

# **Introduction of “CRIC Cross Sectors Forum(CSF)”**

Wednesday, 11th October, 2017  
CRIC Cross Sectors Forum

# Agenda

1. Cross Sectors Forum's Overview
2. Activities and Results on 1<sup>st</sup> period and Current
3. Top layers meeting
4. Future work plan

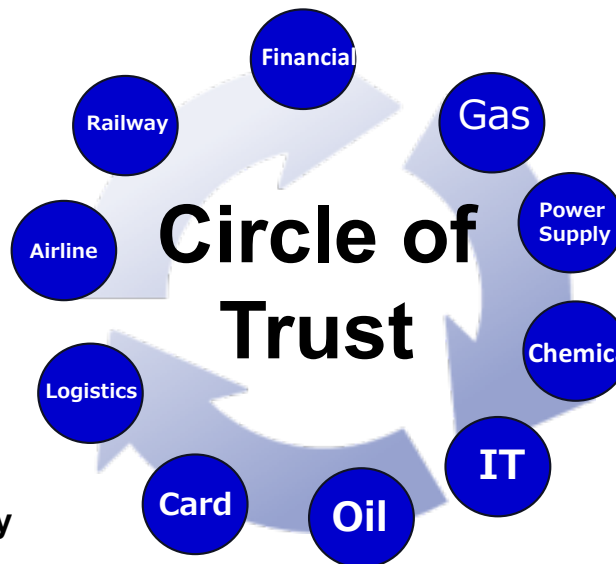
# **1. Cross Sectors Forum's Overview**

# CRIC Cross Sectors Forum

## Cyber Risk Intelligence Center Cross Sectors Forum - CRIC CSF"

- [URL: http://cyber-risk.or.jp/](http://cyber-risk.or.jp/)
- Launched in June 2015
- Trigger to Launched: Advisory Board of Cybersecurity in "Keidanren"
- Published a cybersecurity policy proposals to the Japanese government in February 2015
- More than 30 companies mainly from 13 Critical Infrastructure Industries (e.g. Finance, Airline, Railway, Power, Energy etc)

**ANA**  
**DNP (Printing)**  
**Fujitsu**  
**Hitachi**  
**JAPAN POST HOLDINGS**  
**JX Holdings**  
**KDDI**  
**KDDI Research**  
**Mitsubishi Corp.**  
**Mitsubishi Electronics**  
**Mitsubishi Heavy Industry**  
**Mizuho Financial Group**  
**NEC**  
**NHK**  
**NTT**

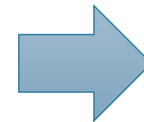


**NYK Line (Transportation)**  
**Nikkei Newspaper**  
**Nippon Express Company**  
**Nippon TV**  
**Nissei (Life Insurance)**  
**Panasonic**  
**Pasona (Staffing)**  
**SONY**  
**Sumitomo Chemical**  
**TBS**  
**Tokyo Gas**  
**Toshiba**  
**Toyota**  
**Yamato Holdings**  
**etc.**

# Motivation of Collaboration

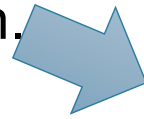
- Readiness enhancement and workforce development are common challenges among industries.
- It is impossible to protect everything by a single company.
- Collaboration beyond sectors is imperative.

- Need **the opportunity for sharing information** that companies want to know/are worried about, but they can't ask/don't know who knows.



Information  
sharing

- Need **the definition of security workforce** to clarify industry needs for effective recruitment and education.



- Expected cost reduction by **sharing workforce development programs and tools**.



Workforce  
development

- Develop professionals who match the needs from industries by educating promising students (**e.g. university students**) who are interested in security.



Industry-  
academia  
Cooperation

## **2. Activities and Results on 1<sup>st</sup> period and Current**

# Working Groups in 1<sup>st</sup> period

(June 2015 – September 2016)

- Set the following groups and promote “Information Sharing”, “Workforce Development”, and “Industry-Academia Cooperation”
- It is important to construct “Circle of Trust” because enhancing cybersecurity readiness is imperative.



# Key considerations on Workforce definitions

The Forum considers the characteristics and circumstances of Japanese companies to make our workforce definitions practical.

Wide variety industries

We build our forum **to cover Japanese wide variety industries.**

Specific characteristics of Japanese companies

We carried out the discussion on **Japanese companies' culture and practices** by specifically clarify that the typical structure of Japanese companies

