

**Cyber Defense Initiative Conference 2022**

# **ASEAN-Japan Cybersecurity Cooperation and Human Resource Development Program**

Office for STI & DX  
Governance and Peacebuilding Department  
Japan International Cooperation Agency (JICA)

10<sup>th</sup> November 2022



1. JICA
2. Global Agenda
3. DX & Cybersecurity Strategy
4. Cybersecurity Cooperation
  - Indonesia
  - Viet Nam
  - Cambodia
  - Training in Japan
  - Thailand (AJCCBC)





## Leading the World with Trust

JICA, with its partners, will take the lead in forging bonds of trust across the world, aspiring for a free, peaceful and prosperous world where people can hope for a better future and explore their diverse potentials.



**16.5 billion** USD

 **1,500 +** PROJECTS

 **13,217** People Trained

 **9,163** Experts and Volunteers

 **150** Countries & regions in operation

 **96** Overseas offices

 **14** Domestic offices

 **1,929** Staff members

\* Approximately 16.5 billion USD with the exchange rate as of March 2020

## Human Security

Fostering societies where all the people can protect themselves from various threats and lead their lives in security and with dignity

## Quality Growth

Promoting sustainable growth with less disparity and without harming environment



Societies where all can live healthy, safe lives

People



Peaceful, just societies without fear and violence

Peace



Prosperous, sustainable economies at harmony with nature

Prosperity



Care for the Planet

Planet



- JICA's cooperation strategies for global issues, stating priorities, targets, and approaches **towards the achievement of SDGs**
- **Maximizing development impacts** on the global issues through further strengthening **partnership among diverse actors** to tackle complex challenges the world faces.



## Prosperity

1. Urban and Regional Development
2. Transportation
3. Energy and Mining
4. Private Sector Development
5. Agriculture and Rural Development

## People

6. Health
7. Improving Nutrition
8. Education
9. Social Security and Development
10. Sport and Development

## Peace

11. Peacebuilding
12. Governance
13. Public Finance and Financial Systems
14. Gender Equality and Women's Empowerment

## 15. Digital for Development

## Planet

16. Climate Change
17. Nature Conservation
18. Environmental Management
19. Sustainable Water Resources Management and Water Supply
20. Disaster Risk Reduction through Pre-disaster Investment and Build Back Better





## JICA Global Agenda

JICA's 20 Strategies for Global Development Issues

NO. 15

## Digital for Development

### DX to Improve Well-being for All

Aiming for a resilient society ensuring people's safety, diverse opportunities and well-being with digital technology.





LDCs have big potentials to reap the benefits of global digitalization

Global **DX Market** has Annual Growth of

**16%**



Global **Smartphone** penetration

will increase **65%** in 2016

To **80%** in 2025

ISSUES > What are the current challenges?

## The Digital Divide and the Cyber Security are Serious Threats.



**3.3** billion people still have no access to the Internet

Cybercrime causes  
**\$1 trillion**  
of damages per year



## Goals

### Innovation Ecosystems

Harness digital technologies and create innovation ecosystems to solve social issues.

### Enabling Environments

Develop infrastructure to promote the benefits of digitization and reduce disparities and cybersecurity risks.

## Focus Areas

### Driving DX across the Sectors



### Basic Infrastructure for Free & Secure Digital Economy

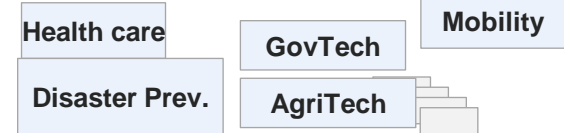
ICT/Digital Infrastructure

Digital Skills and Business

Cybersecurity

### DX Challenges / Leads

Launch quick-win DX use cases for JICA ODA projects and promote the long-run DX mainstreaming in target sectors and regions.



### Cybersecurity

Capacity building on cybersecurity especially Asia Region countries by referring Data Free Flow with Trust (DFFT) concept.

- In order to promote digitalization in developing countries, it is essential to realize a free and secure digital society, which is the basis of digitalization.
- From the perspective of Japan's security as well, Japan is expanding assistance with cyber security as a priority area.
- Mainly, (1) cooperation focused on improving the capacity of the national CSIRT, which serves as the base, (2) cooperation that contributes to human resource development in the partner country, and (3) literacy improvement, such as training and enlightenment activities for public institutions, including critical infrastructure operators.

Disclaimer: The representations on the map are for illustrative purposes only and do not represent JICA's views on the legal status, borders and demarcations thereof, or geographical names in any country or region.

