Outline of the Standards for Information Security Measures for the Central Government Computer Systems

National Information Security Center (NISC)

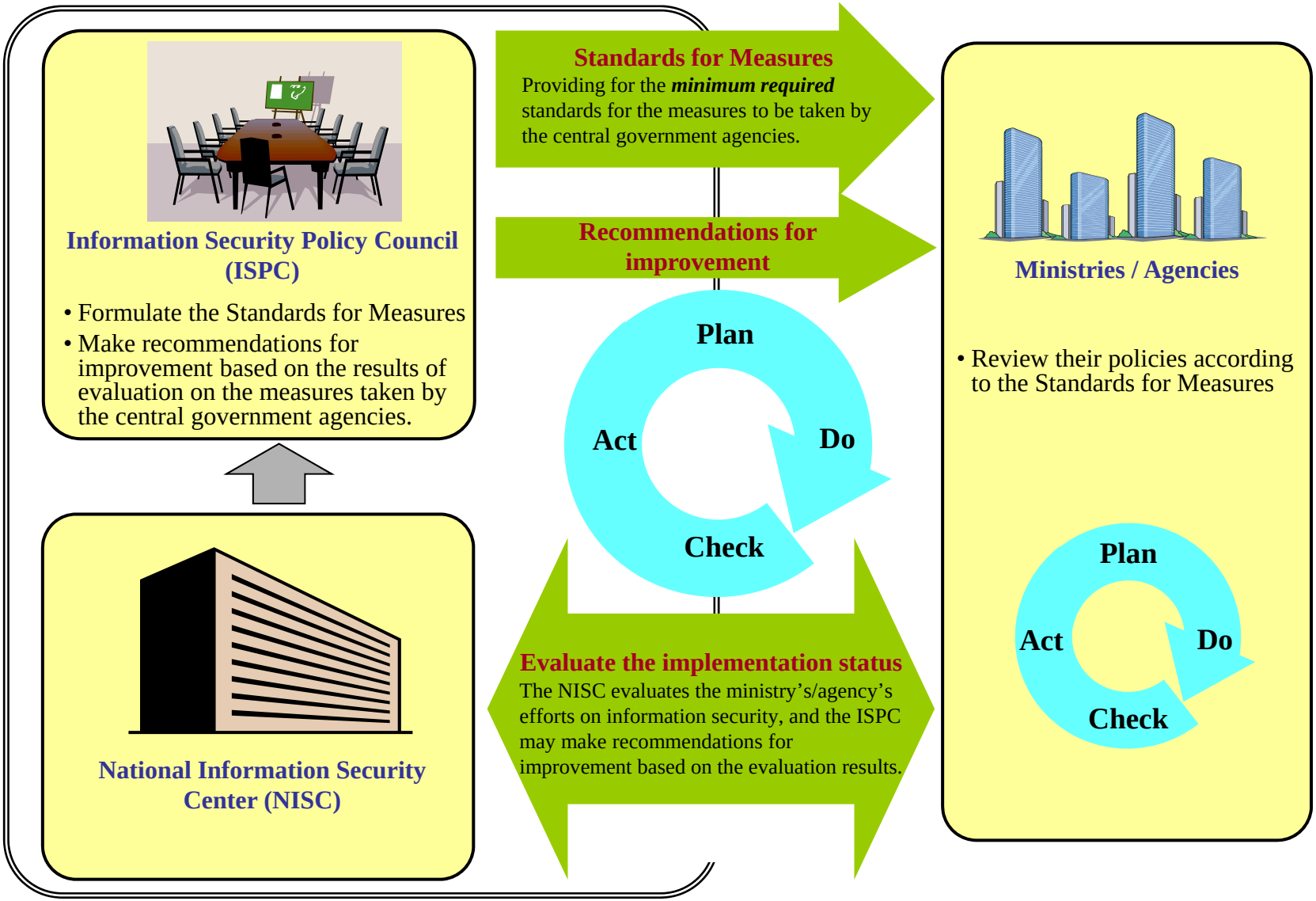
http://www.nisc.go.jp/eng/

“Standards for Information Security Measures for the Central Government Computer Systems”

