

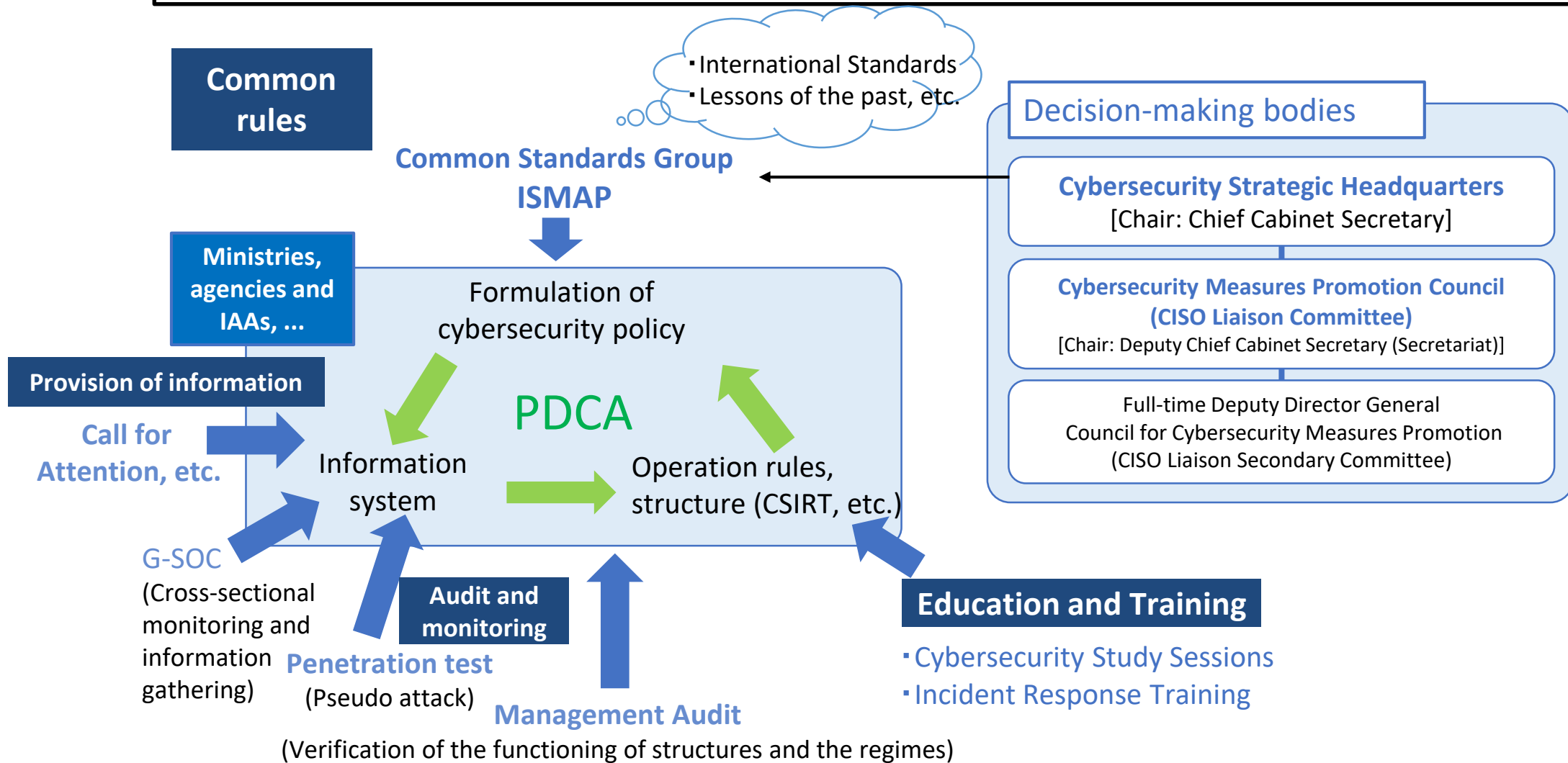


# Common Standards Group for Cybersecurity Measures for Government Agencies and Related Agencies (※)

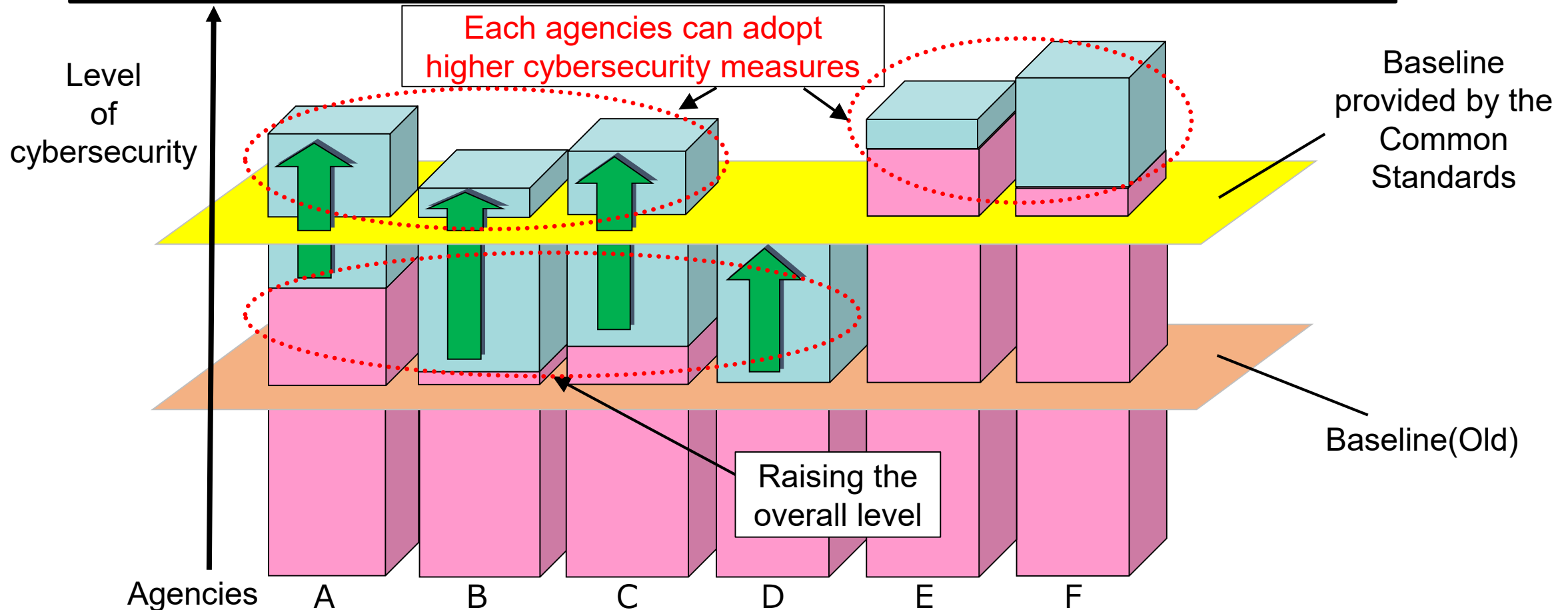
- (※) Common Standards Group includes:
- Common Model of Cybersecurity Measures for Government Agencies and Related Agencies
  - Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies
  - Guidelines for Formulating Measures Criteria for Government Agencies and Related Agencies

**National Center of Incident Readiness and Strategy for Cybersecurity (NISC)  
Cabinet Secretariat**

• At NISC, through the formulation of common rules (Common Standards), audit/ monitoring, education/ training, etc., the PDCA cycle of all government agencies, etc. is appropriately implemented to comprehensively strengthen cybersecurity measures.



- Common Standards are the unified framework for cybersecurity of government agencies and incorporated administrative agencies.
- It shows the baseline of cybersecurity of government agencies and related agencies, etc., and it is possible to take higher measures at the discretion of each organization.