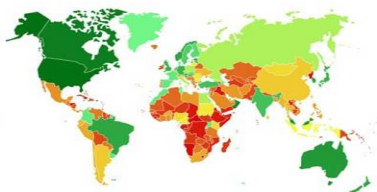
- 
- ASEAN:** ASEAN-Japan Capacity Building Program for Cybersecurity and Trusted Digital Services
  - Indonesia:** Human Resource Development for CS Professionals
  - Vietnam:** Capacity Building for Cyber Security
  - Cambodia:** Improvement of Cyber Resilience
  - Malaysia:** 5G and Cybersecurity Training
  - Mongolia:** Development of HR in Cybersecurity
  - Bangladesh:** Capacity Development on Cyber Security
  - Kirgizstan:** Strengthening Capacity of Cybersecurity
  - Armenia:** Cybersecurity Training

## Training in Japan

- Defense Practice Against Cyber Attacks
- International Law and Policy Formation for Enhancement of Cybersecurity

Disclaimer: The representations on the map are for illustrative purposes only and do not represent JICA's views on the legal status, borders and demarcations thereof, or geographical names in any country or region.

**GLOBAL  
CYBERSECURITY  
INDEX**

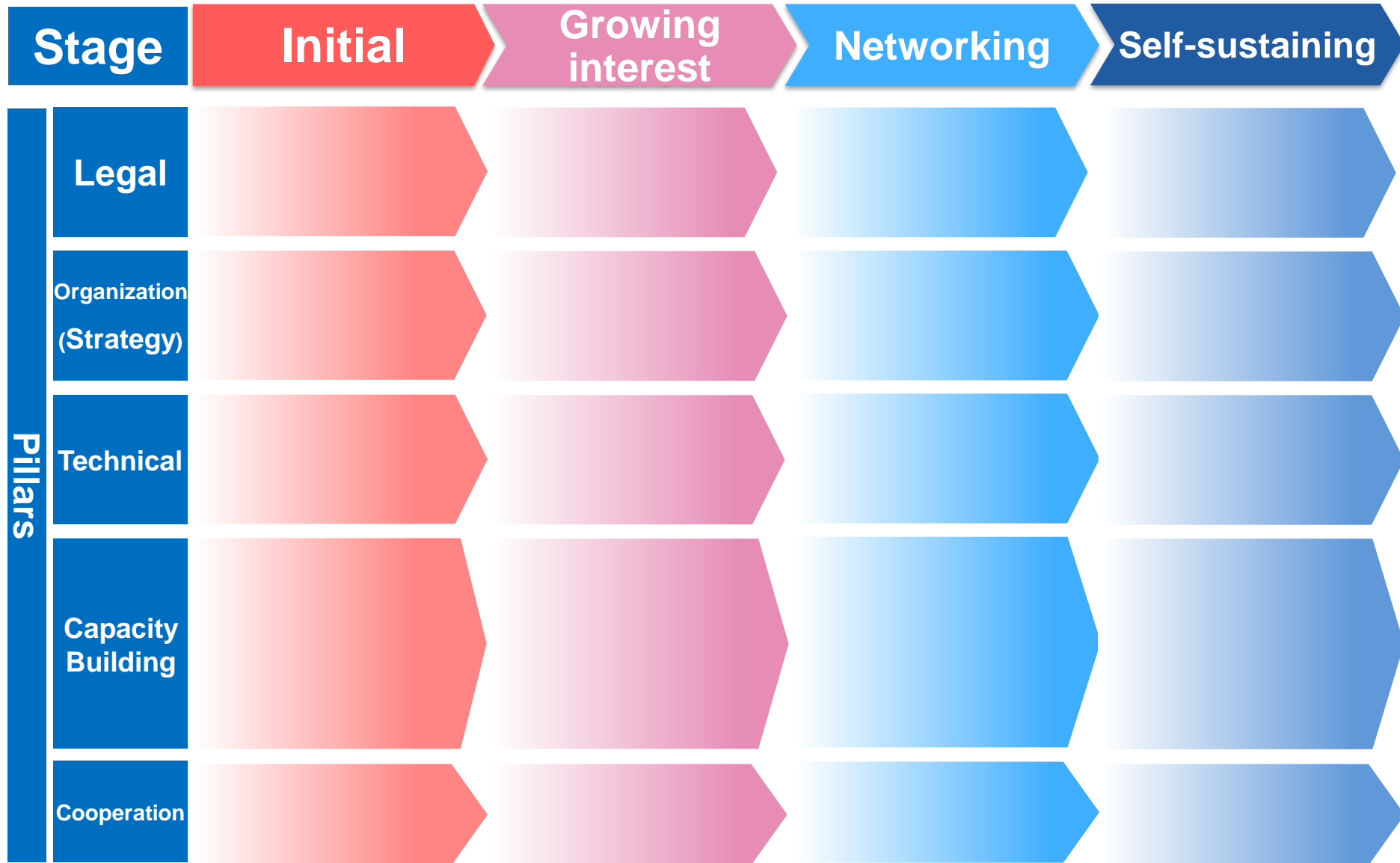


## Ranking among 193 + 1 countries

	2020	2018	2017
US	1	2	2
Korea	4	15	13
Singapore	4	6	1
Malaysia	5	8	3
Japan	7	14	11
Indonesia	24	41	70
Viet Nam	25	50	101
Thailand	44	35	20
Philippines	61	58	37
Brunei	85	64	53
Myanmar	99	128	99
Lao	131	120	77
Cambodia	132	131	92



