SECTION 4
Presentation Materials

Government Information Security Standard Criteria
Introduction

NiDA

October 1 2009

H.E. Chea Manit , Deputy Secretary General
and iSMTT team leader

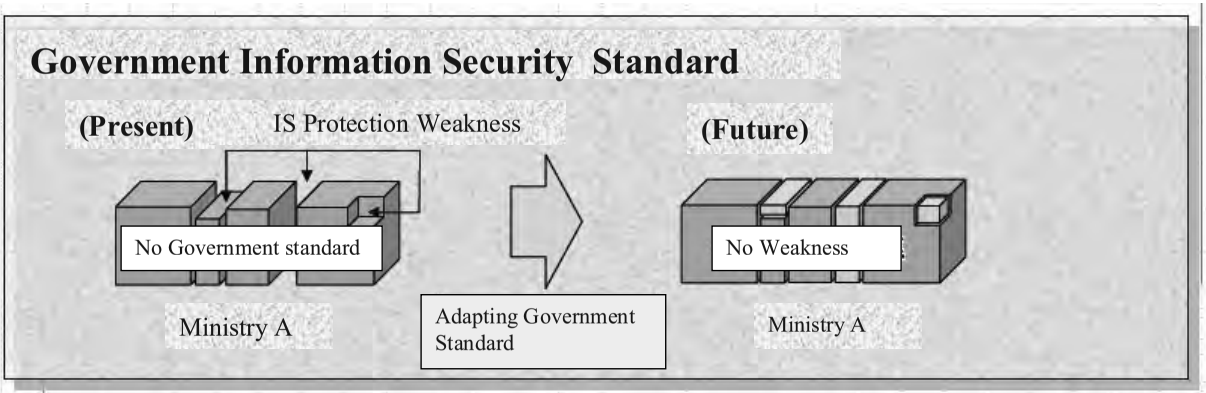
Yoshinori Kurachi JICA Expert

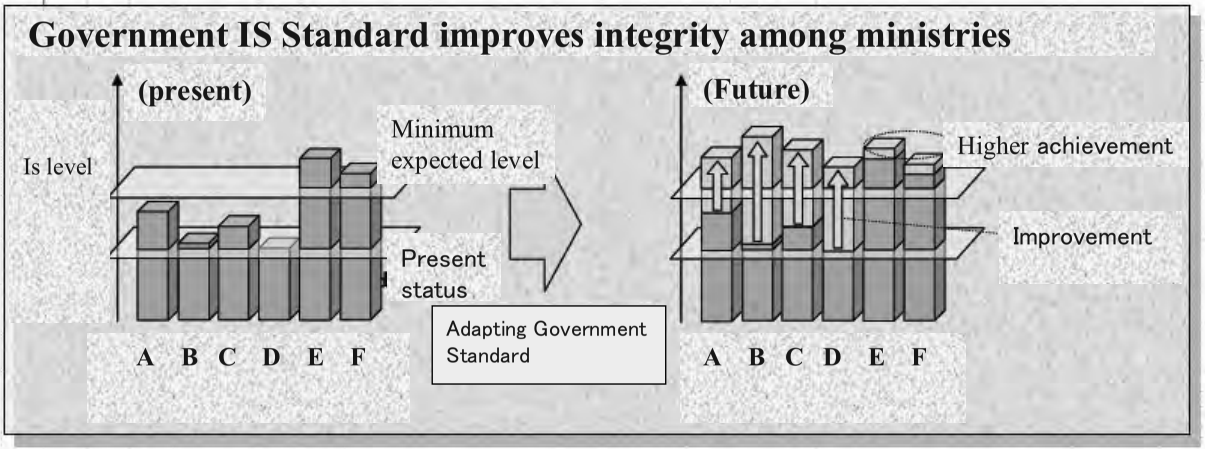
Government Information Security Standard Criteria

