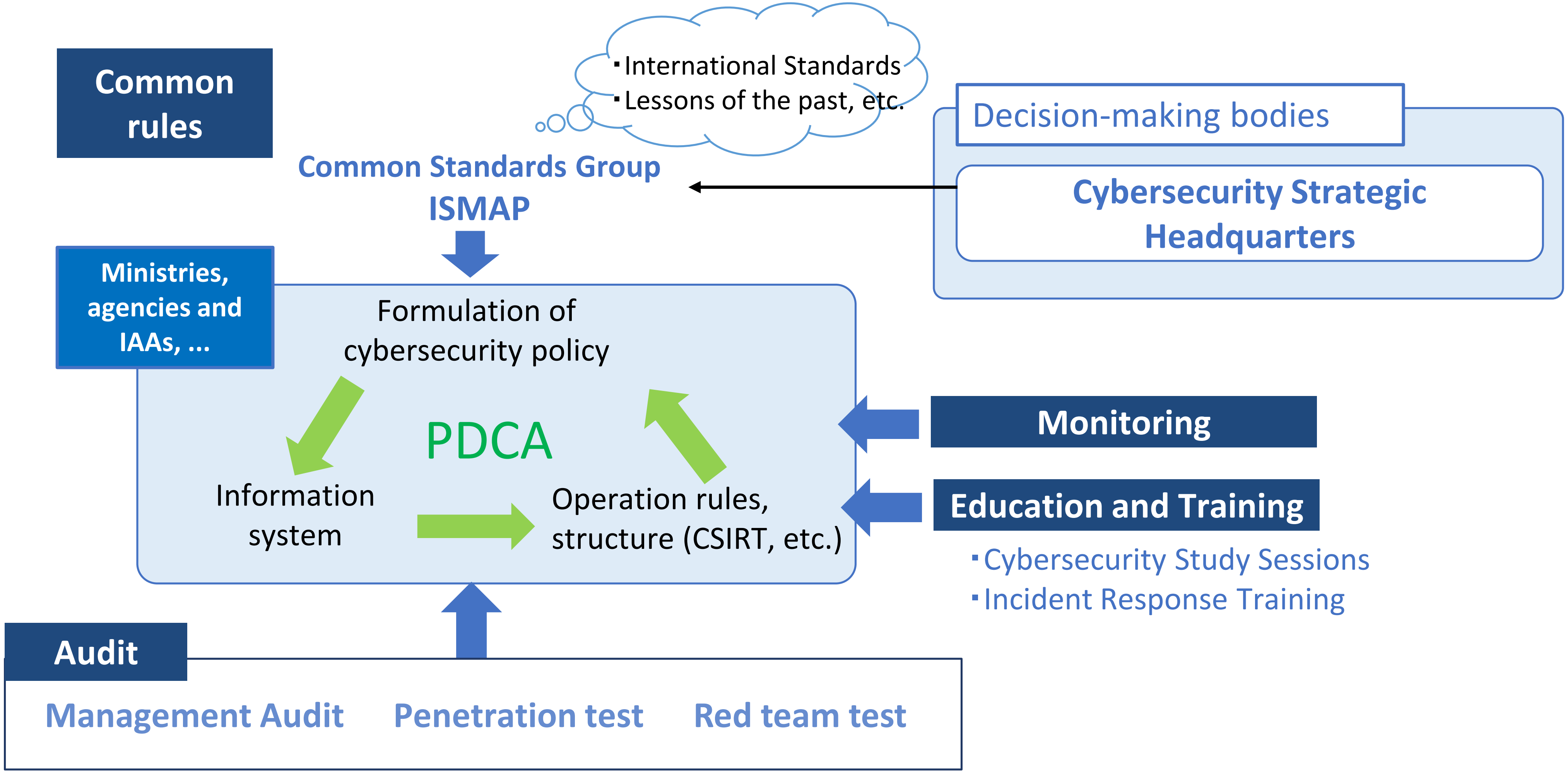
Common Standards Group for Cybersecurity Measures for Government Agencies and Related Agencies

National Cybersecurity Office（NCO)