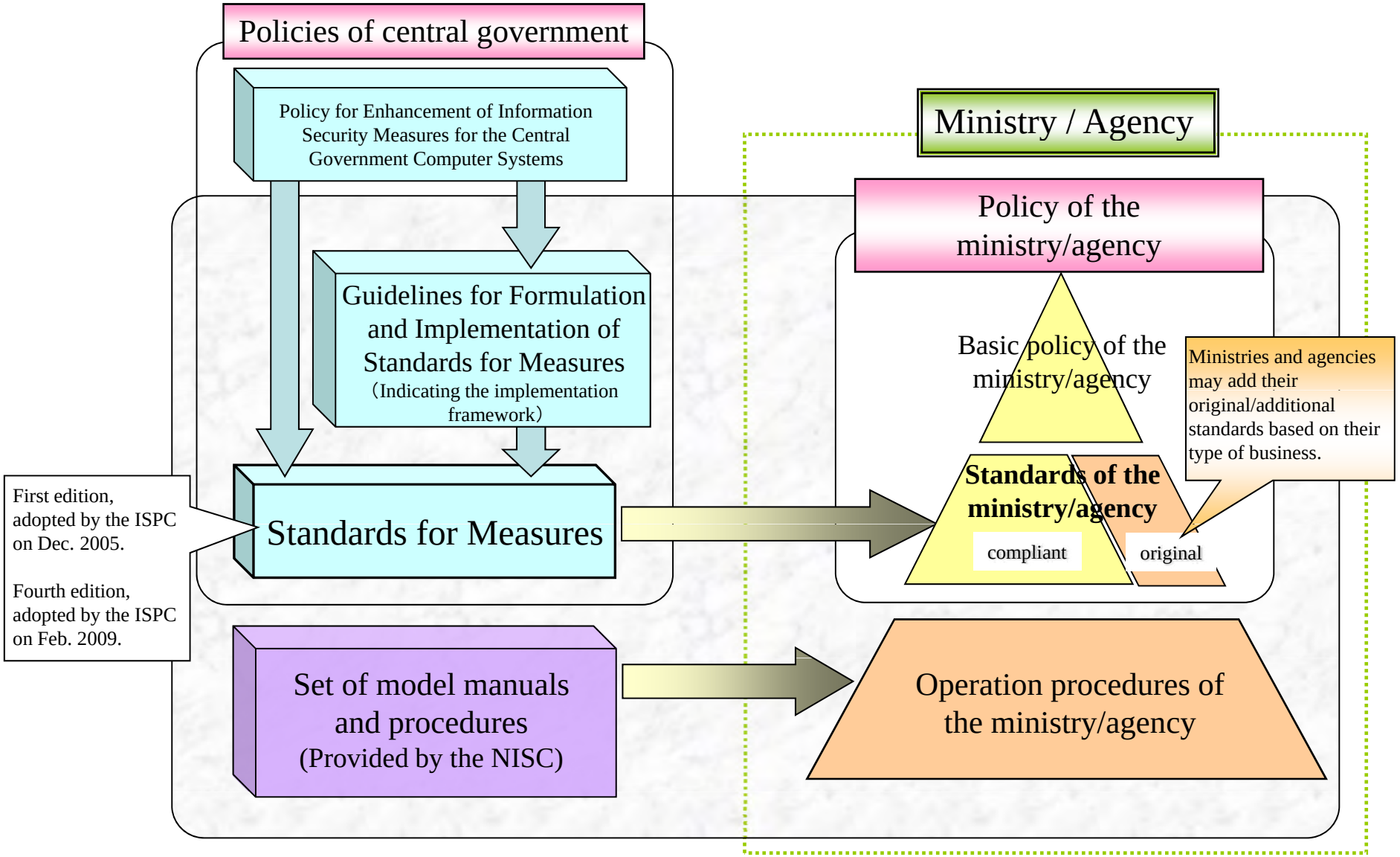
- ✓ To raise the information security level of the whole government, the Information Security Policy Council (ISPC) formulated the **“Standards for Information Security Measures for the Central Government Computer Systems” (Standards for Measures).** (Dec. 2005)
- ✓ Each ministry/agency formulates **its information security policy and standards**, which complies with the Standards for Measures, and **the NISC evaluates the level of the ministry’s /agency’s efforts on information security**.
- ✓ **The ISPC may make recommendations for improvement** based on the results of the evaluation.

Improvement effort is performed based on PDCA cycle.

