the perspective of information security, what are the key issues when selecting outsourcing partners? (Multiple choice up to 3)



Q16 What kind of information security requirements do you include in your contracts? (Select all that apply)



Q17 Please indicate the implementation status of information security measures for each type of information you handle. (Select all that apply)

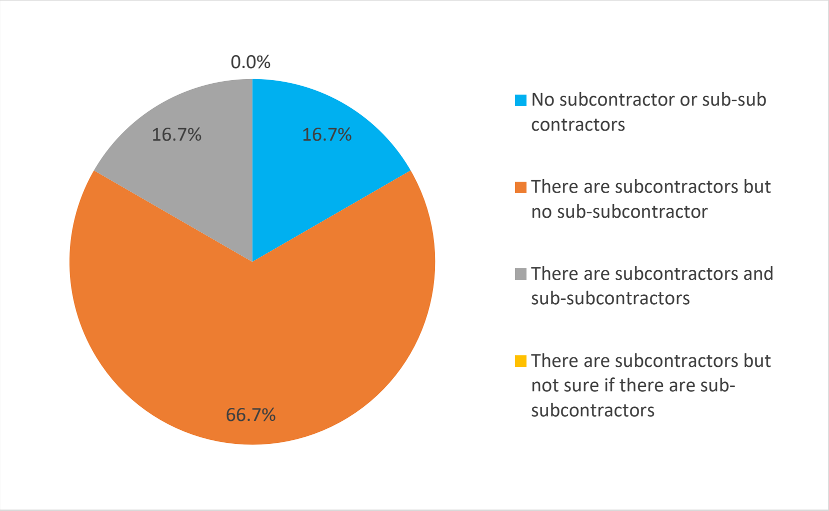


Q18 Please feel free to describe anything you would like to say about information security in the supply chain.

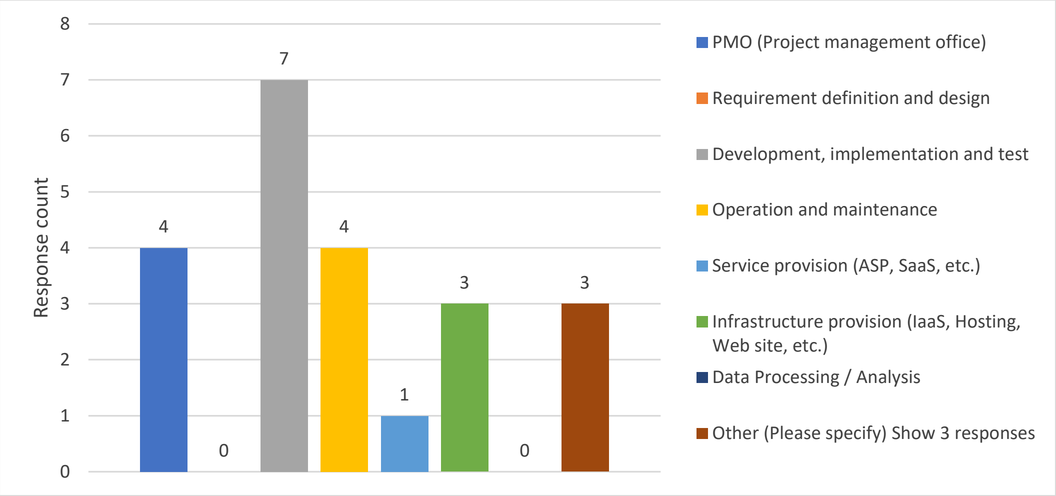
Cybersecurity is never just a technology problem, it's a people, processes and knowledge problem.
Information security must be handled properly from the beginning until the end of the whole process

From Q19 to Q30 were responded by Contractor companies

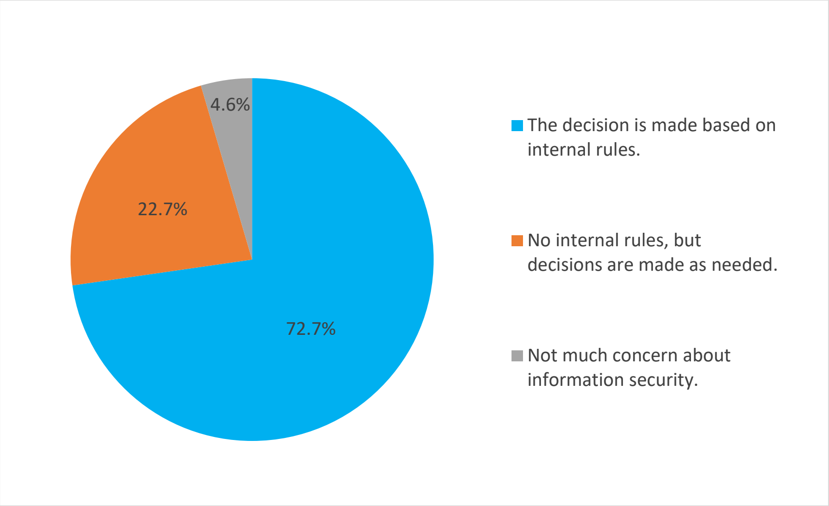
Q19 Do you have sub-contractors or / and sub-sub contractors for your Company ?