Cabinet Secretariat

Common Cybersecurity Measures for All Government Agencies

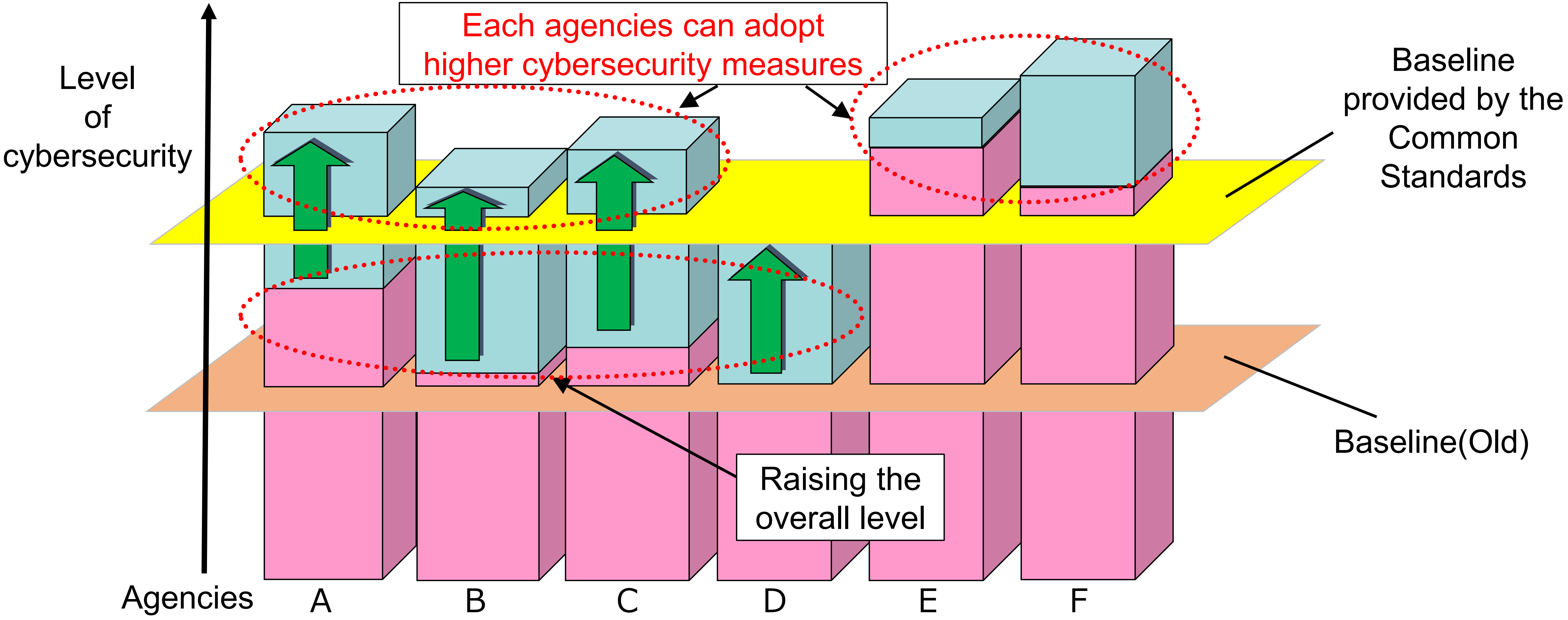
- At NCO, through the formulation of common rules (Common Standards), audit/ monitoring, education/ training, etc., the PDCA cycle of all government agencies, etc. is appropriately implemented to comprehensively strengthen cybersecurity measures.



Common rules
・International Standards
・Lessons of the past, etc.
Common Standards Group
ISMAP
Decision-making bodies
Cybersecurity Strategic Headquarters
Ministries, agencies and IAAs, ...
Formulation of cybersecurity policy
PDCA
Information system
Operation rules, structure (CSIRT, etc.)
Monitoring
Education and Training
・Cybersecurity Study Sessions
・Incident Response Training
Audit
Management Audit
Penetration test
Red team test

Role of Common Standards for 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.