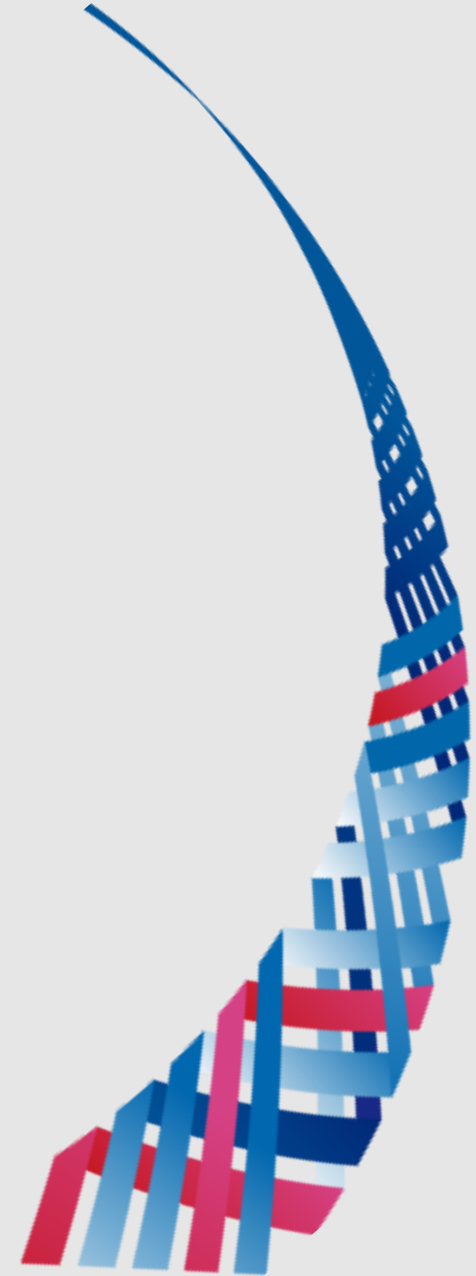
# Cooperation for Cyber Security





# Cybersecurity Cooperation

- Indonesia
- Viet Nam
- Cambodia
- Training in Japan
- Thailand (ASEAN)



- Period: 2019.6- 2024.6 (5 years)
- Implementation agency
  - University of Indonesia (UI)
  - Ministry of Communication and Information Technology



## Project purpose

Cyber security (CS) professionals demanded by the Indonesian ICT entities are developed in University of Indonesia (UI)

### Output1

CS short courses are held by UI  
*(Master degree level)*

**Commercial Academy Course, Customized hands-on training etc.**

### Output2

Open source CS tools are localized or developed

### Output3

Open courseware in CS is developed and opened to public

### Output4

A network for CS entities among the world is strengthened

**Provide training to neighbor Countries (CLMV, TL)**

## Course objective

- Learn how to make decision makers understand the importance of cybersecurity

CIO, CISO, IT dev. head  
**(Course participants)**



**CEO, CFO etc.**

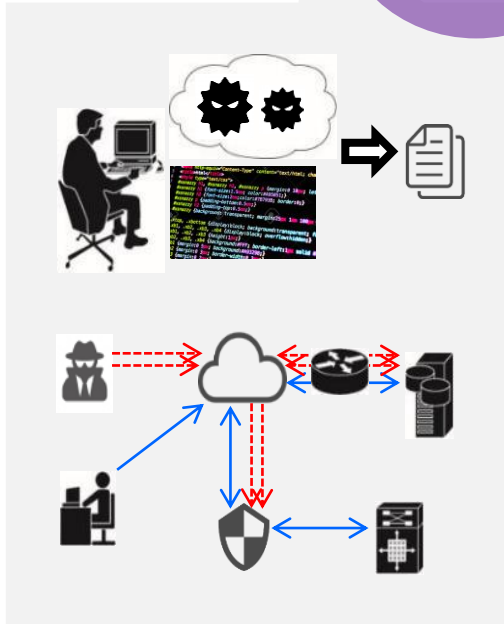
## Course contents

- CEO's way of thinking, Impact of incidents to Profit & Loss Statement, Balance Sheet and stock price
- Cyber incident response exercise using movie, Risk management
- Effective reporting and presentation technique

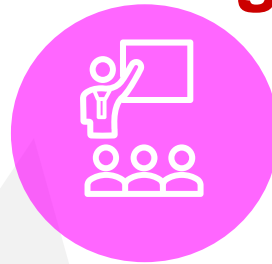


<b>Overall Goal</b>	<b>Cyber Resilience for Vietnamese Government is Increased</b>
<b>Project Purpose</b>	Capacity of AIS for Cybersecurity is Enhanced