- Government Common Standards are **an integrated framework to improve information security level of Government Agencies and Incorporated Administrative Agencies based on the Basic Act on Cybersecurity.**
- Government Common Standards define **a baseline for information security measures to be implemented by Government Agencies and Related Agencies.**
- Government Agencies and Incorporated Administrative Agencies **formulate information security policy for each organization in compliance with the Government Common Standards** considering characteristics of information handled by the organization. This is intended to ensure that a certain information security level in any Government Agencies and Related Agencies is maintained.

## The Basic Act on Cybersecurity (Act No. 104 of 2014) (Excerpt)

Act 26 Functions under Jurisdiction of the Headquarters  
(Omitted)

- (ii) **establishing the standards of cybersecurity measures for national administrative organs, incorporated administrative agencies and designated corporations**, and promoting the implementation of the evaluation (including audit) of measures based on the standards and other measures taken based on the standards

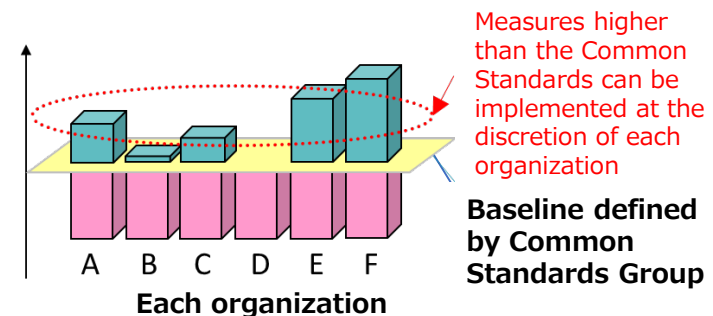
## Common Model of Cybersecurity Measures for Government Agencies and Related Agencies

(July 4, 2023 Headquarter Revision) (Excerpt)

Article 6 Agencies, etc. shall establish basic policies and standards for countermeasures based on the characteristics of their own organizations.  
(Omitted)

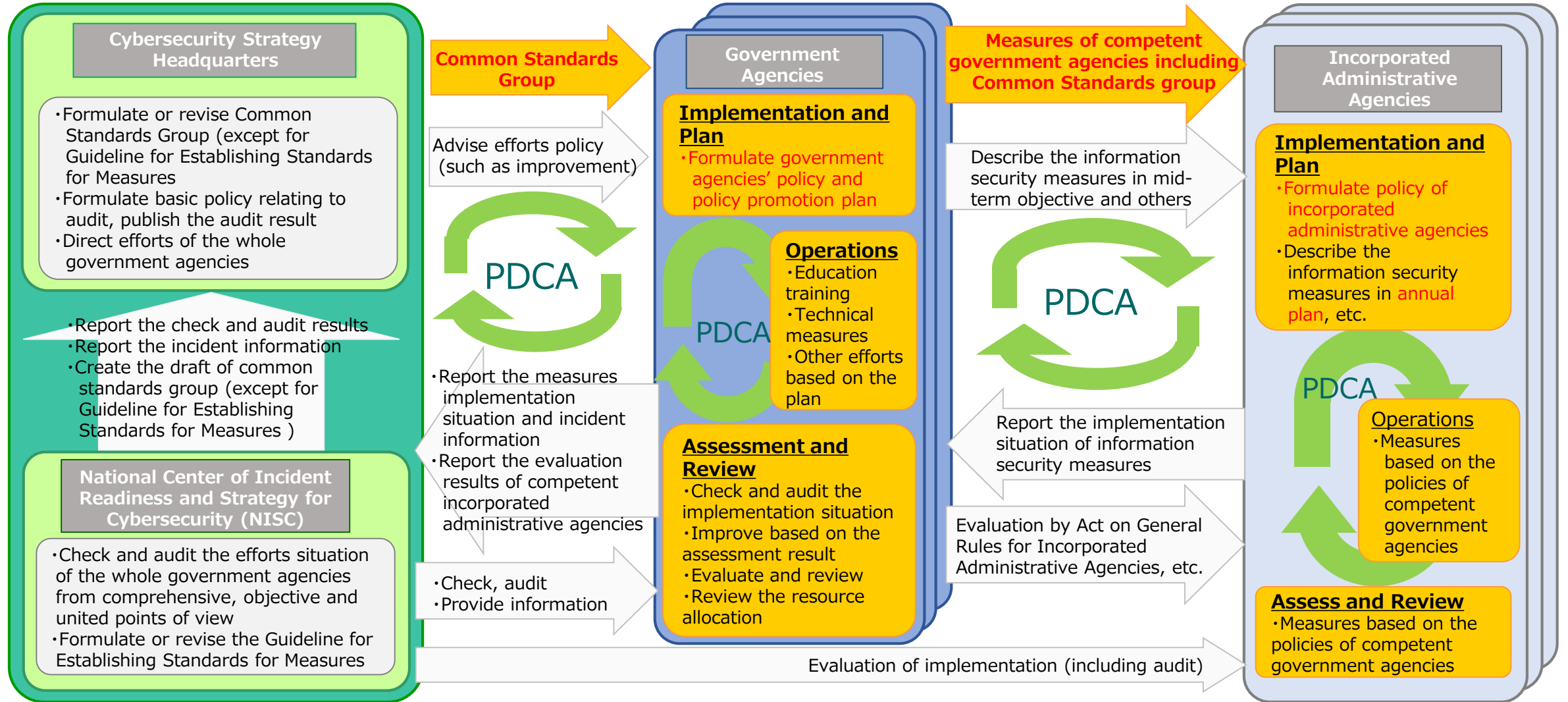
3 The countermeasure standards shall conform to the Common Standards and shall be stipulated to enable information security measures that are **the same as or higher than the Common Standards.**