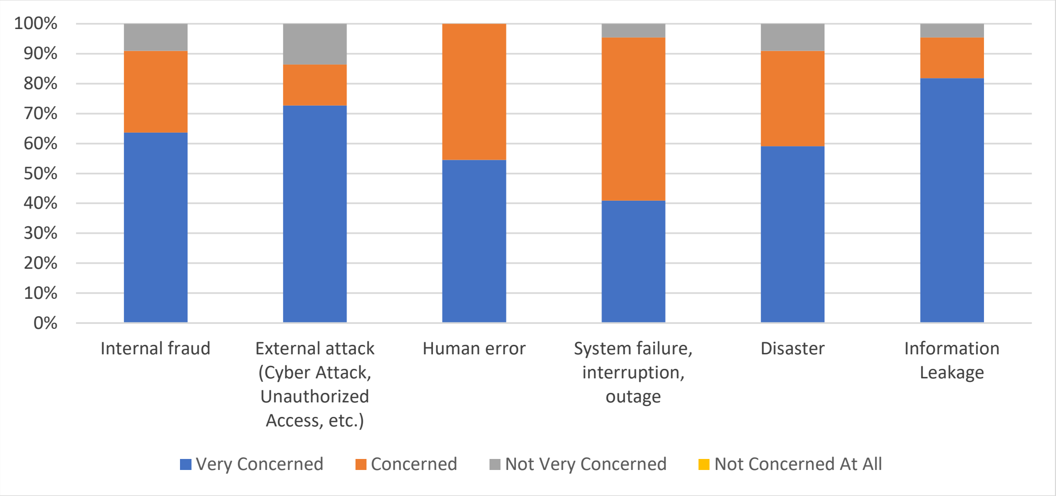
Q20 Please select all that apply to your Company current existing IT system services.



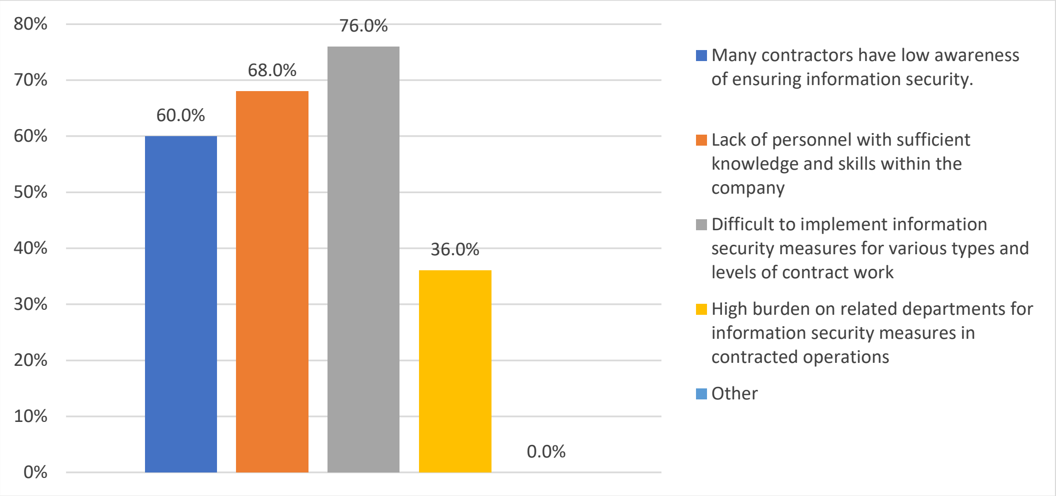
Q21 What basis does your company decide whether or not to outsource information security ?



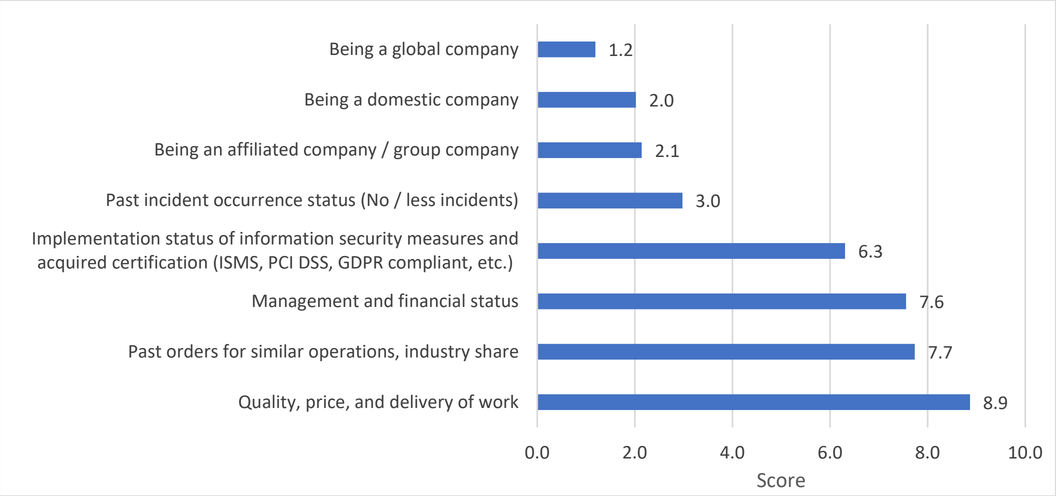
Q22 How concerned are you about the information security risks associated with outsourced assets?



Q23 What do you consider to be the most important information security issues in contracts with outsourcers? (Multiple choice up to 3)