General Rules

1.1.1.1 GISSC position in the IS Management Documentation

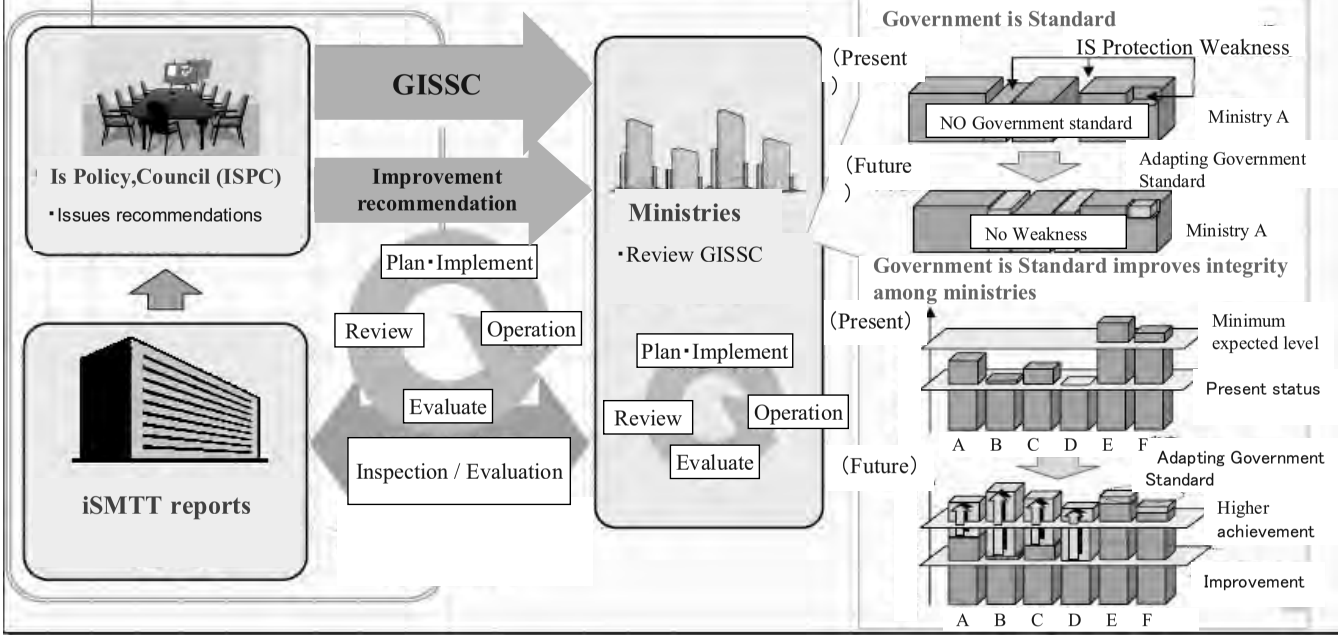
As a basic rule, every Ministry is responsible to plan and implement information security measures in order to avoid any accident within the Ministry Information and Communication System. However, the government should provide both the Fundamental Policies and an integrated framework as the **standard guideline**, so that all government agencies can develop and improve their information security measures with good integrity according to their own priorities.


Government Information Security Standard
(Present)
IS Protection Weakness
No Government standard
Ministry A
Adapting Government Standard
(Future)
No Weakness
Ministry A