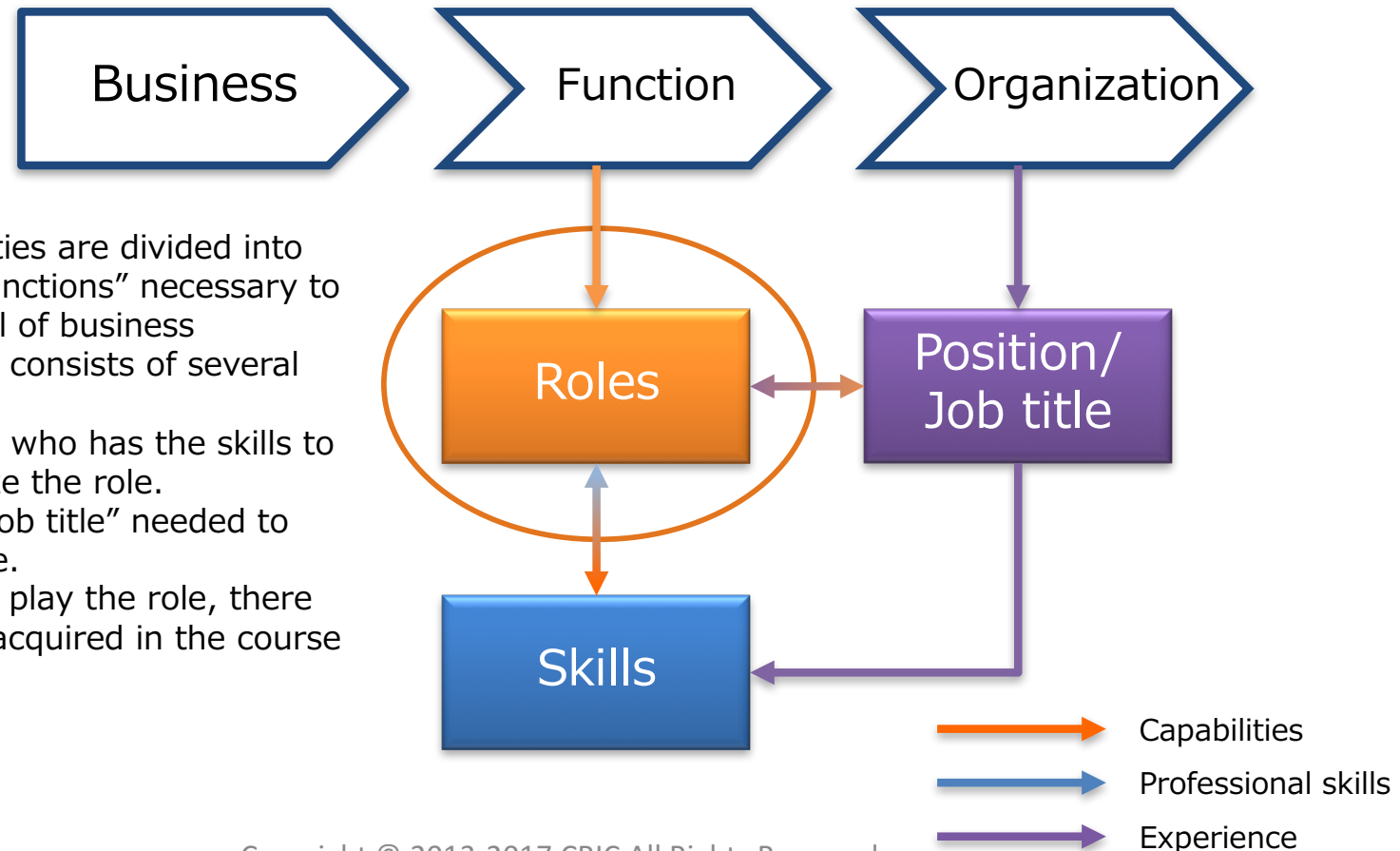
Balance between core business role and security role