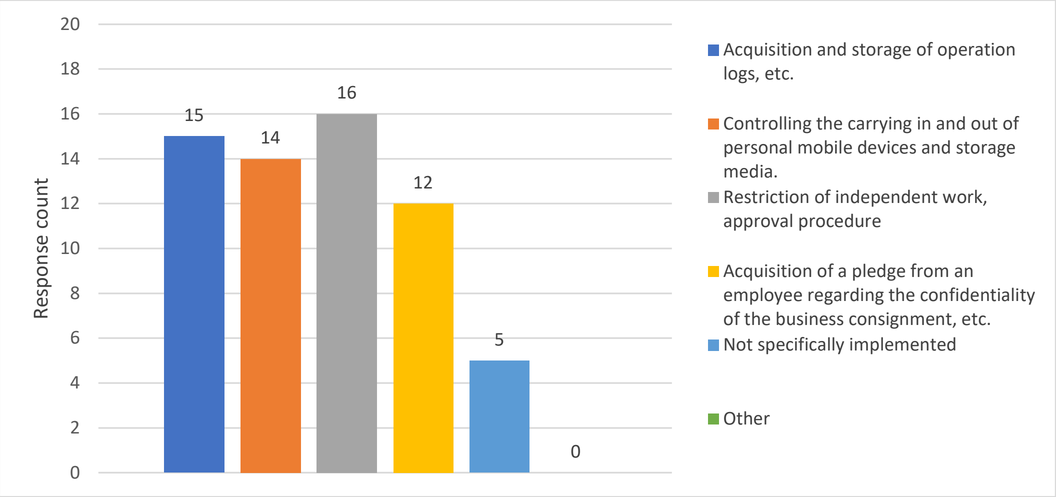


Q24 What do you emphasize about your business proposals to the outsourcer? Please choose the four most important items in order of priority

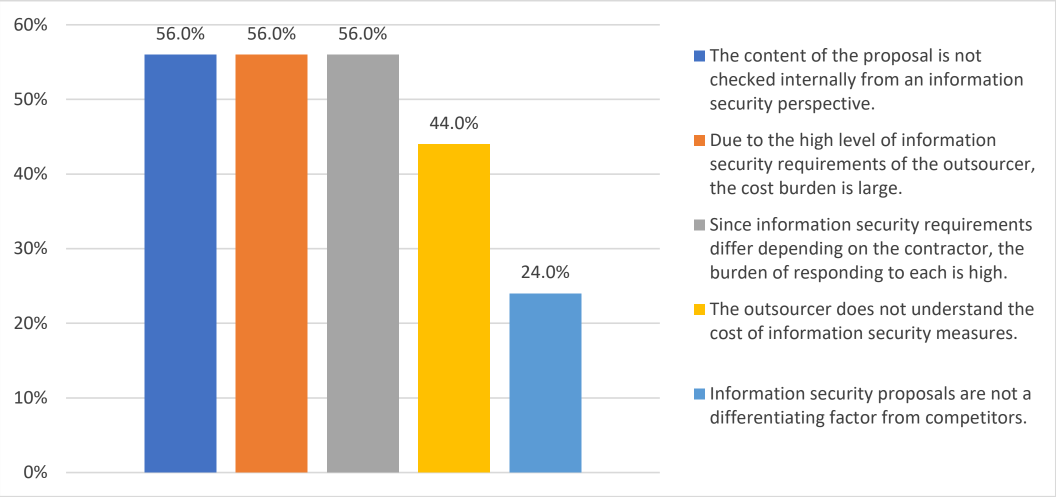


Note: The score is calculated based on the priority. Greater value means higher priority.

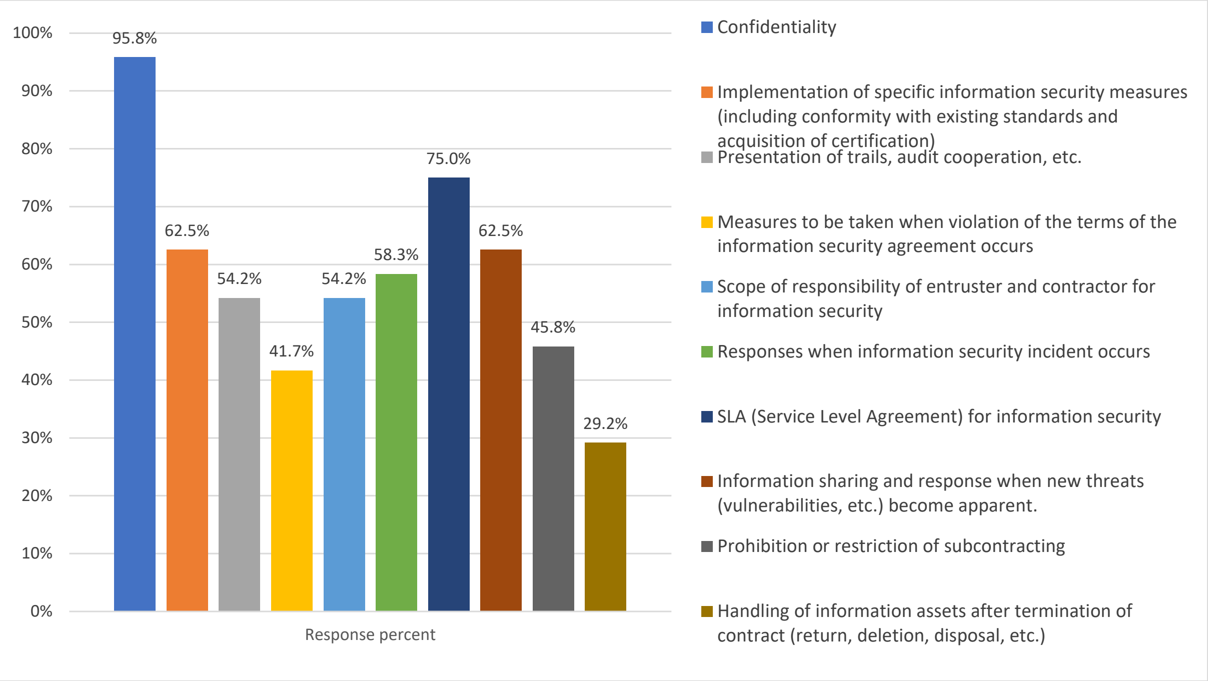
Q25 What kind of information security measures do you take to prevent internal fraud in your contracted business? (Select all that apply)