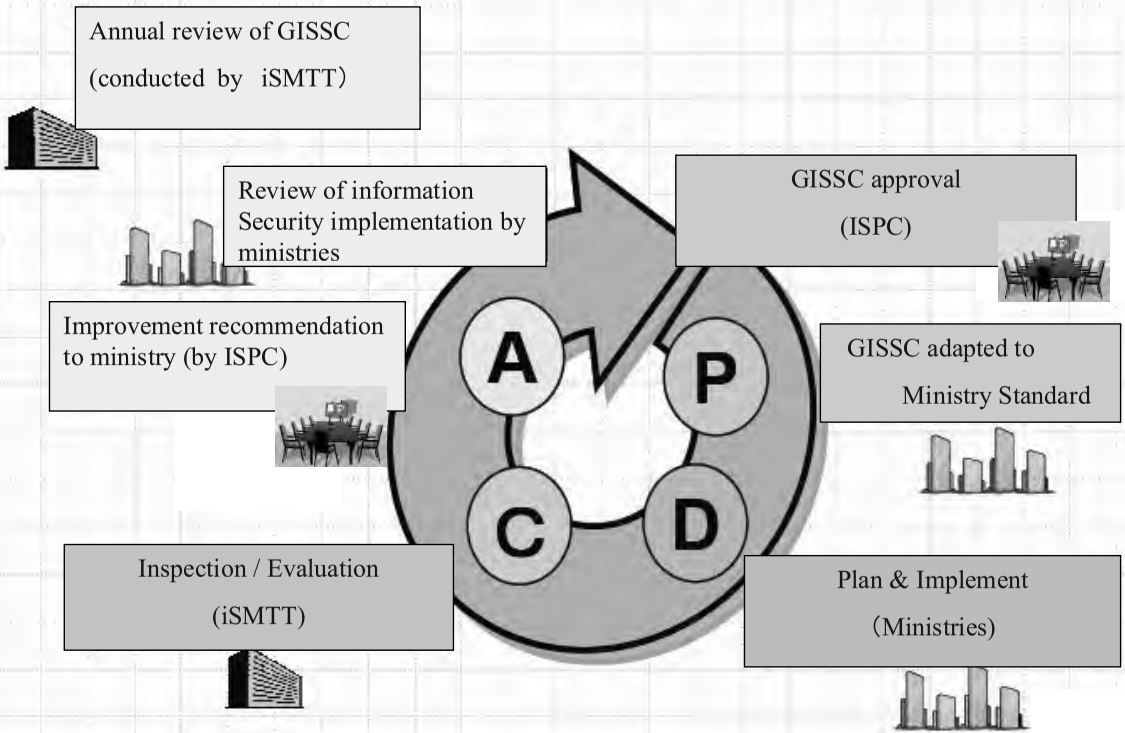

Government IS Standard improves integrity among ministries
(present)
Is level
Minimum expected level
Present status
A B C D E F
Adapting Government Standard
(Future)
Higher achievement
Improvement
A B C D E F

Apply Government Information Security Standard as Design Guideline

・Each Ministry Implements Improvement Plan According to Government IS Standard Guideline (GISSC).
・iSMTT inspects/evaluates effectiveness of the implementations. The National IS Council may issue improvement recommendations according to the iSMTT report.



PDCA (Plan/Do/Check/Action) procedures based on GISSC



General Rules

1.1.1.2 GISSC utilization method

The GISSC is designed to protect the government information asset. Information asset includes the followings:

/ Data stored in computers and electric storage media.

/ Printed documents contains ICT system description.

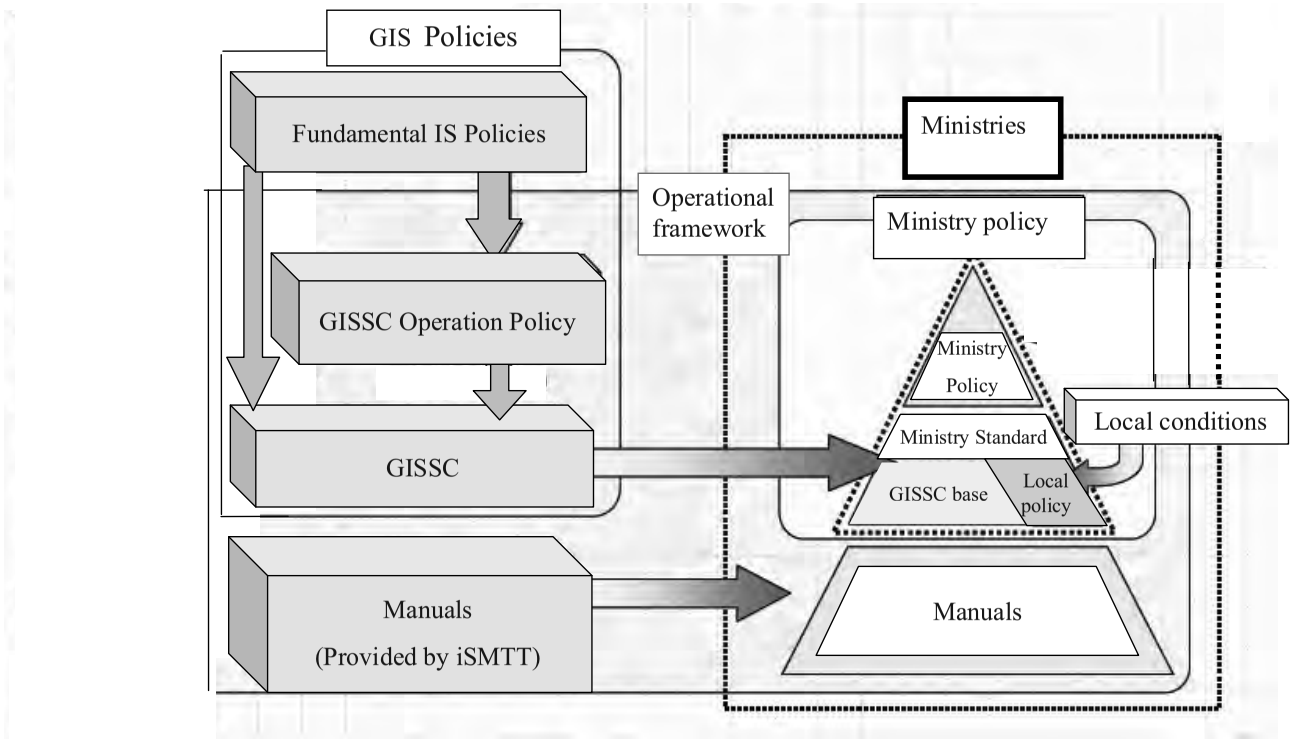
/ Printed computer output.