**Security related roles** must be considered in conjunction with **the core business roles.**



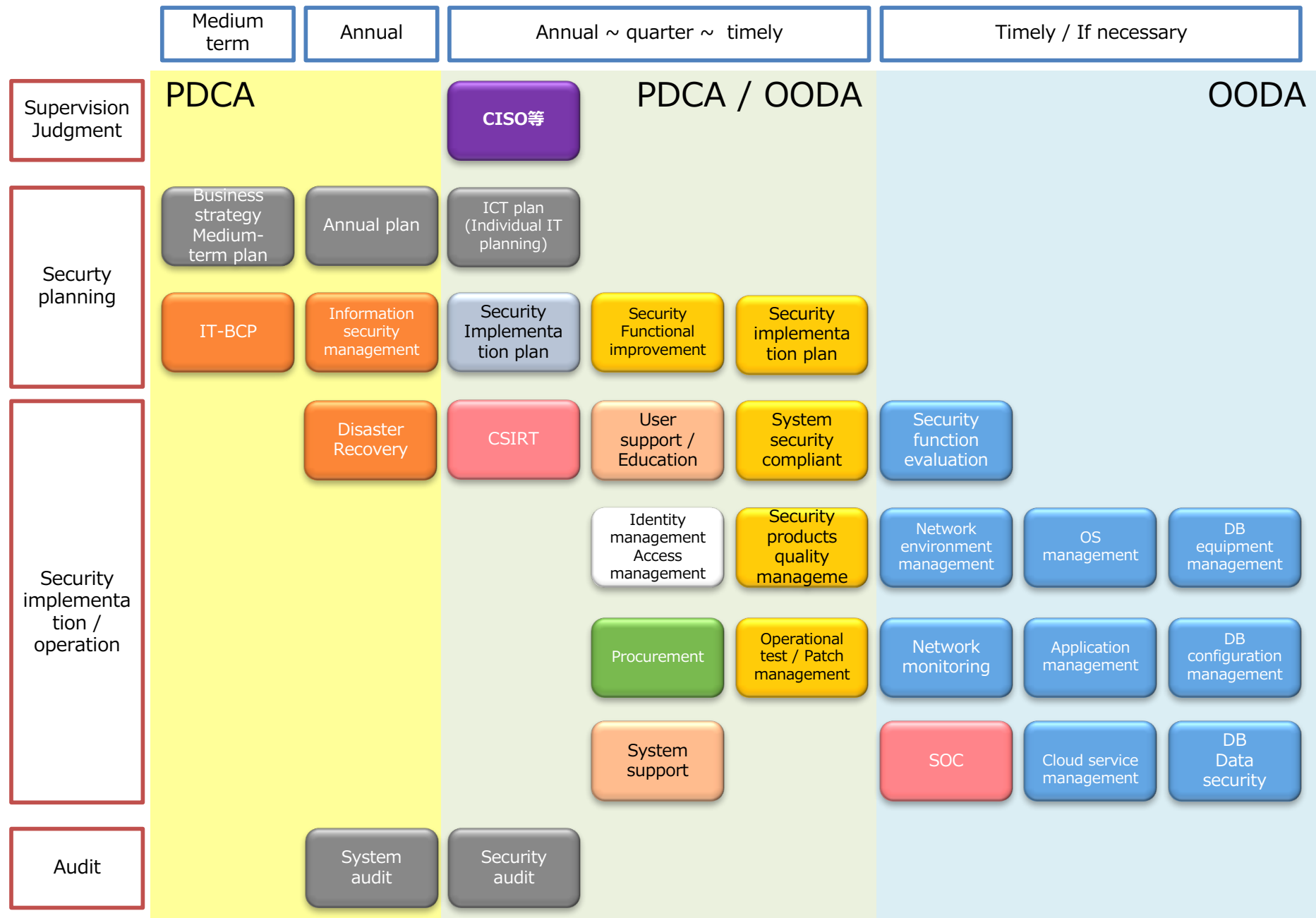
# Relationship between Organization and Workforce

- Security workforces of user companies are different from that of security vendors regarding its roles, career and capabilities.
- **Excellent workforce is the workforce that can fulfill the role.** Company have to provide the environment on which they can use their capability to play the role.
- In our approach, the relationship of “Roles”, “Position/Job title”, and “Skill” is below;



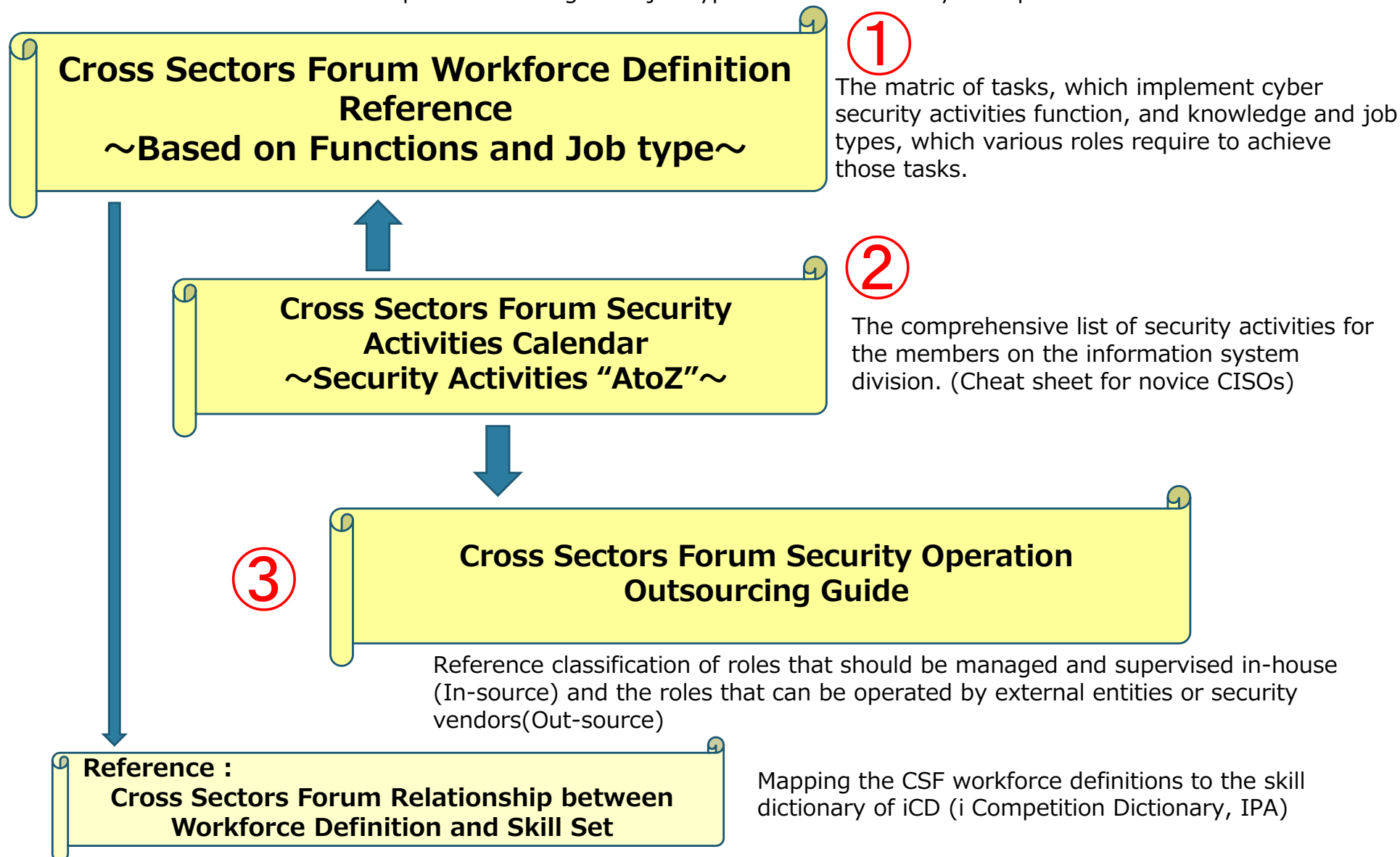
- Company activities are divided into some of the “Functions” necessary to achieve the goal of business
- Each “Function” consists of several “Roles”.
- Assign a person who has the skills to be able to realize the role.
- Give “Position/Job title” needed to perform the role.
- Require skills to play the role, there are skills to be acquired in the course to play the role.