Information security level



# PDCA cycle of the Government Agencies and Related Agencies as a whole

• Ensure the information security of Government Agencies and Related Agencies as a whole by appropriately implementing the PDCA cycle of individual organizations and the PDCA cycle of the Government Agencies and Related Agencies as a whole through the operation of Common Standards Group.



# Background of the Revision

- Government Common Standards Group (※) is **an integrated framework to improve information security level of Government Agencies and Incorporated Administrative Agencies** based on the Basic Act on Cybersecurity. (※) It consist of Common Model, Common Standards and Guideline.
- The review of Government Common Standards Group is based on the recent situation and includes strengthening of **measures for subcontractors and software** in consideration of increasing risks of cyber attack for supply chain and strengthening of measures of servers redundancy in consideration of increasing use of cloud services and the characteristics of latest DDoS attacks.

## Clarification of measures for subcontractors (e.g. outsourced maintenance of information systems)

➔ Revision Point 「1. Strengthening of information security measures for supply chain」

- The event of leakage of information of Government Agencies contracted out to a subcontractor occurred. The risks of cyber-attack that exploits vulnerabilities of supply chain have increased with the complication of supply chain.

## Clarification of information security measures when using cloud services

➔ Revision Point 「2. Strengthening of measures in consideration of increasing use of cloud services」

- Use of cloud services by Government Agencies has increased. Strengthening of security is required through a series of processes of procurement, development, operation and disposal. The measures for secure use of the cloud services such as SNS need to be validated.

## Strengthening of information security measures when using software

➔ Revision Point 「3. Strengthening of information security measures when using software」

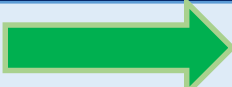
- Cyber-attacks targeting software are getting more complicated and sophisticated. Such attacks exploit improper configuration of software and the update of the proper network monitoring software. Because security measures when using software are strengthened by Government Agencies in US, they also need to be strengthened in Japan.