Improvement based on PDCA cycle



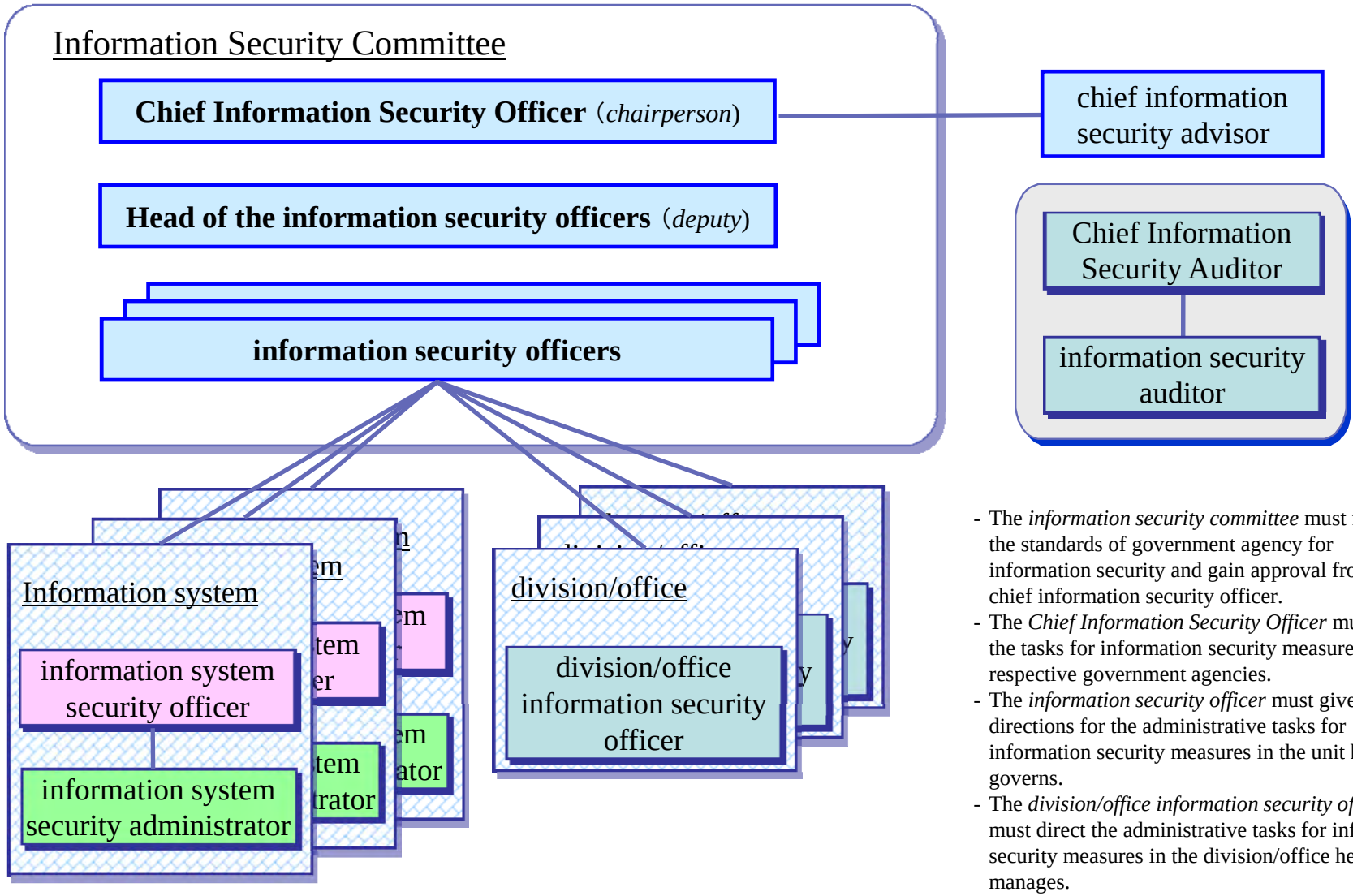
Framework of Information Security Measures of the Government



Contents of Standards for Measures

Table of Contents

Concept of the Organization and System of a ministry/agency



- The *information security committee* must formulate the standards of government agency for information security and gain approval from the chief information security officer.
- The *Chief Information Security Officer* must direct the tasks for information security measures in the respective government agencies.
- The *information security officer* must give directions for the administrative tasks for information security measures in the unit he or she governs.
- The *division/office information security officer* must direct the administrative tasks for information security measures in the division/office he or she manages.