# Function definition of cyber security measures



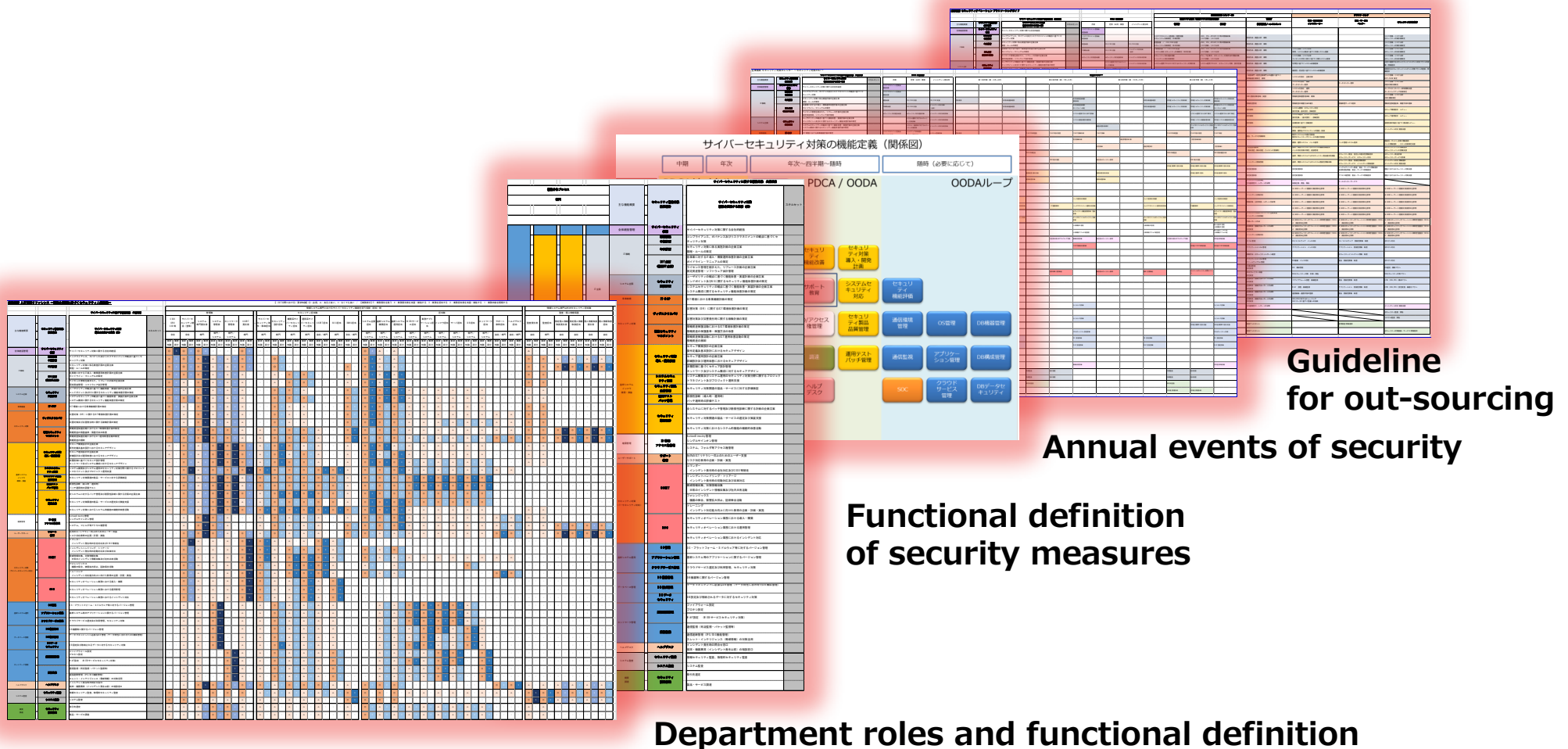
# Outputs of Cross Sectors Forum (1<sup>st</sup> period)