## Equipment



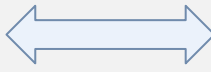
## Training



Task Role



Skill



Ability range

**Career Development Plan**

Role : **Incident Handler**

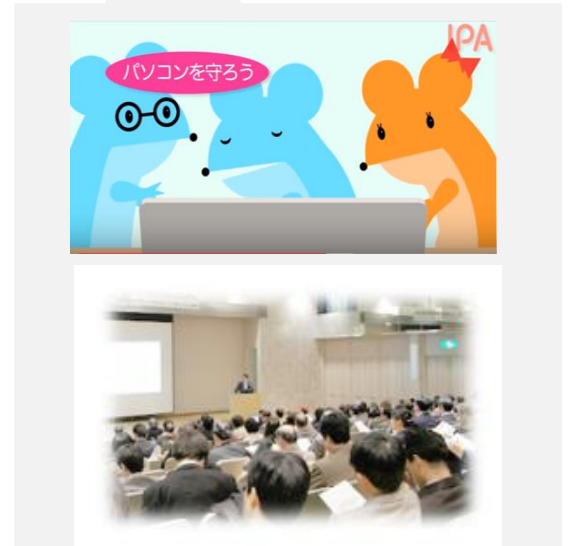
Current skill: ○○○, ◇◇◇

Required skill: △△△, □□□

Required training: Course **B, D**

Training schedule

## Materials for Awareness Raising



## Security Training

A total of about **654 people were trained**, contributing to the development of cyber security professionals within the Vietnamese government.

Individual **144** people, Total **87** course,

Ratio of who passed the international certification exam to trainees: **57.7 %**

Ratio of who passed the international certification exam to examinees: **77.4 %**

## Security Body of Knowledge (SecBoK)

## Security roles

### <Level of knowledge and skills>

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

<b>1</b>
<b>2</b>
<b>0.5</b>

KSA -ID	Field	Level	KSA (knowledge, Skill, Ability) Description	Commander, Triage	Incident manager, Incident handler	Curator	Researcher	Self assessment, Solution analyst	Vulnerability diagnostic consultant	Education / Awareness raising
K0288	01 IT/Security Basics	L	Knowledge of industry standard security models.			1	1	1		
K0203	01 IT/Security Basics	M	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).			0.5	0.5	0.5	0.5	
K0059	01 IT/Security Basics	L	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	2	2	2	2	2	2	2
K0147	01 IT/Security Basics	L	Knowledge of emerging security issues, risks, and vulnerabilities.	2	2	2	2	2	2	2
K0239	02 IT Human Skill	M	Knowledge of media production, communication, and dissemination techniques and methods, including alternative ways to inform via written, oral, and visual media.							1
S0070	02 IT Human Skill	M	Skill in talking to others to convey information effectively	1	2			2		1