Each agencies can adopt higher cybersecurity measures
Level of cybersecurity
Baseline provided by the Common Standards
Baseline(Old)
Raising the overall level
Agencies
A
B
C
D
E
F

What are Common Standards for Cybersecurity Measures?

- 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

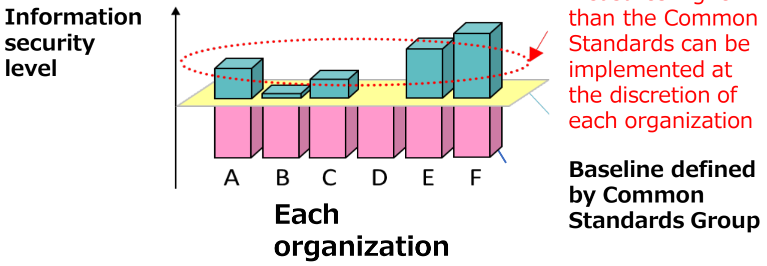
Common Model of Cybersecurity Measures for Government Agencies and Related Agencies

（June 27, 2025 Headquarter Revision）(Excerpt)

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

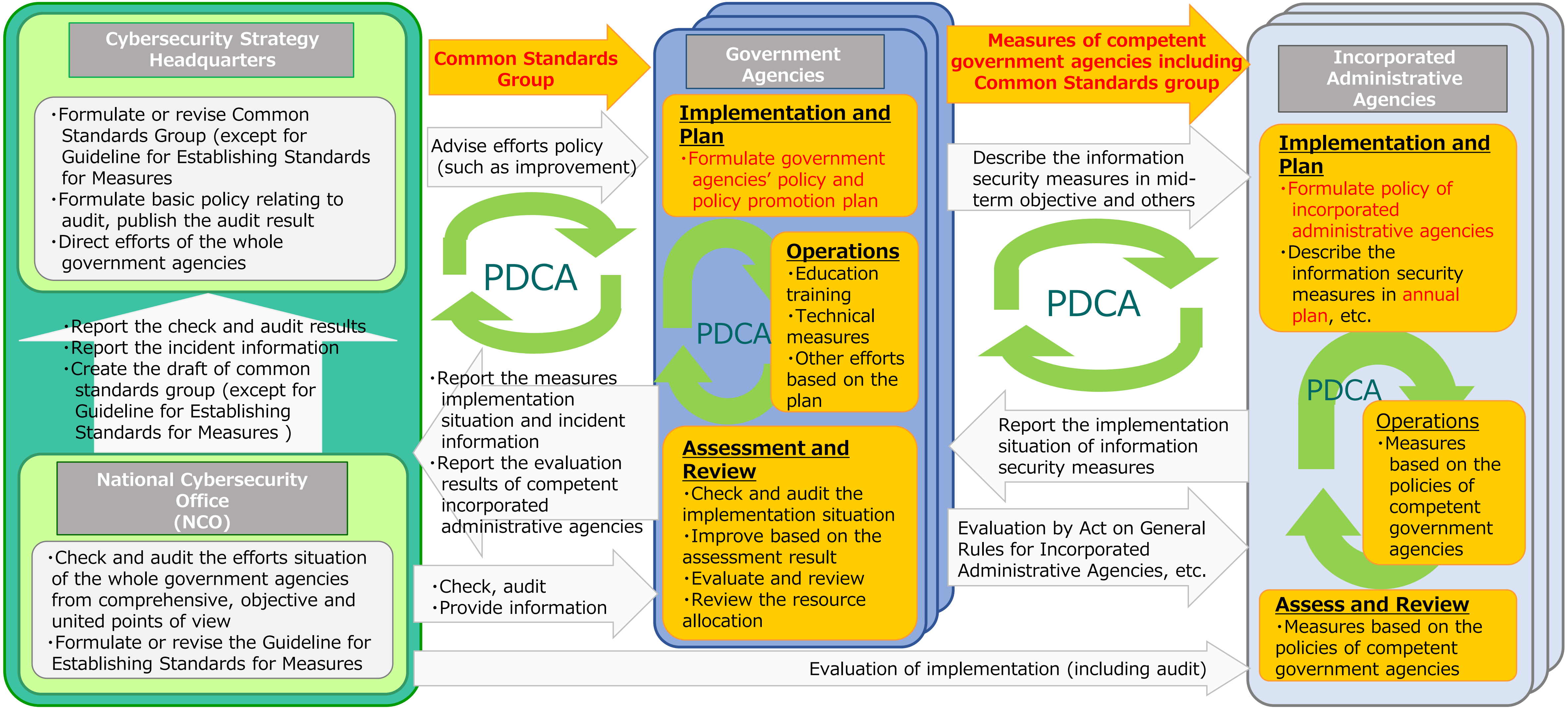
(Omitted)