- The Scope of the 1<sup>st</sup> period is the information systems division in the Japanese user companies.
- Identify the required Cybersecurity related functions in the scope
- Define workforce with the required knowledge and job type that are necessary to implement those functions



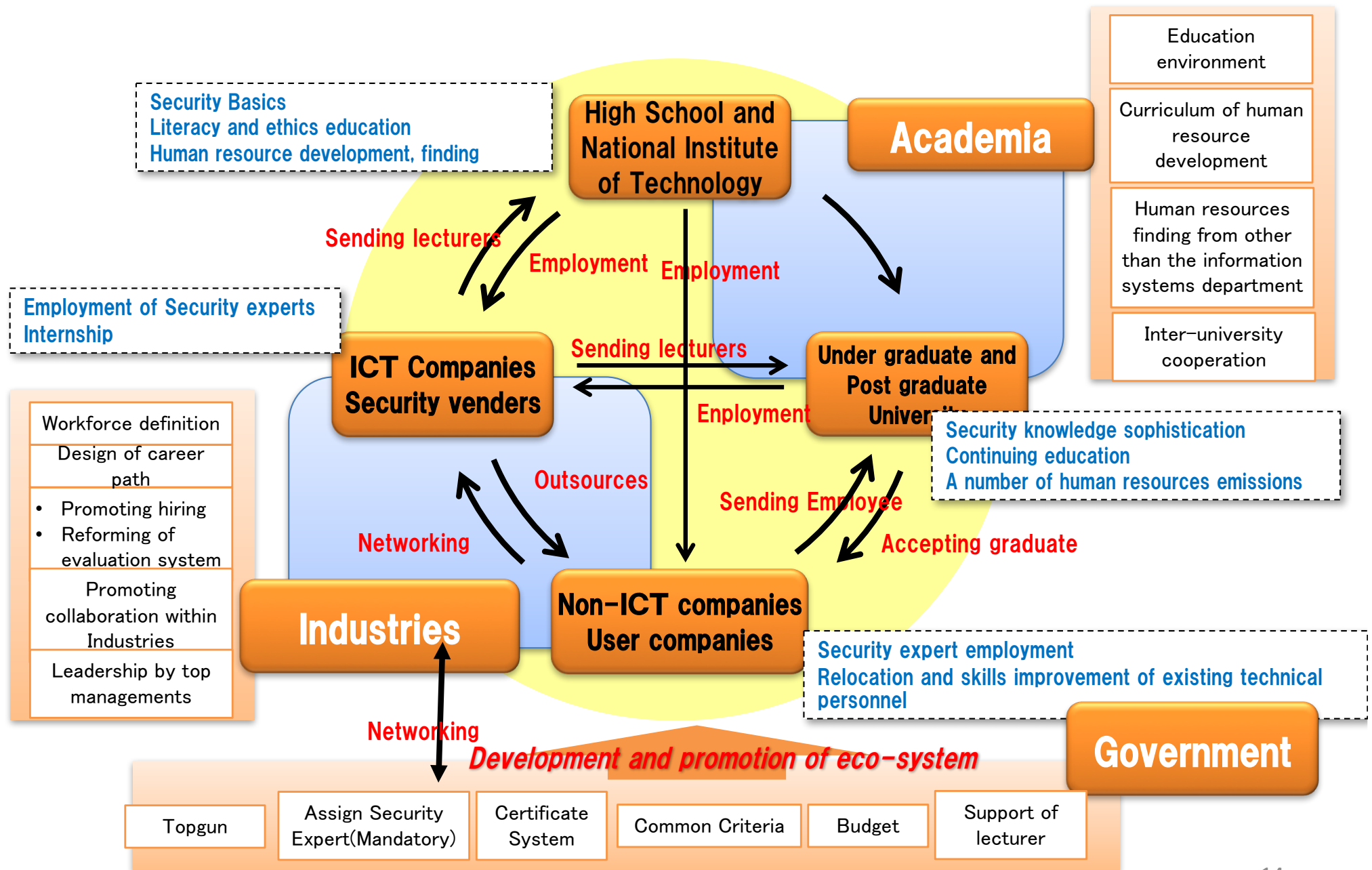
# Cross-sectors collaboration for Cybersecurity Workforce Development

- Cybersecurity workforce definition for Japanese companies.
- Sharing into industry organizations and government organizations.