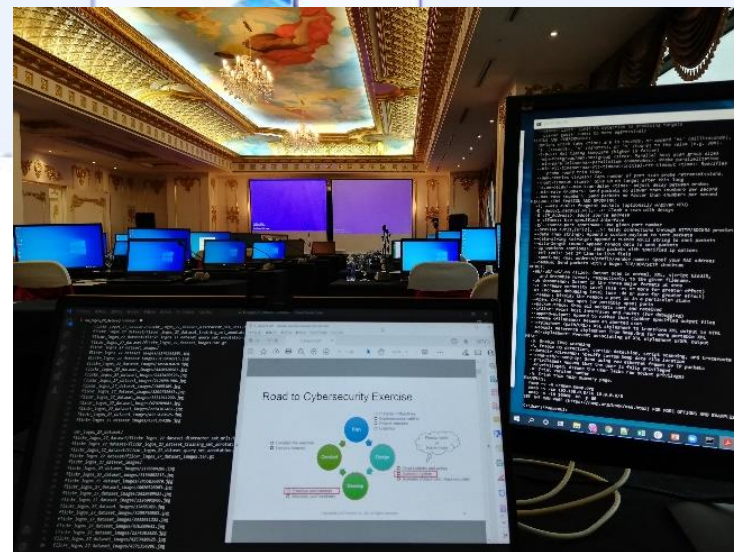
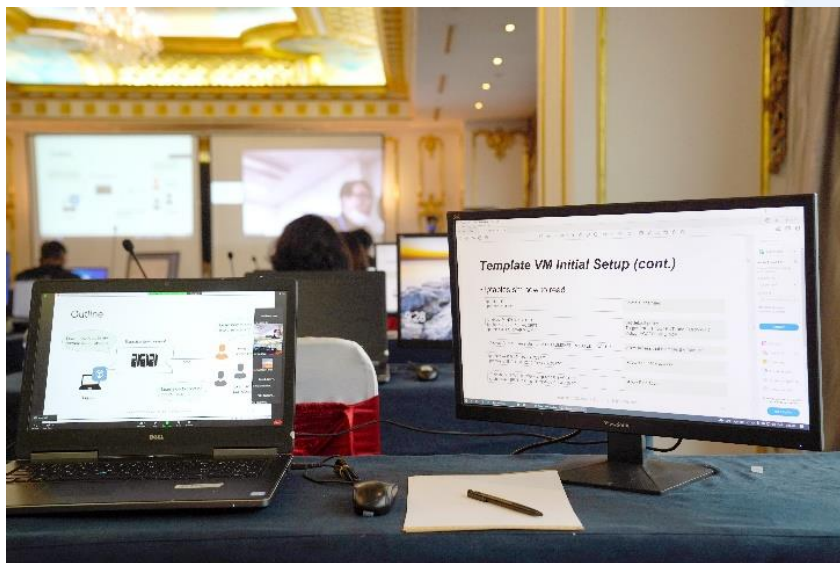
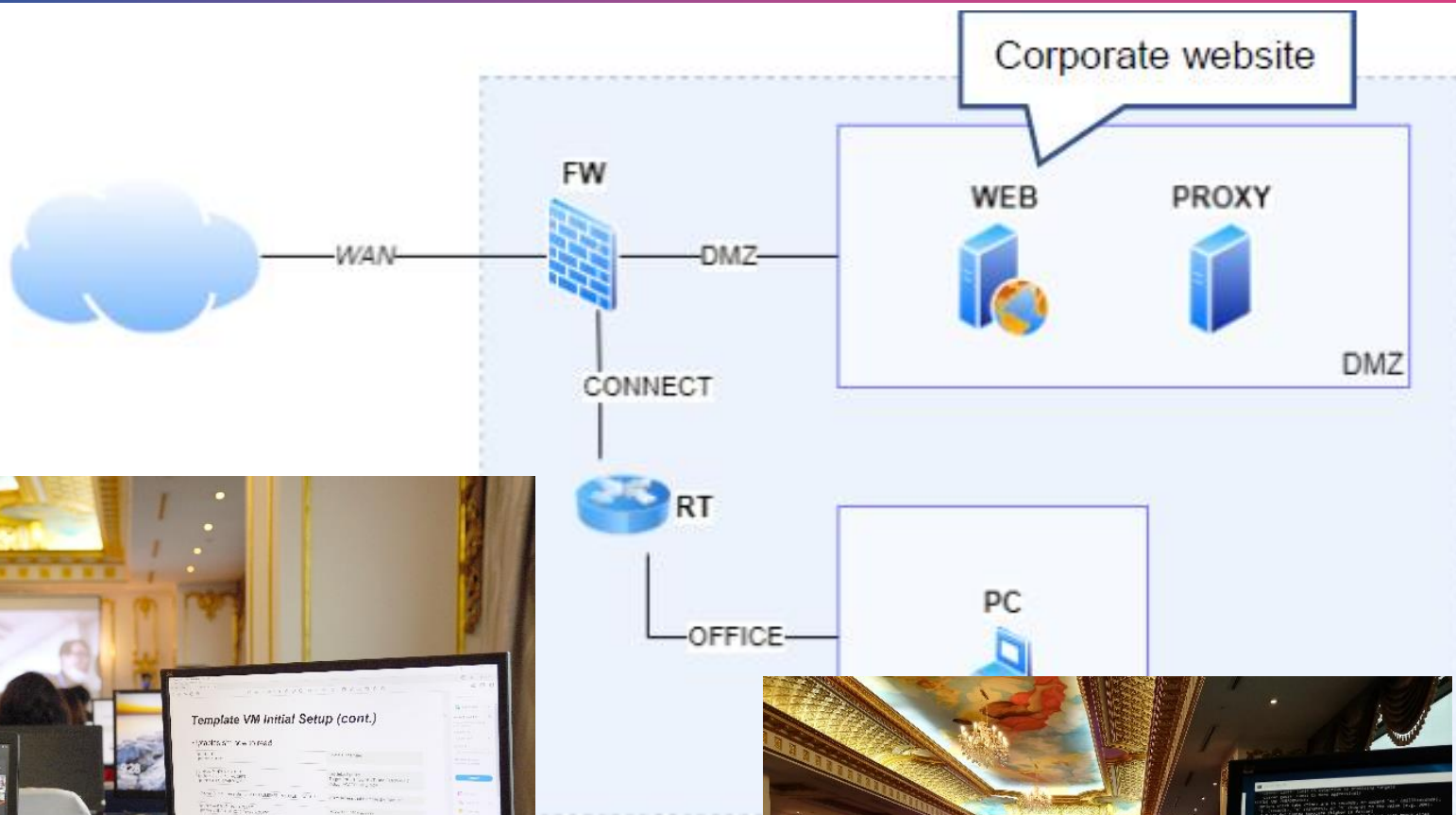
## Knowledge, Skill, Ability

## Security Roles and Course Mapping

- = Mandatory
- = Suggested
- If the number is given, choose one from same numbered training courses