Information classification in Standards for Measures

CONFIDENTIALITY

CLASSIFICATION	CLASSIFICATION STANDARD	MARKING
Confidentiality Class-3	The information that is handled in the tasks of the government agency and requires as much confidentiality as "confidential documents."	(example) *do not copy* *do not re-distribute* *encryption required*
Confidentiality Class-2	The information that is handled in the tasks of the government agency and does not require so much confidentiality as confidential documents but the leakage thereof can infringe citizens' rights or hinder the operation of tasks of the government agency.	
Confidentiality Class-1	The information that is not confidentiality class-2 information or confidentiality class-3 information.	

INTEGRITY

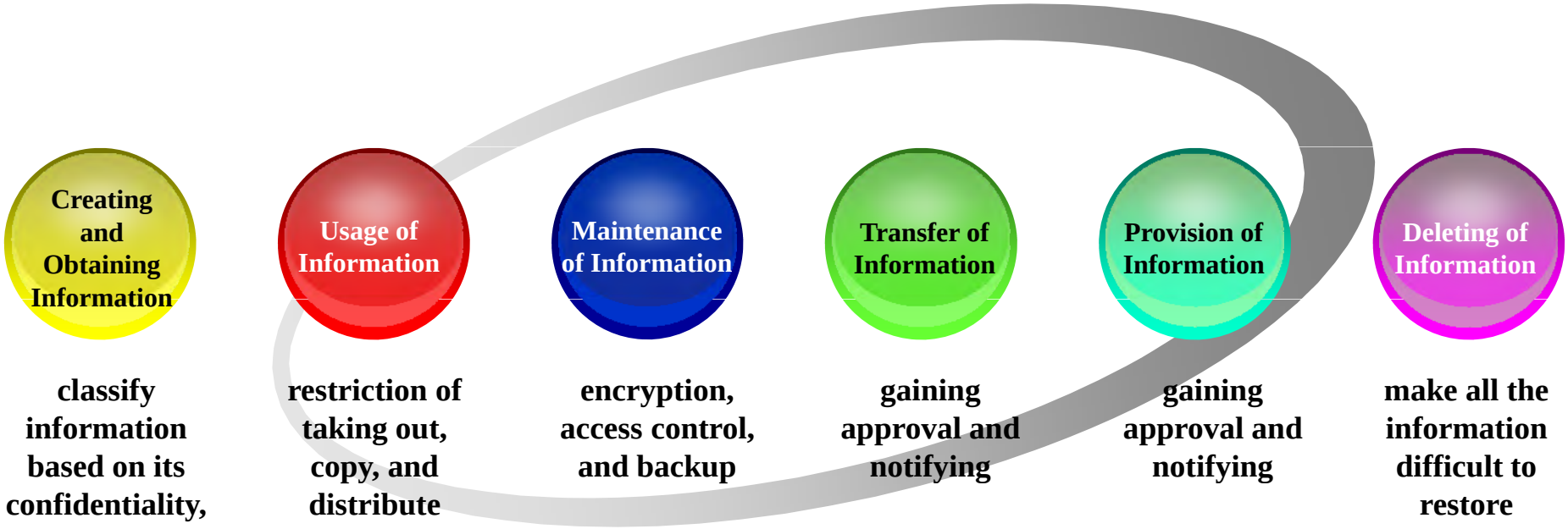
CLASSIFICATION	CLASSIFICATION STANDARD	MARKING
Integrity Class-2	The information that is handled in the tasks of the government agency (except written documents) and can infringe citizens' rights or have an impact (except minor ones) on accurate operation of tasks of the government agency if altered, wrongly described, or damaged.	(example) *preserve until yymmdd*
Integrity Class-1	The information that is not integrity class-2 information (except written documents.)	

AVAILABILITY

CLASSIFICATION	CLASSIFICATION STANDARD	MARKING
Availability Class-2	The information that is handled in the tasks of the government agency (except written documents) and can infringe citizens' rights or have an impact (except minor ones) on the stable operation of tasks of the government agency if damaged, lost, or made unavailable.	(example) *resume service in 1hr.*
Availability Class-1	The information that is not availability class-2 information (except written documents.)	