References of workforce definition  
2017/10/11

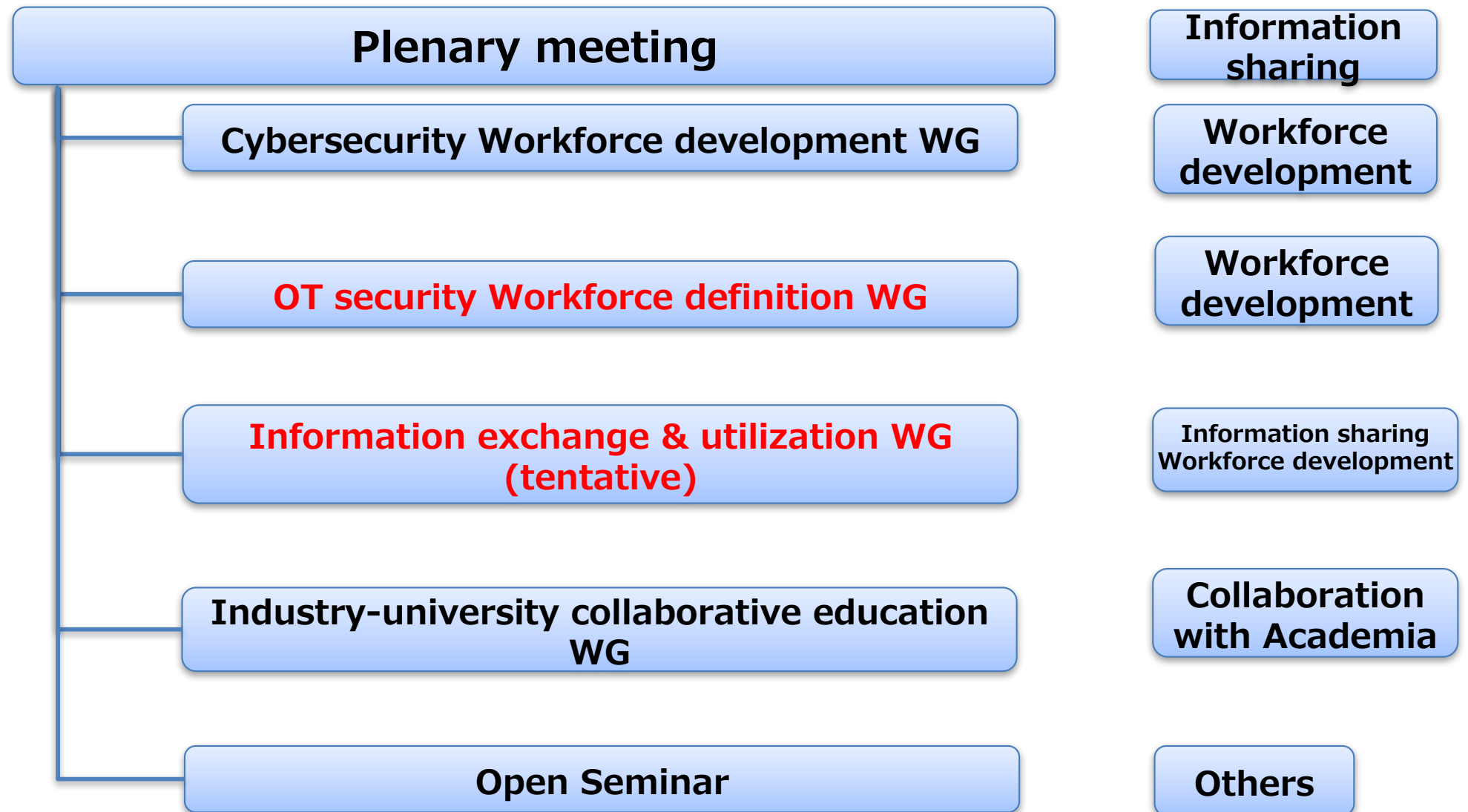
# Eco-System for Cyber Security Workforce Development



# New structure of WG in 2<sup>nd</sup> period

(October 2017 – September 2018)