Training Course				CISO	POC	Notification	Commander	Triage	Incident manager	Incident handler
Category	Course / certificate title	Abbreviation	Vendor							
Management	Certified Information Systems Security Professional	CISSP	(ISC)2	●			○		○1	
	Certified Information Security Manager	CISM	ISACA	○					○1	
	Certified Information Systems Auditor	CISA	ISACA	○						
Basic cybersecurity	CompTIA Security Plus	CompTIA S+	CompTIA		○1	○1		○1		
	Certified Security Specialist	ECSS	EC-Council		○1	○1		○1		
Network	Certified Network Associate	CCNA	Cisco							○1
	Certified Network Professional	CCNP	Cisco							○1
	Certified Network Associate Security	CCNAS	Cisco							○
Pentest / Forensic	Certified Ethical Hacker	CEH	EC-Council				○			●2
	Licensed Penetration Tester	LPT	EC-Council							○
	Computer Hacking Forensic Investigator	CHFI	EC-Council				○			●2





# 1. Animation videos for Child Online Protection



<https://www.youtube.com/channel/UCz39i69Rz9nbqzffcziCqsw>

## 2. COP portal website



<https://vn-cop.vn/>

## 3. Branding kit

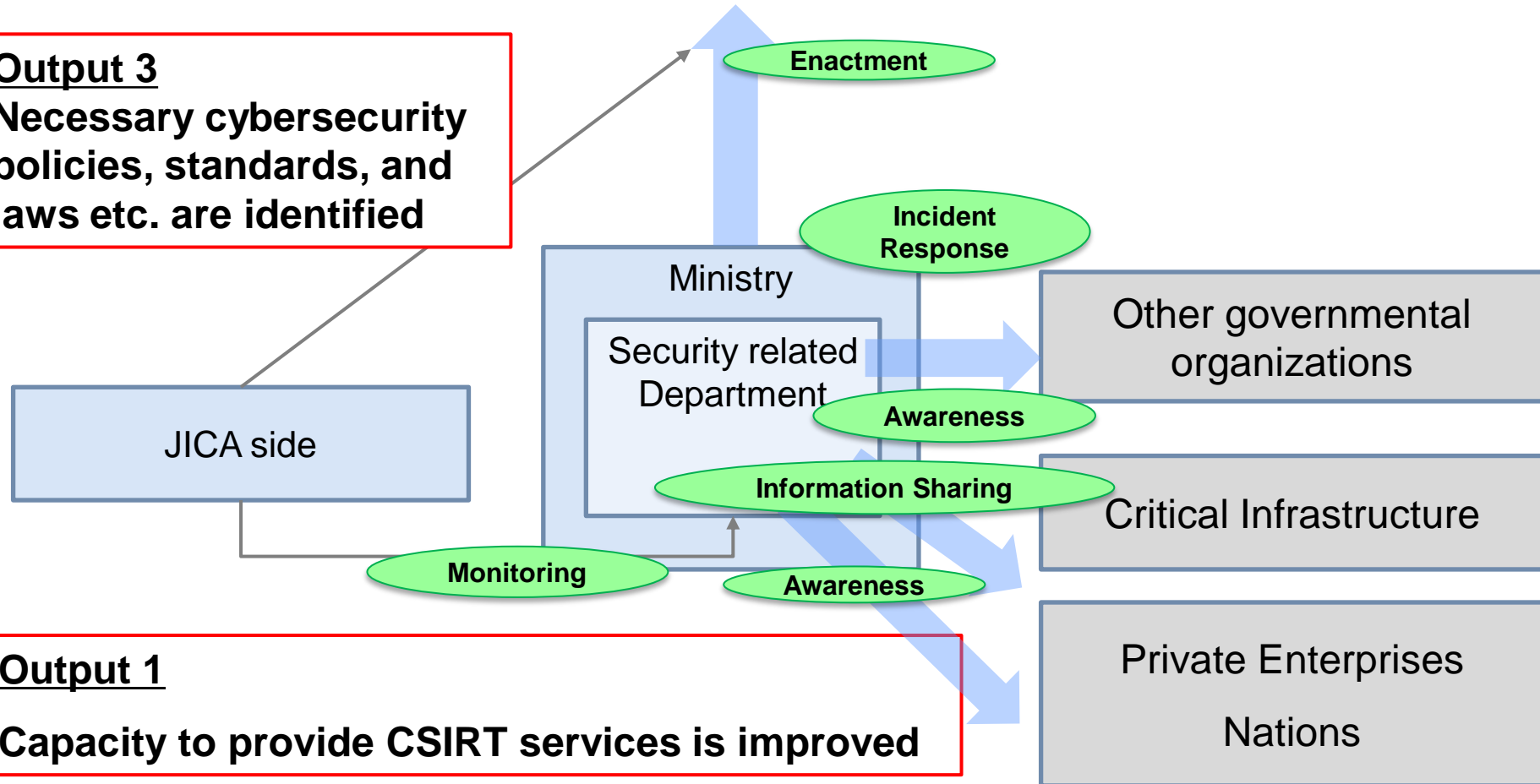


**VN-COP Network**  
Không gian mạng an toàn, công dân số tương lai



Policies, Strategy, Laws, Regulations and Standards etc.