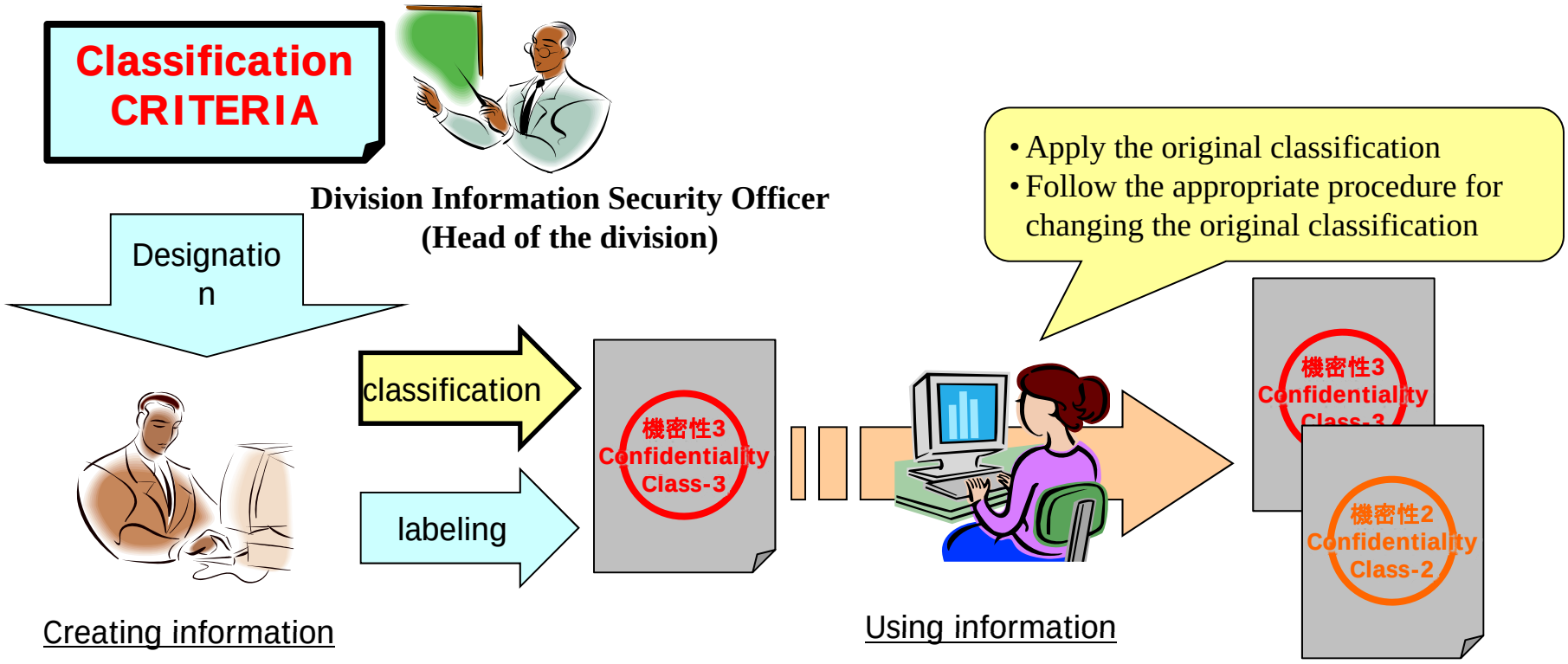
Requirements at each stage of information lifecycle

- Chapter 1.3 of the Standards for Measures, “Measures for Information,” defines compliance requirements at each stage of the information lifecycle – creation, usage, maintenance, transfer, provision, and deletion, and also indicates the measures that employees must always take when they execute their tasks to protect information.