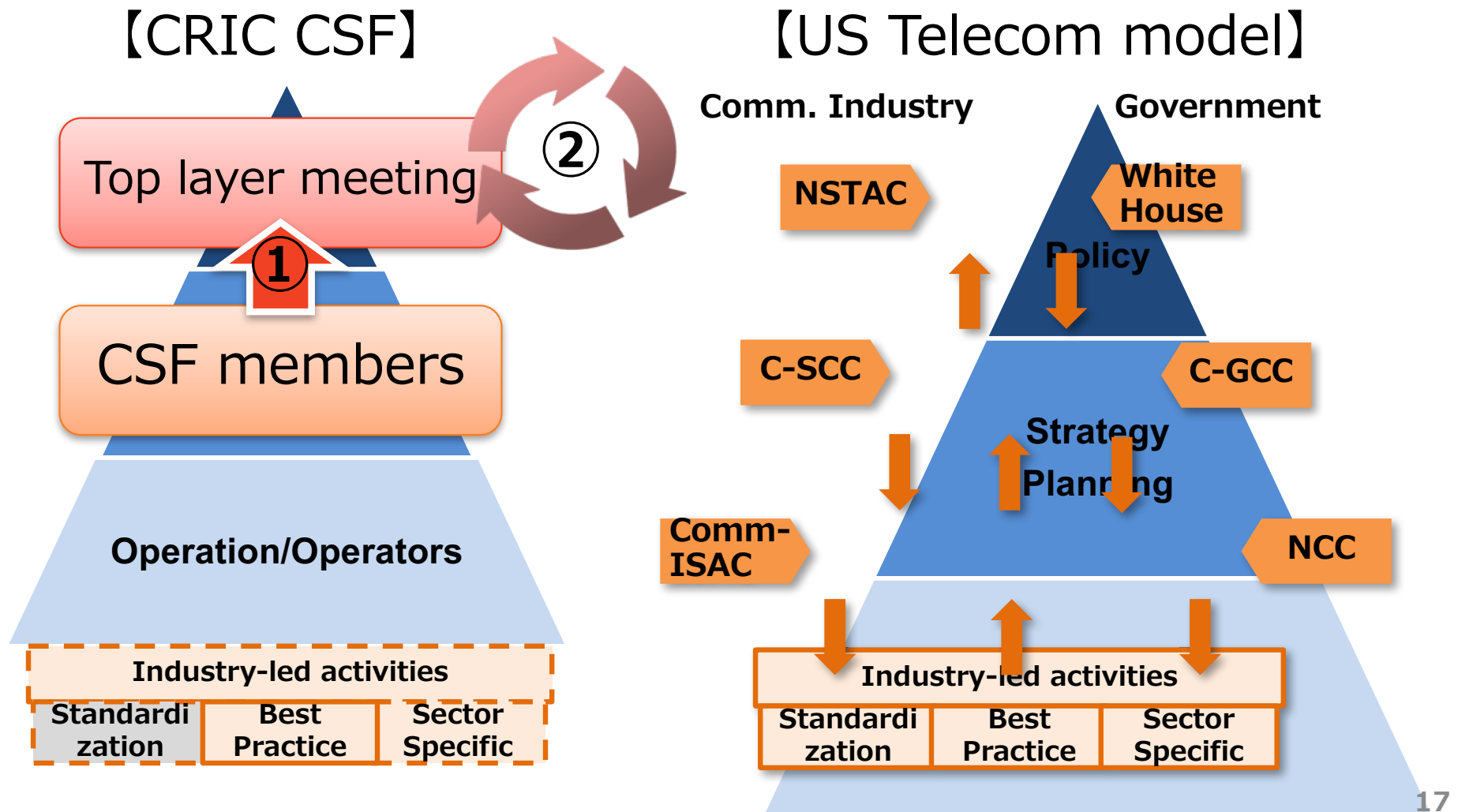
- 2017/4/1 Transition to a consortium with corporate status (established under the existing group "Cyber Risk Intelligence Center (CRIC)")



# **3. Top Layers Meeting**

# Background of the top tier meeting

- The involvement of the top tier and management person is essential.
- Reference the US telecommunications industry to strengthen collaboration across industries
  - ① Gain support from the management with the understanding of management
  - ② Establishment of Trusted Network in cross-industry management





# 1<sup>st</sup> TOP layer meeting

## Focus points

- ① Confirm the necessity of working across industries (cooperation beyond industries is necessary as a response to the IoT era when all are connected, etc.)
- ② Promotion of CSF initiatives (importance of building trust circle, etc.)
- ③ Understanding of management and leadership (Establishment of Trusted Network among cross-industry management)

### Cross-Sector Forum for Cybersecurity Workforce Development

#### Conference and Reception



Meeting report:  
Monday, October 17, 2016;  
Keidanren Kaikan,  
North & South Keidanren Halls

The Cross-Sector Forum for Cybersecurity Workforce Development (hereafter the Forum) was launched on June 9, 2015. Responding to the recommendations published by the Keidanren (the Japan Business Federation) on February 17, 2015, NTT, NEC and Hitachi suggested to major critical infrastructure providers for strengthening cybersecurity measures.

The conference and reception were an opportunity to recap what had been done in the past twelve months, look ahead to more proactive initiatives, share information that the managements of participating businesses had gathered, and make personal connections.

#### 1. Opening Remarks



Opening the conference, Hiromichi Shinohara (Senior Executive Vice President, Chief Technology Officer and Chief Information Security Officer of NTT Group), who had called for the forum, gave a welcome speech.

In his speech, with an eye to the Tokyo 2020 Olympics and Paralympics, he emphasized the following three issues in strengthening cybersecurity:

1. The importance of initiatives that cut across different industries (and in the age of the Internet of Things (IoT), the importance of cooperation that breaks through the walls between different industries).
2. The importance of building cross-industrial "circles of trust"
3. Awareness and leadership at management level and the development of cross-industrial circles of trust at management level



Showing the presentation slide listing the businesses participating in the Forum, he expressed gratitude to the 48 participants for their continuing efforts in the fifteen months since the Forum was launched.