**Output 3**  
Necessary cybersecurity policies, standards, and laws etc. are identified



**Output 1**  
Capacity to provide CSIRT services is improved

**Output 2** Activities for strengthening cybersecurity of related organizations (other ministries, CII operators, etc.) will be enhanced

# AJCCBC

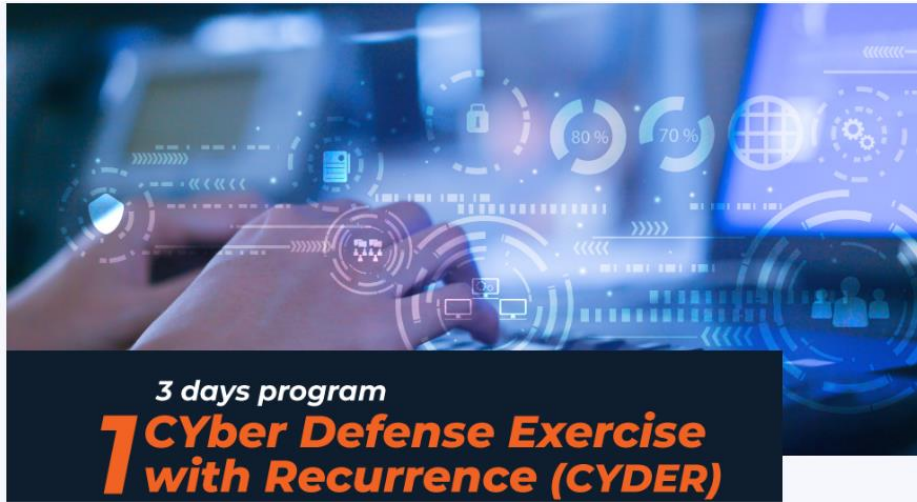
**ASEAN-JAPAN  
CYBERSECURITY  
CAPACITY BUILDING CENTRE**



The ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) was established under the guidance of TELMIN/SOM in 2018 and funded by Japan ASEAN Integration Fund (JAIF 2.0) with the aim to develop a cybersecurity workforce of 700+ over 4 years to enhance the capacity of cybersecurity experts and specialists in the ASEAN Member States (AMS) by providing trainings and other activities to participants from AMS.