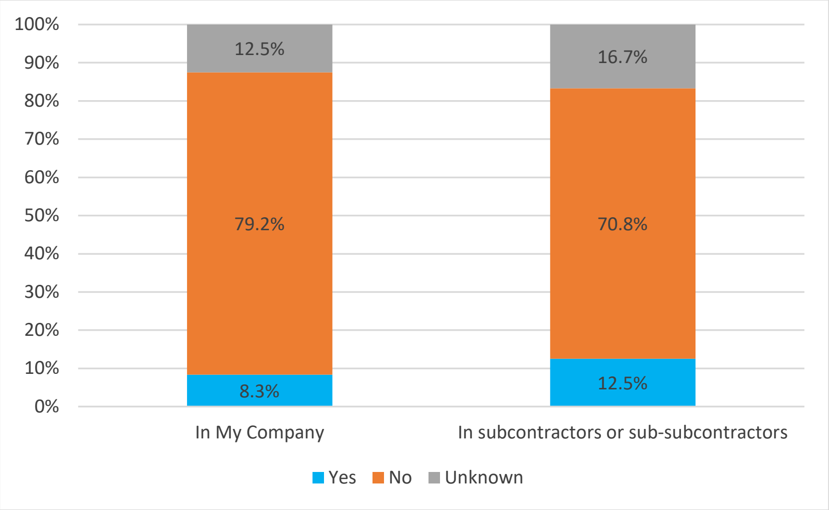
Q26 From the perspective of information security, what are the key issues when proposing to the outsourcers? (Multiple choice up to 3)



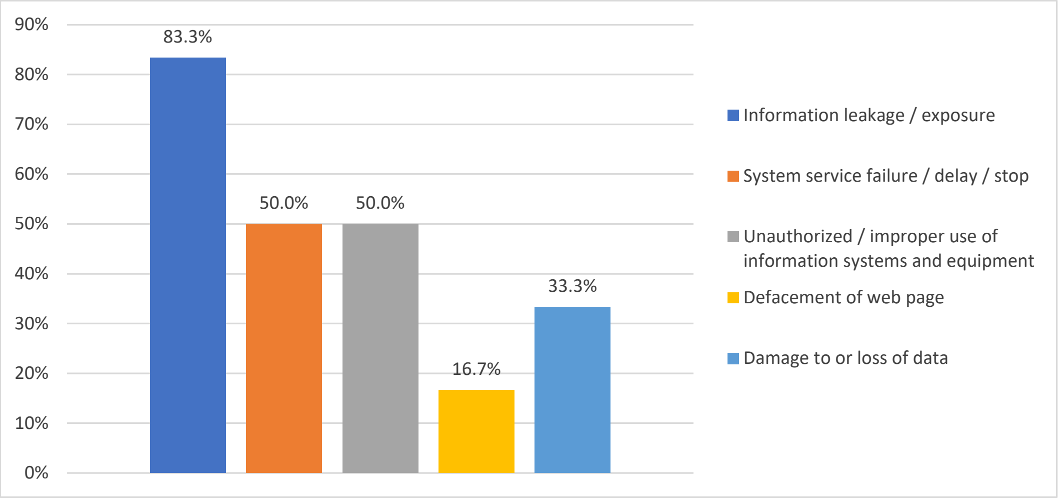
Q27 What kind of information security requirements are included in the contracts with entrusters? (Select all that apply)



Q28 Have you ever had an incident in the past three years of outsourced work in your company or subcontractor? (Select one for each row)



Q29 Please answer if you chose “Yes” in above question. What kind of incident occurred?



Q30 Please feel free to describe anything you would like to say about information security in the supply chain.

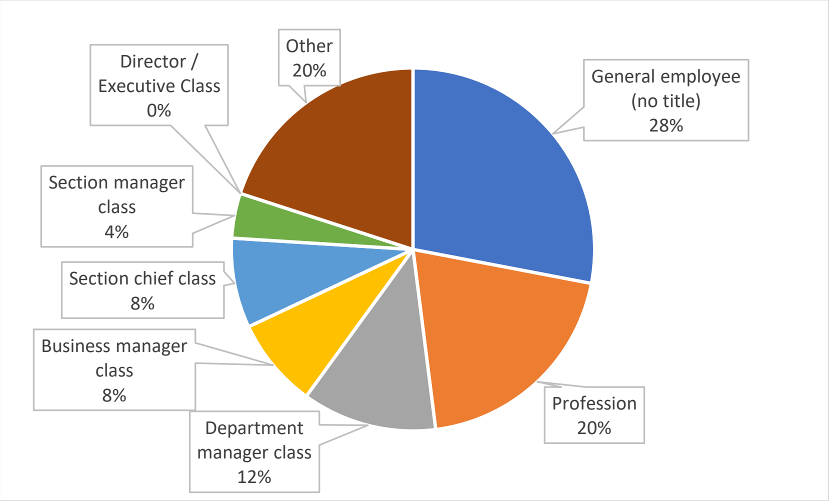
IT Security Regulation
Information Security is a must since the begining day of information technology being implemented
Cybersecurity is never just a technology problem, it’s a people, processes and knowledge problem.
Very important due to data privacy

APPENDIX D RESULTS OF PRELIMINARY SURVEY (FORENSIC)

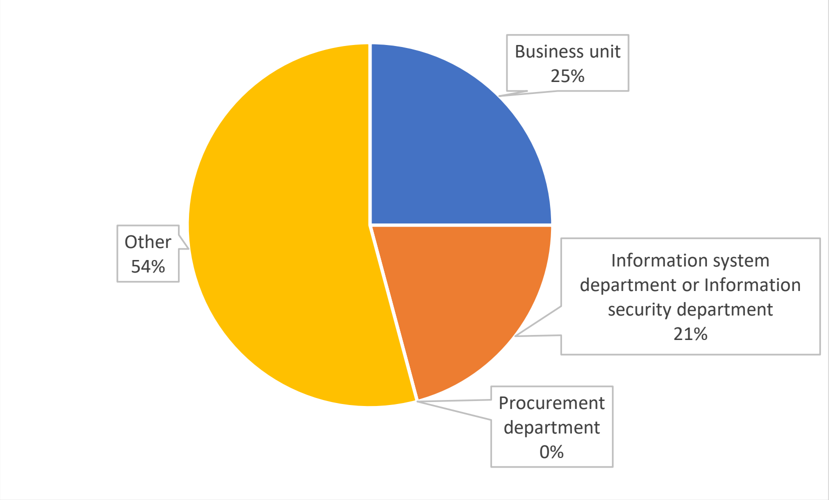
Q1 First Name, Last Name, Company / Organization, Company Address, City, Zip Code, Country, State, Phone, Email