GISSC is applied to all government personnel, including hired ICT consultants.

All measures are provided with priority level. Priority varies according to either the importance of the information asset or the impact of the IS threats. Information Security measures should have good sustainability. Therefore, every measures should be reviewed periodically under the consistency with the GISSC guidelines.

IS Documentation Hierarchy

Position of GISSC



Government Information Security Standard Criteria

General Rules

1.2 Organization and responsibility development

(1) A Chief Information Security Officer is appointed who has a supreme responsibility to all information security management decision at every Ministry.

(2) An Information Security Management Committee is organized in order to review and plan IS policies and implementation plan.

(3) Information Security Managers are appointed in order to manage all information security works within the ministry. Managers are responsible to make and sustain rules regarding Government staff relocation (source of all confusions). It is important mission for the managers to maintain good communications with other IS mangers of other ministries.

(4) Breach of rules

When government personnel becomes to know a breach of information security rules, it has to be reported to IS Manager immediately. IS Managers will take appropriate actions. If needed, a fact of the breach of rules should be reported to the Chief IS Officer.

Government Information Security Standard Criteria

General Rules

1.2 Administration

Information Security measure education should be planned and implemented every year.

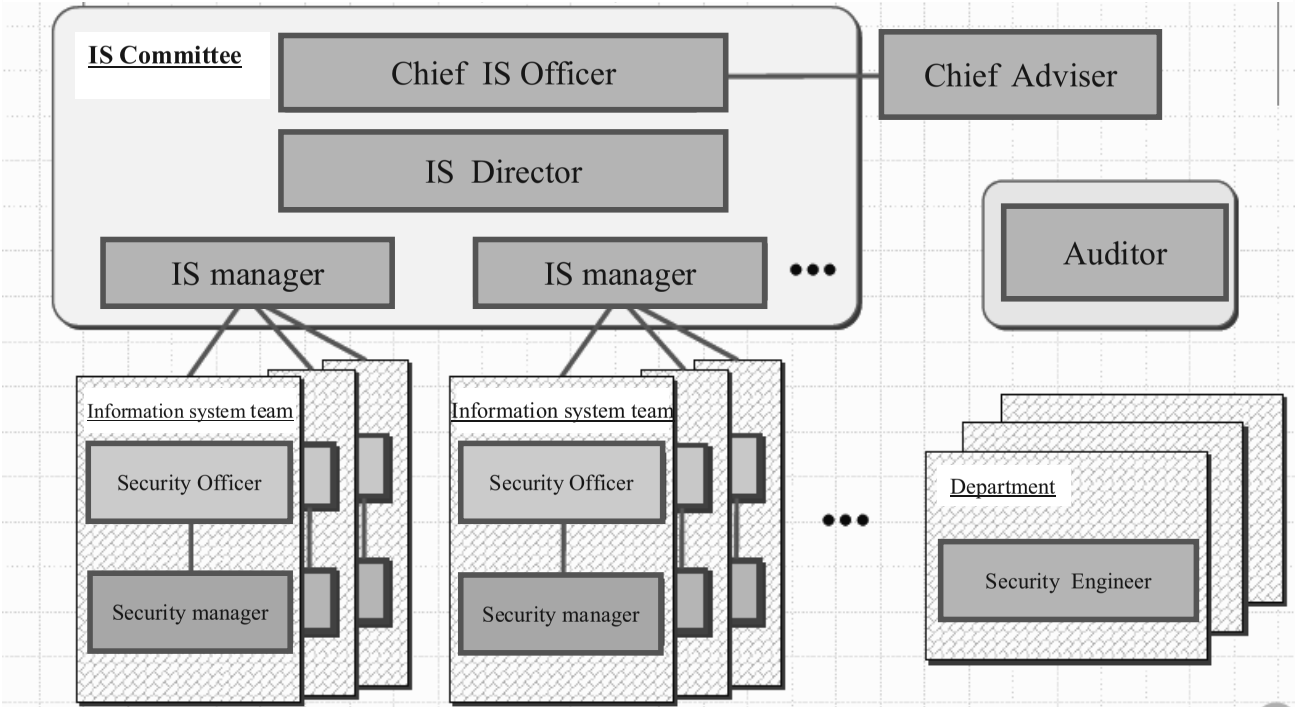
When incidents occur, report should be made immediately according to predetermined manual.

1.2.3 Inspection

Every Ministry is requested to arrange self inspection plan for their information security management implementation status every year.
A inspection report should be given to the Chief IS Officer.
Collected reports are summarized and published within the government.