# AJCCBC – 3 days training program



3 days program  
**1 Cyber Defense Exercise with Recurrence (CYDER)**



2 days program  
**3 Hands-on Malware Analysis**



2 days program  
**2 Hands-on Network Forensics**



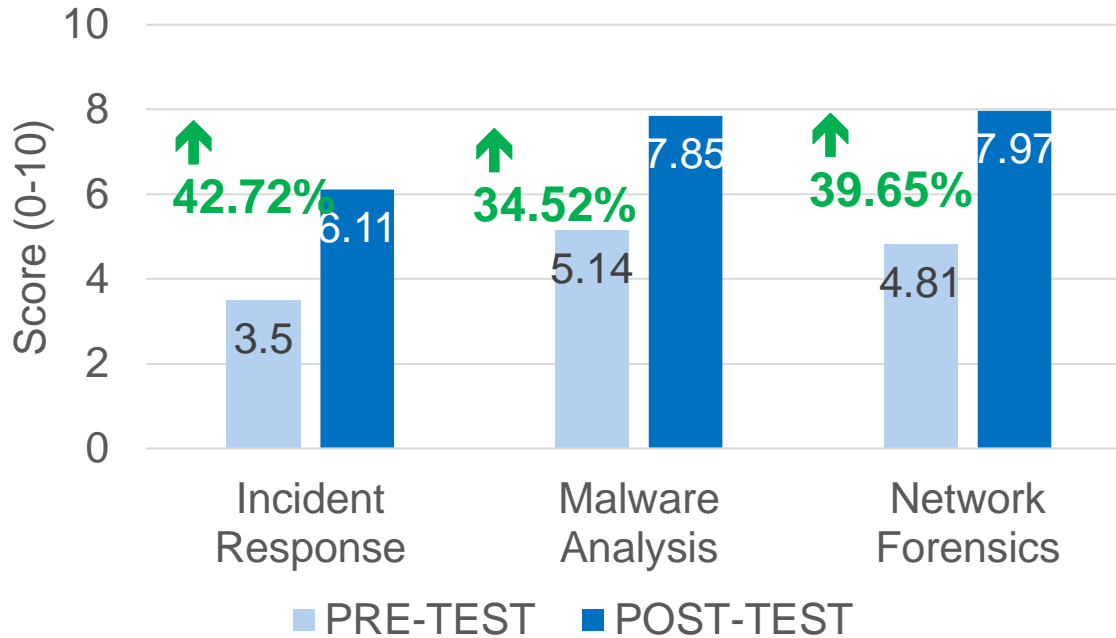


3 days program

**4** **Cyber SEA Game**  
(ASEAN Youth Cybersecurity  
Technical Challenge)

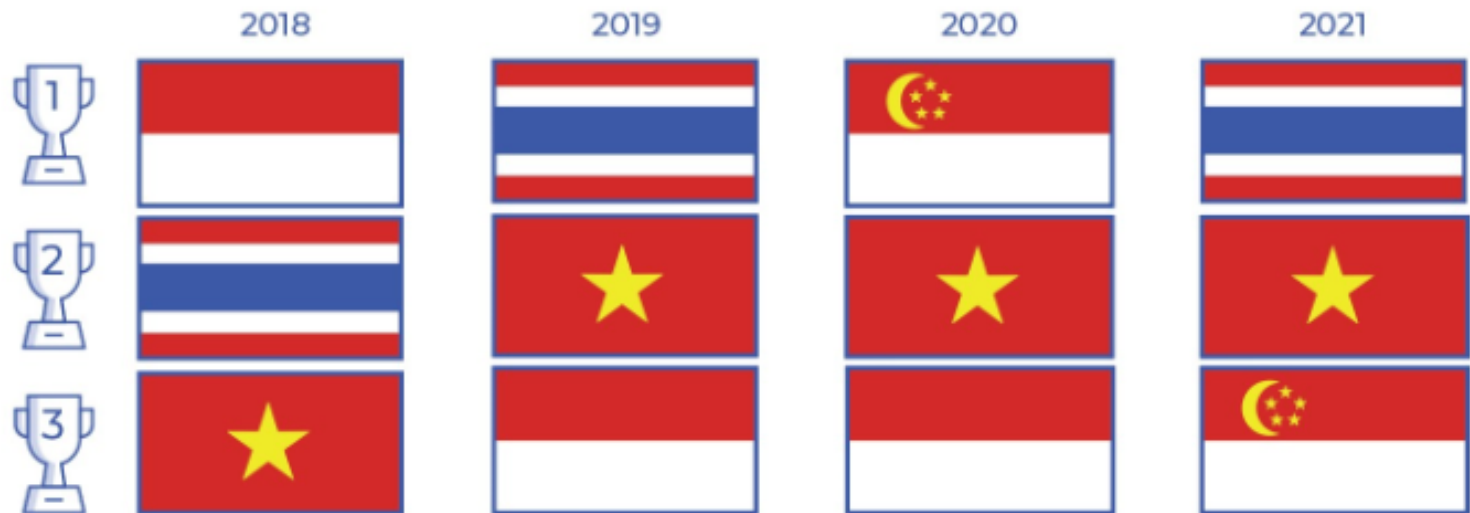
# ASEAN Member States - Improvement

Training Improvement



The comparison between pre-test and post-test suggests that the capacity of the personnel was remarkably enhanced.

Cyber SEA Game Champions





The most required 3 cybersecurity skills are Threat Intelligence analysis, Penetration testing, and Security analysis.

(According to the survey in 2021 among 76 AJCCBC alumni)

- 
- #1 Threat intelligence analysis**
  - #2 Penetration testing**
  - #3 Security analysis**
  - #4 Cloud computing security
  - #5 Risk assessment, analysis and management
  - #6 Data management protection
  - #7 Application security
  - #8 Governance risk management and compliance
  - #9 Security engineer
  - #10 Security administrator

## Major Activities



Period: Mar. 2023 - Feb. 2027  
Target: ASEAN member states

01



- Hands-on Training for ASEAN Cybersecurity Professionals will be held 6 times every year
- E.g., CYDER exercises, Network Forensics, Malware Analysis, Trusted Digital Services course

02



- Cyber SEA Game (ASEAN Youth Cybersecurity Technical Challenge) will be held once time a year
- Winner will be invited to the SECCON final match held in Japan

03



- Seminar, Hands-on or Self-learning Cybersecurity-related course with 3<sup>rd</sup> parties
- Research activities



## Looking for possible partnerships with private sectors for ASEAN

1. Potential partners in Thailand who could provide;
  - Cybersecurity training courses
  - Other related services or training courses, seminars, webinars, etc.
  - Data collection survey
2. General cybersecurity market outlook in Thailand and ASEAN.
3. Potential partners who could provide cybersecurity training/seminar/webinar in Cambodia, Philippines, or other countries in ASEAN and Asia.



# Digital transformation

JICA, Office for STI and DX

YAMAZAKI Hiroto ([yamazaki.hiroto3@jica.go.jp](mailto:yamazaki.hiroto3@jica.go.jp))



JICA DX website

<https://www.jica.go.jp/activities/issues/digital/jicadx/index.html>



JICA Channel

<https://www.youtube.com/user/jicachannel1>