#### 2. Activity Report



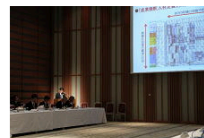
For the secretariat, Toru Kawamura of NTT Group reported on activities of the Forum. He mentioned three main points:

1. Industry-led respectful discussion with a bottom-up approach
2. Building cross-industrial circles of trust
3. Publishing findings that can be made available to government and academia

He expressed gratitude for the continuing cooperation of the participants.

He then explained spreadsheets related to the "Personnel Specification Reference", which is one of the products of the Forum, and made the following two requests to the executives in attendance:

1. To encourage the adoption and use of the tools, such as the "Personnel Specification Reference", as part of management processes, making use of them as advanced tools for evaluation of employment sufficiency and setting targets for, training and recruitment of staff
2. To endorse members' continuing participation to the new stage (the second phase) in October 2016



(Participants taking a look at the 1st phase outcome) References and tools ↓



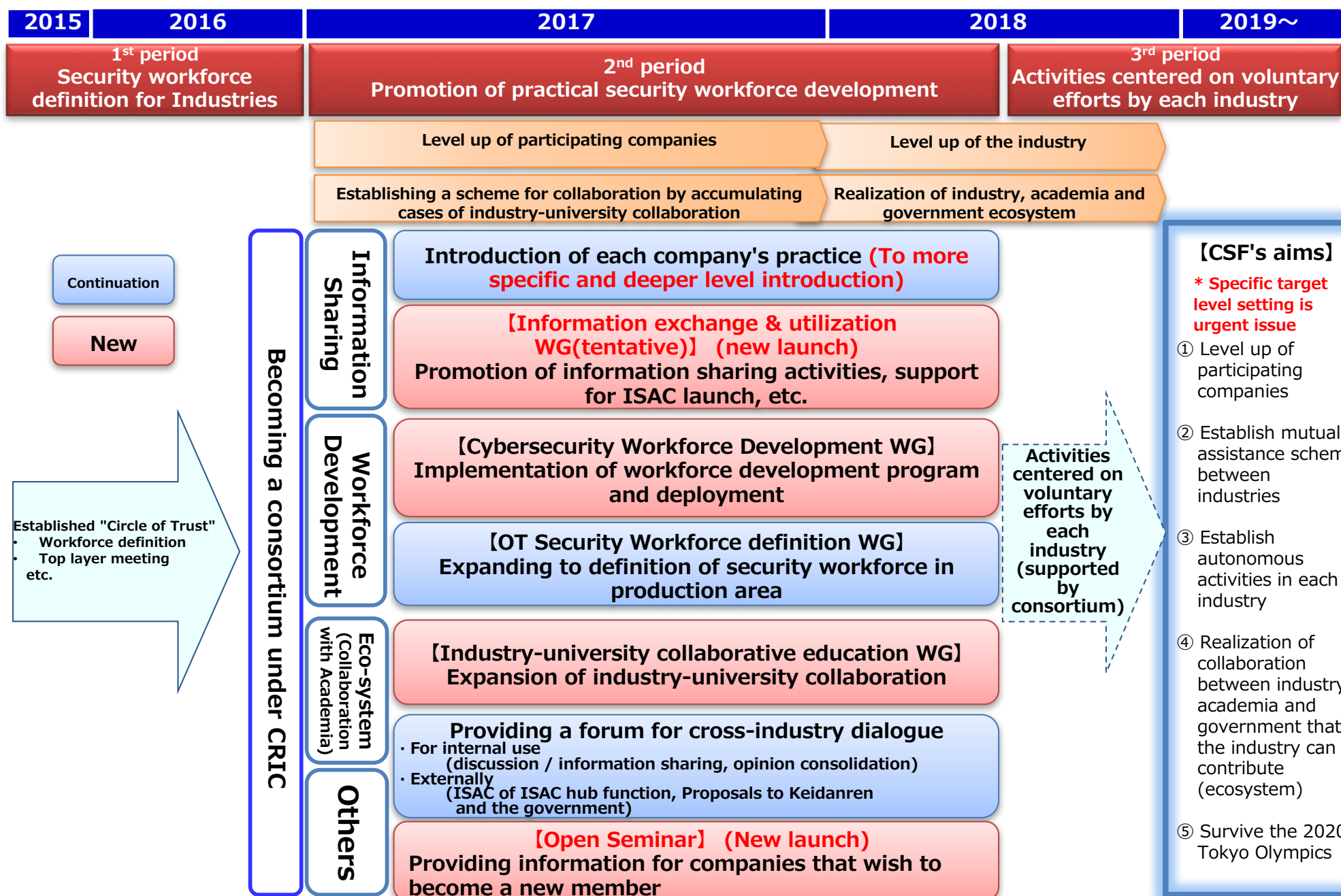
Top layer meeting scene

Publish a report to broadly share the summary of the meeting

[http://cyber-risk.or.jp/sansanren/conference\\_20161017\\_en.html](http://cyber-risk.or.jp/sansanren/conference_20161017_en.html)

## **4. Future work plan**

# Future Activities Plan



Thank you