# HOW TO MAKE TOP MANAGEMENTS AWARE OF CYBERSECURITY

## Course Syllabus

Cyber Security Professional Program

Subject Code: COM0010a / Version: 1.0
Updated on 29/09/2021

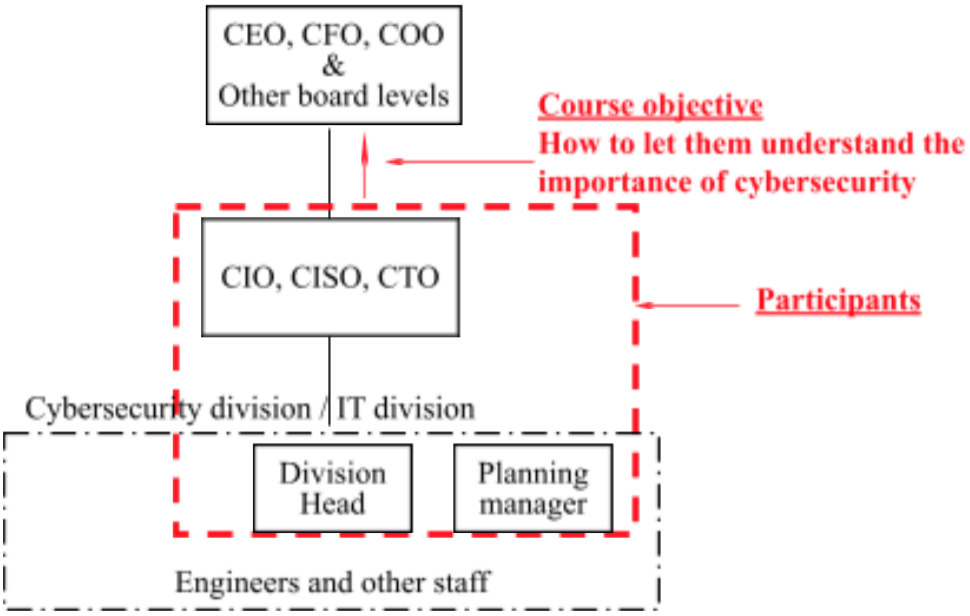
Official content of **idCARE.UI**
Indonesia Cyber Awareness and Resilience Center

Supported by **JICA**
Japan International Cooperation Agency

# Course Syllabus

As of 29 Sept 2021

| | |
|---|---|
| Course Title | **How to Make Top Managements Aware of Cybersecurity** |
| Course goals | The participants are expected to understand how to make decision makers (CEO and other board level management) aware of the importance of cybersecurity and practice it. |
| Course Objective | 1. Module 1:<br>Able to explain the methodology and relevant subjects of the decision makers' thoughts and responsibility on cybersecurity.<br>2. Module2:<br>Able to propose appropriate responses to the cyber incident.<br>3. Module 3:<br>Able to recognize various types of cybersecurity attacks and their impacts on the organization.<br>4. Module 4:<br>Able to explain basic cybersecurity risks, management and assessment.<br>Able to show decision makers the specific steps to improve the cybersecurity of their own organization.<br>5. Module 5:<br>Able to manage cyber risk processes including identification, analysis, evaluation and addressing organization’s cybersecurity threats.<br>6. Module 6<br>Able to make effective reports and presentations on the importance of cybersecurity for decision makers. |
| Participants | CIO, CISO, CTO and IT planning managers in the enterprises and government sectors. |

| | |
|---|---|
| Diagram: course objective and participants |  CEO, CFO, COO<br>&<br>Other board levels<br>Course objective<br>How to let them understand the importance of cybersecurity<br>CIO, CISO, CTO<br>Participants<br>Cybersecurity division / IT division<br>Division Head<br>Planning manager<br>Engineers and other staff |
| Prerequisites | The participants should have experience in managing IT related divisions or sections, and have basic knowledge of cybersecurity. |
| Course content and schedule<br><br>16 sessions<br><br>(1session = 50min) | ***Pretest***<br><br>**1. Module 1: Introduction**<br><br>1.1. What do decision makers think of cybersecurity?<br>● A decision maker's responsibility<br><br>***Module 1 Test***<br><br>**2. Module 2: Cyber Incident Response Exercise Using Movie**<br><br>2.1. Group discussion with movie material<br>● Cyber incident happens and grows bigger with unexpected reasons<br>● Think of appropriate response towards the cyber incident<br>● Group discussion and presentation<br><br>***Module 2 Test***<br><br>**3. Module 3: Cyber Attacks**<br><br>3.1. Understanding cyber-attack situation<br>● Who attacks and why?<br>● Resources for cyber attacks<br>● Exercise and discussion<br><br>3.2. Today's cyber attacks<br>● Example of cyber attacks<br>● Exercise and discussion<br><br>3.3. Vulnerability and malware<br>● Vulnerability database |

- Malware types

***Module 3 Test***

**4. Module 4: Cybersecurity Management**

4.1. Cybersecurity risk and management
- Cybersecurity as business risk
- FIVE key items for good cybersecurity management
- Exercise and discussion

4.2. Cybersecurity assessment
- Cybersecurity assessment vs risk assessment
- Cybersecurity assessment framework
- Exercise and discussion

4.3. 10 steps to cybersecurity

***Module 4 Test***

**5. Module 5: Risk Management**

5.1. Capturing and controlling risks
- Risk identification
- Risk assessment
- Risk mitigation and control
- Exercise and discussion

5.2. Calculation of Impact to Financial Statement
- Evaluation of Reported Loss
- Recoverable Revenue/Cost
- Exercise and discussion

5.3. Top Management Prioritization Framework
- Calculate the costs and losses
- Exercise and discussion

***Module 5 Test***

**6. Module 6: Effective Reporting and Presentation Technique**

6.1. How to effectively appeal the importance of cybersecurity to decision makers.
- Logical and Efficient
  - Pyramid Structure
  - MECE
- Strategic presentation
  - AUCDA framework
- Tips for presentation

6.2. Exercise and discussion

| | |
|---|---|
| | ***Module 6 Test***<br>***Post Test*** |
| Scheme of Instructions | Lecture 100%   Hands-on Training 0% |
| Keywords | Cybersecurity, management, decision maker, awareness, ciso, cio, cto, it manager, risk management, cybersecurity assessment, cybersecurity framework, risk quantification, financial statement, reporting technique, presentation technique, cybersecurity investment |
| Tools (software) required for hands-on training | **N. A.** |
| Reference books | 1. Introduction to Cybersecurity Management (ASIN: B07QSBSDQN)<br>2. CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers 1st Edition (ISBN 1498740448)<br>3. CISO Desk Reference Guide: A Practical Guide for CISOs (ISBN 0997744154)<br>4. CISO Desk Reference Guide Volume 2: A Practical Guide for CISOs (ISBN 0997744146)<br>5. World-Class Risk Management (ISBN 151199777X)<br>6. Superforecasting: The Art and Science of Prediction (ISBN 0804136696)<br>7. The Pyramid Principle: Logic in Writing and Thinking (ISBN 0273710516)<br>8. TED Talks: The Official TED Guide to Public Speaking (ISBN 0544634497) |