<This response result is not disclosed because the responses include privacy information.>

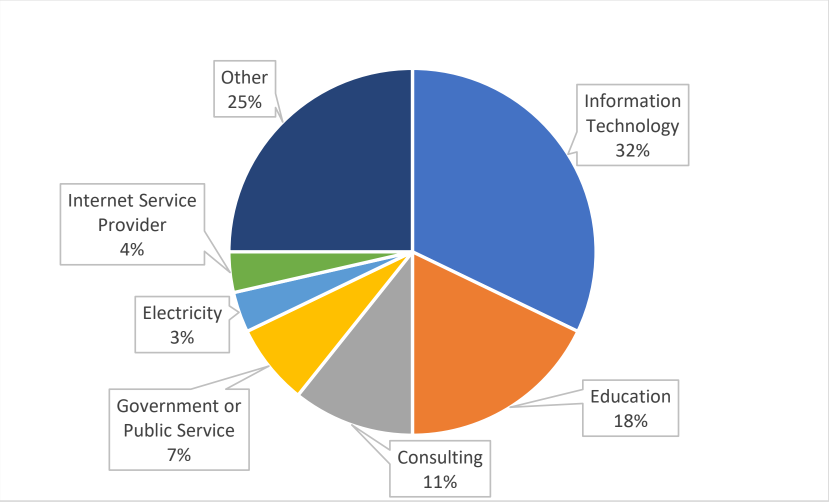
Q2 Please select your title



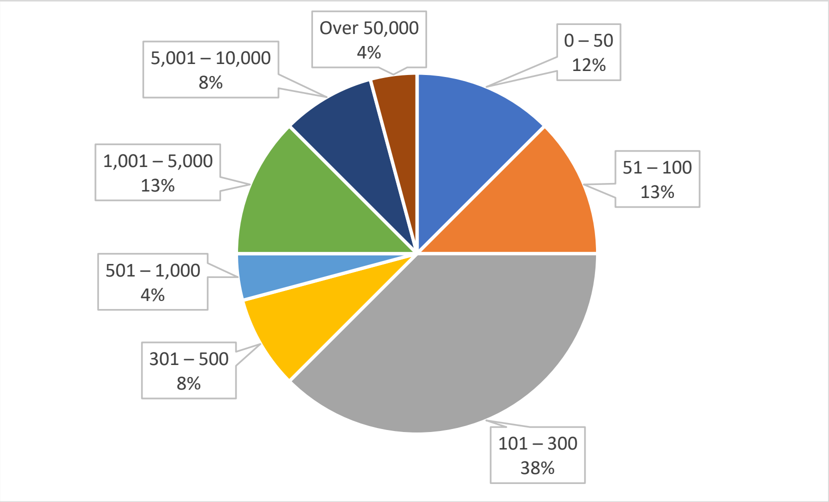
Q3 Please select your department / division



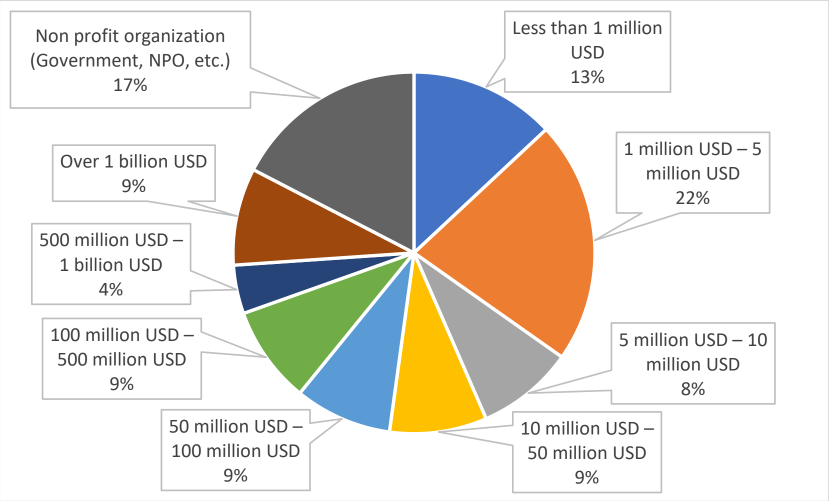
Q4 What industry is your company categorized to?



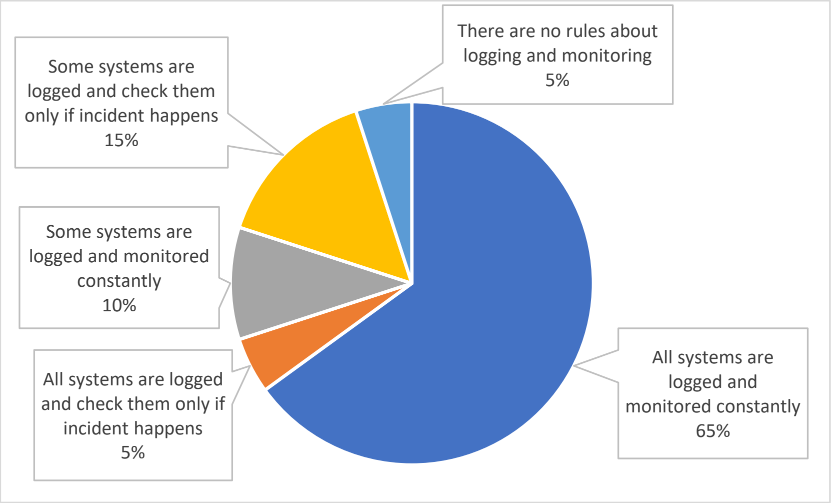
Q5 Please select the total number of employees at your company (including full-time and part-time employees).