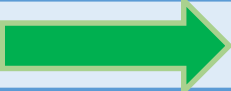
## Strengthening of measures in consideration of threats and technology trends

➔ Revision Point 「4. Strengthening of cyber resilience and measures in consideration of threats and technology trends」

- Facing increasing DDoS attacks that may lead to the malfunction of web sites, the security measures for such attacks need to be strengthened. Facing increasing Ransomware attacks, the security measures related to information systems protection, recovery and backup need to be strengthened for Government Agencies.

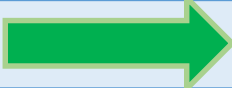
# Point of the Revision①

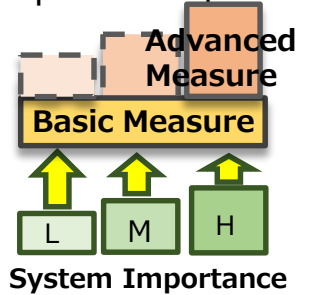
	Current (2021 Edition)	 <b>Point of the Revision</b>
<b>1. Strengthening of information security measures for supply chain</b>	<ul style="list-style-type: none"> <li>○ General information security controls for subcontractors are stipulated.</li> </ul>	<ul style="list-style-type: none"> <li>➤ To protect government information when subcontracting tasks, <b><u>security measures (※) for subcontractors such as access controls, log management and monitoring, referring to NIST supply chain controls,</u></b> are included in the contract and their implementation is required throughout the consignment period.            (※) The following eight types of security measures are stipulated referring to NIST SP800-171            ①Establishment and maintenance of incident response capabilities, ②Entity authentication and access control, ③Acquisition and monitoring of logs, ④Physical protection of equipment, etc, ⑤Notification and control of personnel, ⑥Asset management·risk evaluation, ⑦Protection of system integrity, ⑧Verification, evaluation , and review of security measures</li> </ul>
<b>2. Strengthening of measures in consideration of increasing use of cloud services</b>	<ul style="list-style-type: none"> <li>○ The cloud services for handling confidential information are selected from the ISMAP cloud services list.</li> <li>○ The cloud services not for handling confidential information are evaluated considering the risks of using it.</li> </ul>	<ul style="list-style-type: none"> <li>➤ As ISMAP is expanded to Incorporated Administrative Agencies and the operation of ISMAP-LIU starts, it is clearly stated that <b><u>the cloud services for handling confidential information are selected from the ISMAP cloud service list.</u></b>            (in the exceptional case that cloud services are selected not from ISMAP cloud services list, for example, because cloud services in the list do not have the required functions, it is necessary for CISO to ensure that the selected cloud services meet the requirements and controls of ISMAP.)</li> <li>➤ Even for the cloud services for not handling confidential information, <b><u>appropriate measures to use cloud services securely such as entity authentication and access control are implemented.</u></b> For the use of cloud services without procurement, an advice about measures is sought from NISC based on an agreement on use of external service without procurement.</li> </ul>

	Current (2021 Edition)	 <b>Point of the Revision</b>
<b>3. Strengthening of information security measures when using software</b>	<ul style="list-style-type: none"> <li>○ Software and equipment are procured according to IT procurement arrangement.</li> <li>○ Measures against software vulnerabilities are regularly implemented at the start of the operation and during the operation</li> </ul>	<ul style="list-style-type: none"> <li>➤ Clearly stated as essential to respond based on IT procurement arrangement for equipment procurement. Regarding critical software (※), security measures to ensure information security level during operation such as maintenance of configuration procedures, training, and regular check of configuration are implemented. (※) the software with critical security functions to control information systems such as control of terminals and servers, integrated entity authentication management, asset management, and network monitoring</li> <li>➤ Software vulnerabilities management such as vulnerabilities assessment is strengthened at the start of operation of servers and terminals.</li> </ul>
<b>4. Strengthening of cyber resilience and measures in consideration of threats and technology trends</b>	<ul style="list-style-type: none"> <li>○ According to characteristics of information systems, the implementation of multi-factor authentications, monitoring function, backup and recovery training are evaluated.</li> <li>○ Enabling the functions to deal with DDoS attacks is implemented.</li> </ul>	<ul style="list-style-type: none"> <li>➤ With cyber attack in mind, <b><u>security measures to protect and recover information systems</u></b> are implemented. (monitoring of information systems, the implementation of multi-factor authentications in the case that advanced entity authentications is required for administrator authority of cloud service, preparing recovery procedures, appropriate backup, review of backup requirements and recovery procedures, prepared for information security incidents)</li> <li>➤ In consideration of the latest DDoS attacks, <b><u>the dedicated devices and service to treat them are implemented and servers, communication lines are redundant</u></b>, and <b><u>formulation of monitoring policy and collection of threat information</u></b> are conducted.</li> <li>➤ To respond to increasing use of cloud services with the implementation of zero-trust architecture in mind, <b><u>continuous assessment and verification of access to information assets and new technical methods to permit and deny access according to trust</u></b> are stipulated.</li> </ul>