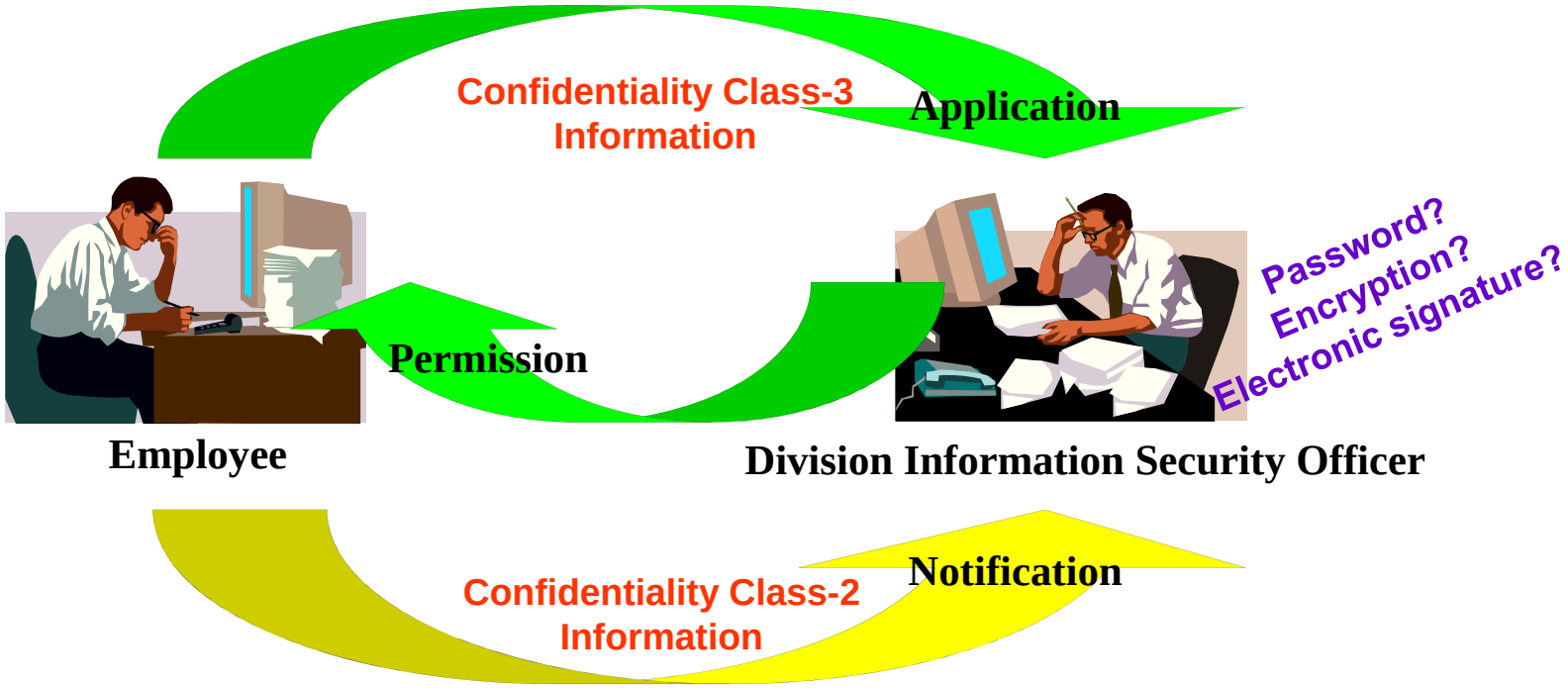
Procedure for the classification of information

- *Division Information Security Officer* is to set the criteria for the classification of information in his/her division, according to the ministry/agency's standards for the designation of classification.
- An employee is required to designate and label the classification of the information, according to the criteria.



Procedure for transferring information

- In transferring confidential information, an employee must gain approval from or notify the *Division Information Security Officer*.
- The *Division Information Security Officer* must consider the application and give permission only when it is appropriate.



Evaluation and Improvement

- To improve ministries' / agencies' activity, the following evaluations are conducted;
  - Implementation report
    - Each government employee must self-check his/her own compliance status to the security policy and report to the ministry/agency every year.
    - Ministries and agencies must report the self-check result to NISC.
    - Approx. 550,000 employees (97% of all government employees) carried out self-check in FY2008.
  - Evaluation on major IT equipments
    - Ministries and agencies must check their major IT equipments such as PCs, Web Servers and Mail Servers once a year, and report the result to NISC.

- Based on the evaluations and the findings, NISC/ISPC gives recommendations/guidance to ministries/agencies.
  - Consolidation of servers
    - Based on the findings from the evaluation on major IT equipments, ISPC recently gave guidance to all ministries and agencies to consolidate their servers connected to the Internet.