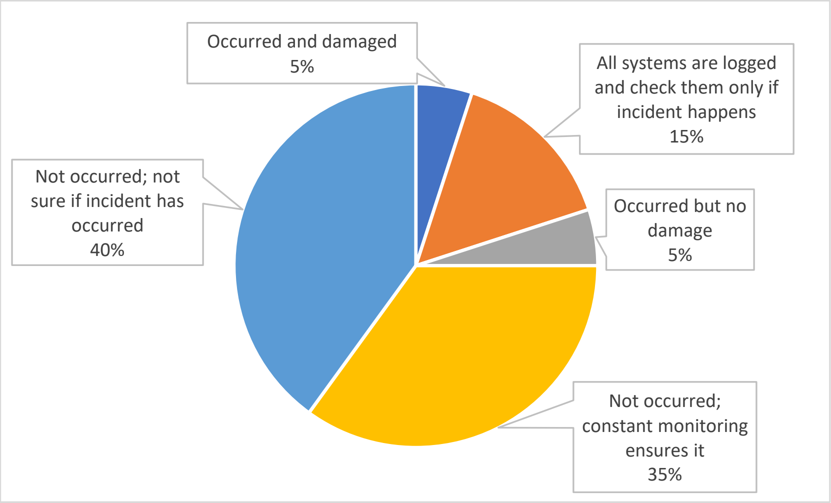
Q6 Please select the estimated sales of your company



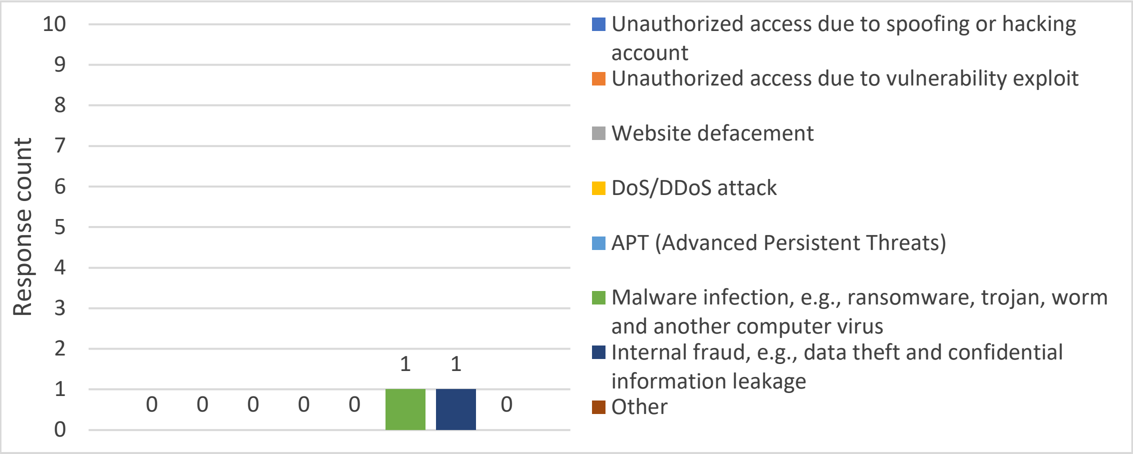
Q7 Please select logging and monitoring status in your company. (Select one)



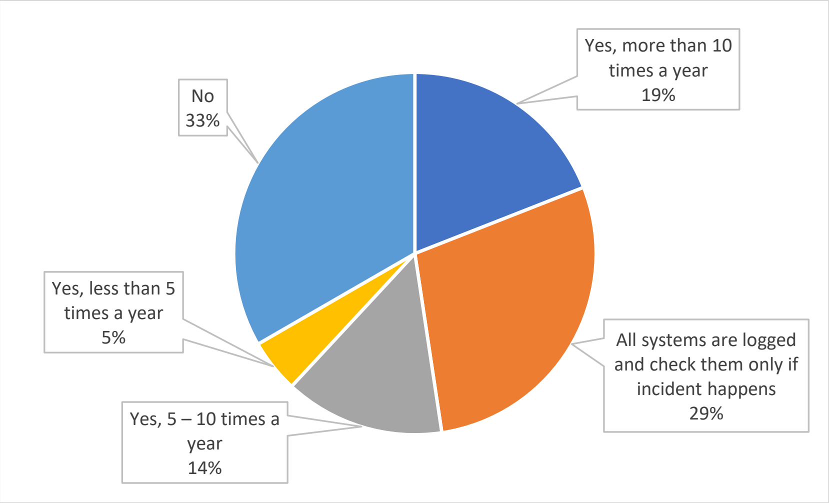
Q8 Please select the occurrence of security incidents (cyberattacks, malware infections, internal fraud, etc.) in your company in the past. (Select one)