# Point of the Revision③

	Current (2021 Edition)	 <b>Point of the Revision</b>
<b>5. Strengthening of cross-organizational security measures and securing measures according to the importance of information systems</b>	<ul style="list-style-type: none"> <li>○ The result of information security review is reported to CISO. (The regular progress report is not stipulated)</li> <li>○ Security measures for Incorporated Administrative Agencies are implemented at their judgement.</li> <li>○ Security measures for the information systems are defined at judgement of Government Agencies and may differ in its degree.</li> </ul>	<ul style="list-style-type: none"> <li>➤ Regarding <b>cross-organizational</b> improvements identified by audit, <b>CISO receives progress reports regularly</b>, monitors the progress of improvements based on the result of audit and controls the entire organization.</li> <li>➤ To support information security measures of Incorporated Administrative Agencies, <b>the required system is prepared for the Government Agencies</b>. The Incorporated Administrative Agencies <b>seek advices from the Government Agencies</b> about the items that require specific expertise.</li> <li>➤ <b>The concept of “classification of information system” is introduced. Advanced measures such as real time log analysis is required for the information systems that are more critical than core business systems</b> in addition to basic measures for all information systems.</li> </ul>



- The Basic Act on Cybersecurity (Act No. 104 of 2014) Based on Article 26 Item 1.2, Standards for cybersecurity for national administrative organizations was formulated. They have been revised every two years to steadily evolve the foundation of the required security measures considering trends in cybersecurity.

## Establishment of Cybersecurity Strategic Headquarters·National Center of Incident Readiness and Strategy for Cybersecurity (NISC)

(January 2015)

### 2016 Edition (31 August 2016 Cybersecurity Strategic Headquarters Decision)

- Incorporated Administrative Agencies and Designated Corporations were added to the scope in addition to Government Agencies.
- The policy focused on strengthening of information security management was added so that information security measures can be implemented appropriately in Incorporated Administrative Agencies.
- Considering occurrences of information security and trends in cyber-attack, the policy related to advance preparation such as a formulation of CSIRT, strengthening of protection of information systems assuming Advanced Persistent Threat by malware infection was added.

### 2018 Edition (25 July 2018 Cybersecurity Strategic Headquarters Decision )

- User-oriented measures was added to allow nation to use government services securely through web sites so on.
- The policy related to effective operation of PDCA cycle for the autonomous capacity building of government agencies was prepared.
- The policy that allows the mobile devices with certain security measures to access network to conduct operation was added.

### 2021 Edition (7 July 2021 Cybersecurity Strategic Headquarters Decision )

- Considering the controls standard of ISMAP, the description of the measures and approaches to be implemented by cloud service users were added.
- Considering major cyber attacks, latest information security cases and security measures, the advanced security measures such as CDN and EDR were described.
  - ※ 1 : CDN (Contents Delivery Network)
  - ※ 2 : EDR (Endpoint Detection and Response)
- Regarding the information security measures for diverse work styles, a criteria for the measures to be implemented by Government Agencies was clarified.

Thank you for your attention.



Know, Protect and Continue  
<https://www.nisc.go.jp/>