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
A
B
C
D
E
F
Each organization
Measures higher than the Common Standards can be implemented at the discretion of each organization
Baseline defined by Common Standards Group

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.



Cybersecurity Strategy Headquarters

・Formulate or revise Common Standards Group (except for Guideline for Establishing Standards for Measures
・Formulate basic policy relating to audit, publish the audit result
・Direct efforts of the whole government agencies

・Report the check and audit results
・Report the incident information
・Create the draft of common standards group (except for Guideline for Establishing Standards for Measures)

National Cybersecurity Office (NCO)

・Check and audit the efforts situation of the whole government agencies from comprehensive, objective and united points of view
・Formulate or revise the Guideline for Establishing Standards for Measures

Common Standards Group

Advise efforts policy (such as improvement)

・Report the measures implementation situation and incident information
・Report the evaluation results of competent incorporated administrative agencies

・Check, audit
・Provide information

Government Agencies

Implementation and Plan
・Formulate government agencies' policy and policy promotion plan

Operations
・Education training
・Technical measures
・Other efforts based on the plan

Assessment and Review
・Check and audit the implementation situation
・Improve based on the assessment result
・Evaluate and review
・Review the resource allocation

Measures of competent government agencies including Common Standards group

Describe the information security measures in mid-term objective and others

Report the implementation situation of information security measures

Evaluation by Act on General Rules for Incorporated Administrative Agencies, etc.

Evaluation of implementation (including audit)

Incorporated Administrative Agencies

Implementation and Plan
・Formulate policy of incorporated administrative agencies
・Describe the information security measures in annual plan, etc.

Operations
・Measures based on the policies of competent government agencies

Assess and Review
・Measures based on the policies of competent government agencies

History of Revisions of Common Standards for Cybersecurity Measures

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 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.
- Regarding the information security measures for diverse work styles, a criteria for the measures to be implemented by Government Agencies was clarified.

※1 : CDN（Contents Delivery Network)
※2 : EDR（Endpoint Detection and Response)

History of Revisions of Common Standards for Cybersecurity Measures

National Cybersecurity Office

2025 Edition (4 July 2023 Cybersecurity Strategic Headquarters Decision)

- Strengthening of information security measures for supply chain. To protect government information when subcontracting tasks, security measures for subcontractors such as access controls, log management and monitoring, referring to NIST supply chain controls, are included in the contract and their implementation is required throughout the consignment period.
- As ISMAP is expanded to Incorporated Administrative Agencies and the operation of ISMAP-LIU starts, it is clearly stated that the cloud services for handling confidential information are selected from the ISMAP cloud service list. Even for the cloud services for not handling confidential information, appropriate measures to use cloud services securely such as entity authentication and access control are implemented.
- Clearly stated as essential to respond based on IT procurement arrangement for equipment procurement.
- Strengthening of cyber resilience and measures in consideration of threats and technology trends. With cyber attack in mind, security measures to protect and recover information systems are implemented.
- 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 in addition to basic measures for all information systems.

Reorganization of the National Center of Incident Readiness and Strategy for Cybersecurity into the National Cybersecurity Office（NCO）

(July 2025)

2027 Edition（27 June 2025 Cybersecurity Strategic Headquarters Decision)

- Revisions made in conjunction with the reorganization of the National Center of Incident Readiness and Strategy for Cybersecurity into the National Cybersecurity Office (NCO).