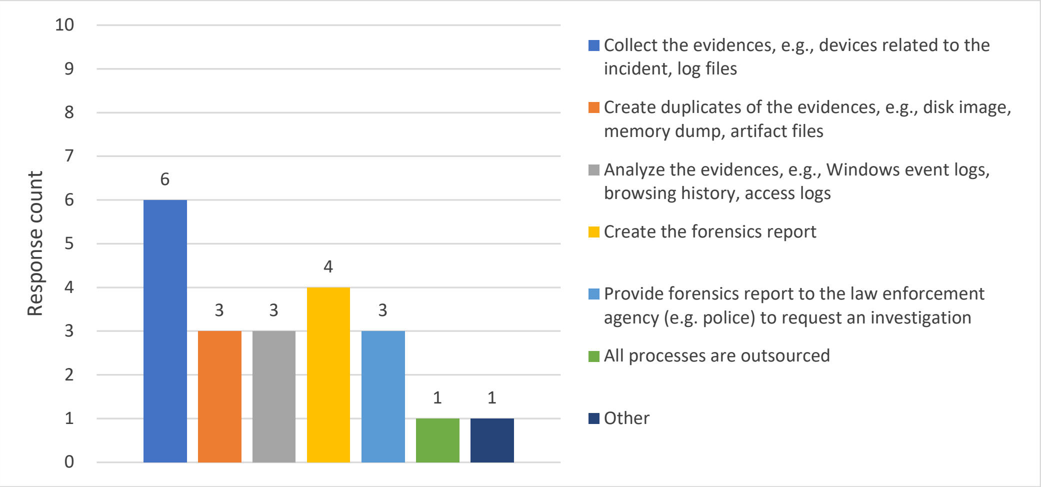
Q9 For those who selected "Occurred" (1)(2) in Previous Question, what kind of cyberattack occurred? (Multiple choice)



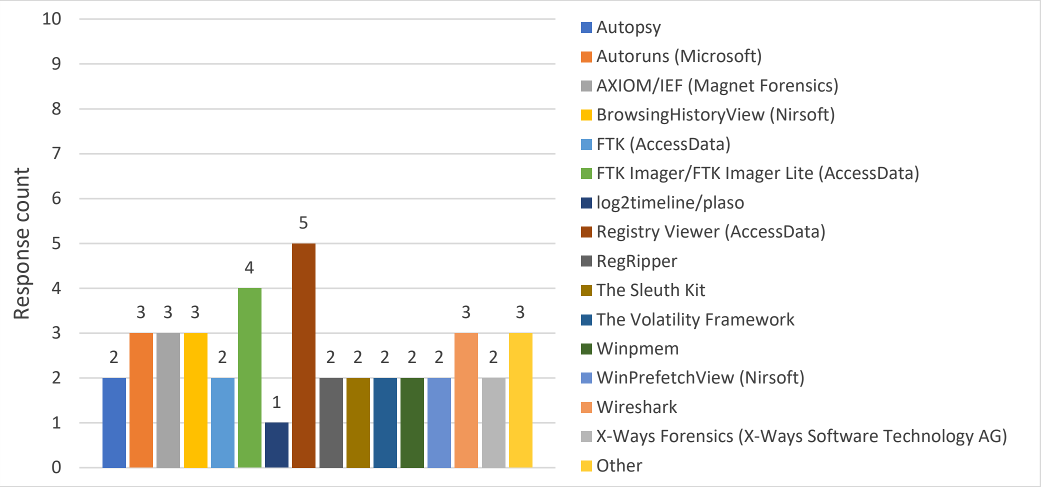
Q10 Has your company performed digital forensics in the past regardless of using internal or external resources? And how often? (Select one)



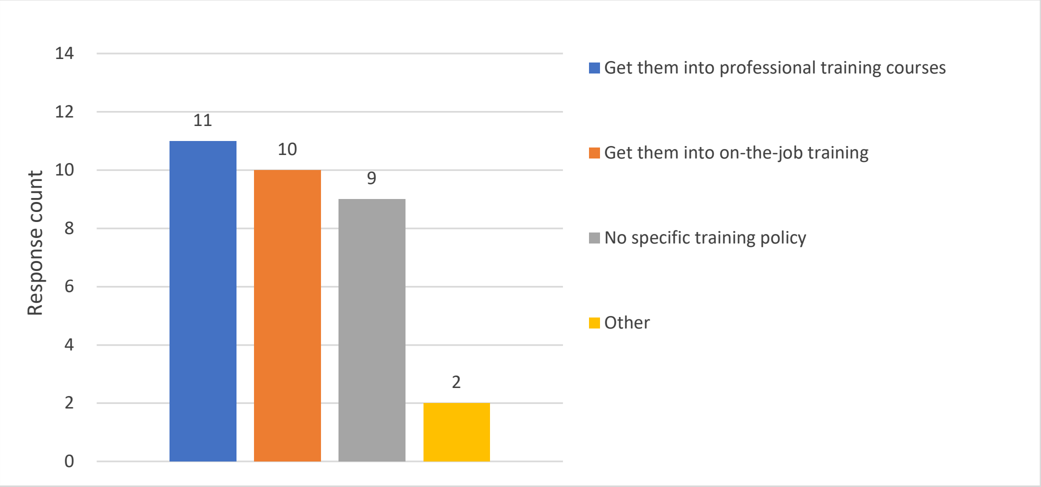
Q11 For those who selected “Yes” in Q10 which forensics process did your company's employees perform? (Multiple choice)



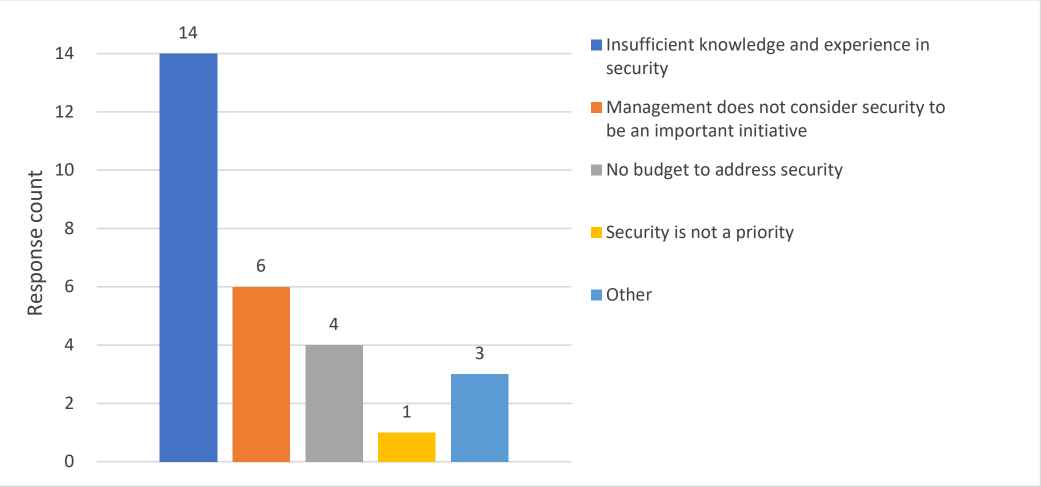
Q12 For those who selected “Yes” in Q10, which forensics process did your company's employees perform? (Multiple choice)



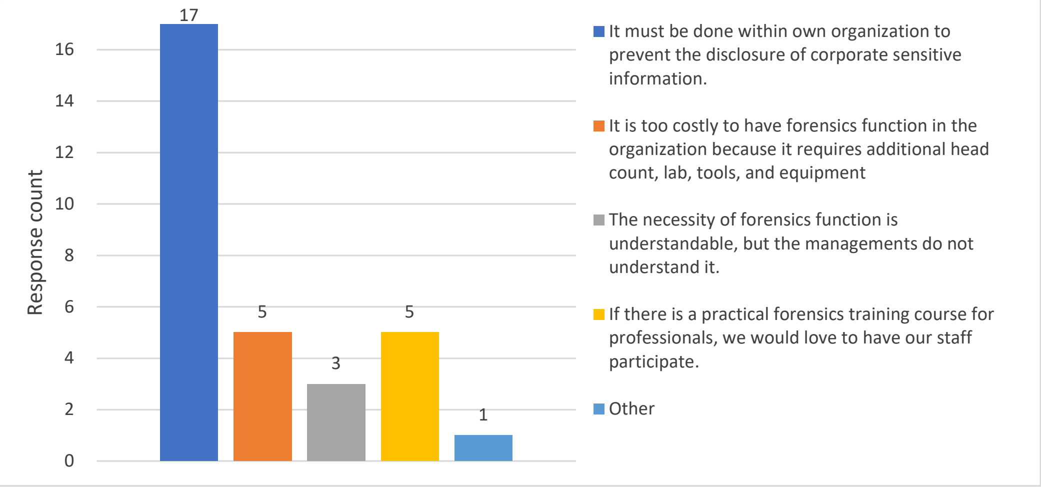
Q13 How do you train employees to perform digital forensics? (Multiple choice)



Q14 Please select the security challenges your company faces. (Multiple choice)



Q15 What do you think of the necessity of digital forensics ? (Multiple choice)



Q16 Please feel free to describe anything you would like to say about digital forensics.

As a digital forensics expert, I see that digital forensics become more important and urgent to continuously develop not only to investigate the security incident, but also to fight against any computer/technology-based crimes and any fraud occurring in any organization. Please contact me for further discussion -> izazi.mubarok@afdi.or.id
Digital Forensic must be learned and developed constantly following the development of Information Technology. Never stop to explore digital forensic in various digital evidence. There are 4 pillars to strengthen Digital Forensic, namely: 1. Qualified Examiners, according to ISO/IEC 27035, 27037, 27042 2. Reliable Tools, according to NIST, Interpol Digital Forensic Experts Group, ISO/IEC 27037, 27042 3. Validated Methods and Standards, according to ISO/IEC 27035, 27037, 27042 4. Accredited Laboratory, according to ISO/IEC 17025
Digital forensic is very expensive but important to implement in every organization with centralized monitored regularly by advanced specialists team in security.
Hal ini penting namun, masih butuh banyak system & sdm yg perlu di perbaiki & di latih
It's becoming more and more important especially in nowadays since everything is connected in digital information world
It is very important to look for digital traces that can indeed be done to look for errors or fraud in a company
I'm not understand about digital forensics
System and data are company assets that need to be manage professionally
Very necessary
Company need digital forensic to investigate employee violation, ethic violation, corruption and other crime done.
Important like insurance, to make sure everything has tracking

APPENDIX E RATING SCORE SHEET FOR TRIAL LESSON

	Category	No.	Evaluation point	Score (*1)
A	Basic knowledge of the field	1	Are there any deficiencies in essential basic knowledge such as operating systems and networks?	
B	Understanding of class contents andappropriateness of explanation	2	Are there any ambiguous explanations of the content that may indicate a lack of understanding?	
		3	Are there any incorrect explanations?	
		4	Are the purposes and cautions explained in the explanation of tools and techniques?	
		5	Are the answers to questions appropriate?	
		6	Are the purpose and goal of the exercise explained?	
		7	Are the positioning of this course among the cybersecurity courses and the learning path (what they need to learn before and after) explained?	
C	Sufficiency of course content (no omissions)	8	Does the lecture cover all the content of the section?	
D	Teaching Techniques	9	Does he / she try to improve students' understanding by giving concrete examples?	
		10	Does he / she try to keep students' concentration by asking questions?	
		11	Is the time allocated for classes, lectures, and exercises appropriate?	
		12	Is there any follow-up for students who do not understand well?	
E	Appropriateness of materials	13	Have the materials been deleted/changed/added?	

*1 Score: 1~5 or N.A. for not applicable

1=Bad (Unable to teach)
2=Poor (Only an assistant)
3=Fair (Can teach with support)
4=Good (Can teach independently)
5=Excellent (Recommended lecturer)

( ) expresses "How about a lecturer?"