Every Ministry reviews summarized report. It is required to make improvement plan according to review result.

Organization & Responsibility



Government Information Security Standard Criteria

General Rules

1.3 Handling Information Asset

1.3.1.1 Data creation and input

1.3.1.2 Use of data

IS Management Committee should make classification and handling rules for all important data base (asset) with regard three view points:

- Confidentiality	Classified/Leaking causes severe damage/others
- Integrity	Falsification causes national damage/others
- Availability	Unable to access causing national damage/other

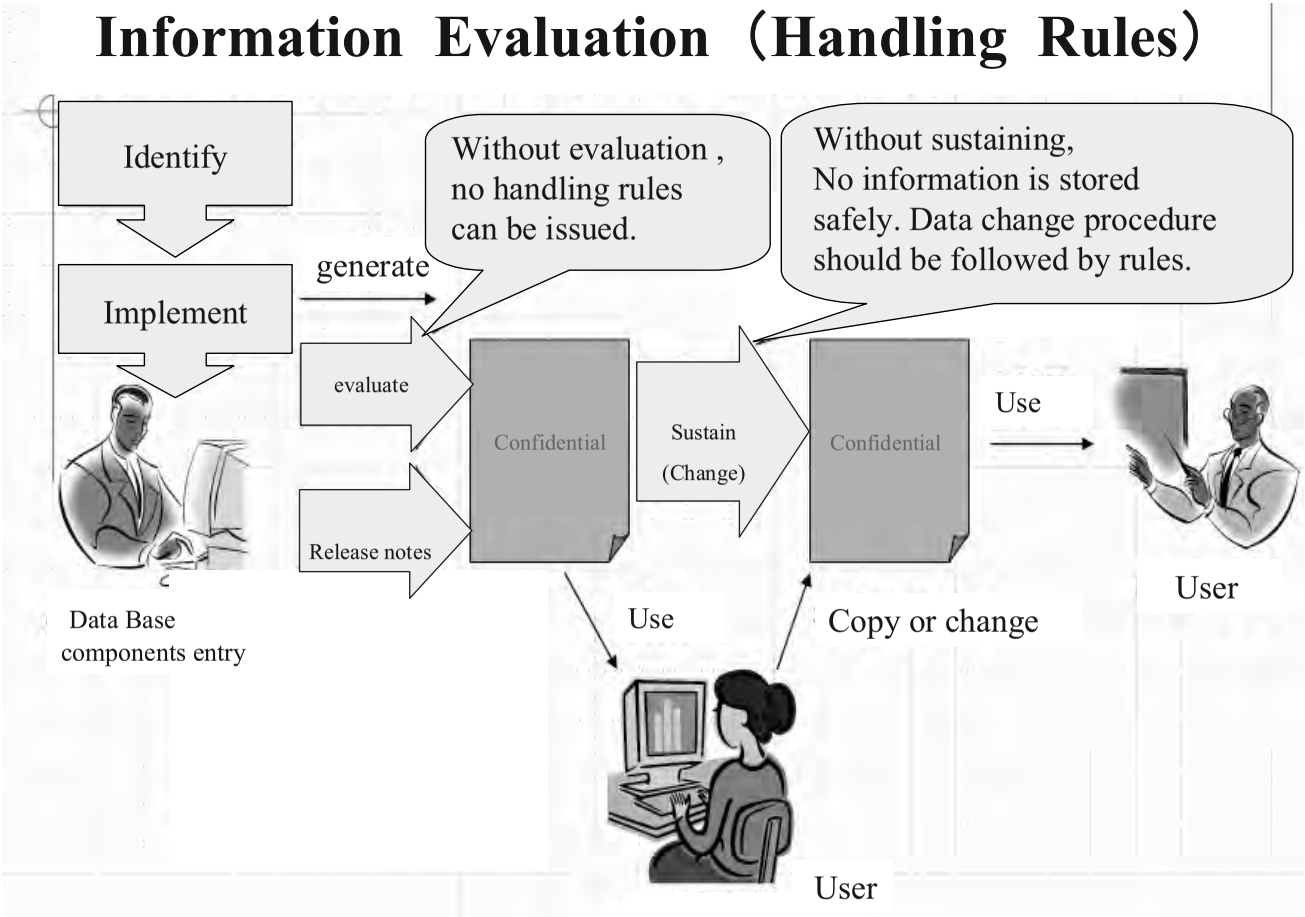
1.3.1.3 Data storing

1.3.1.4 Data transferring

1.3.1.5 Data publication

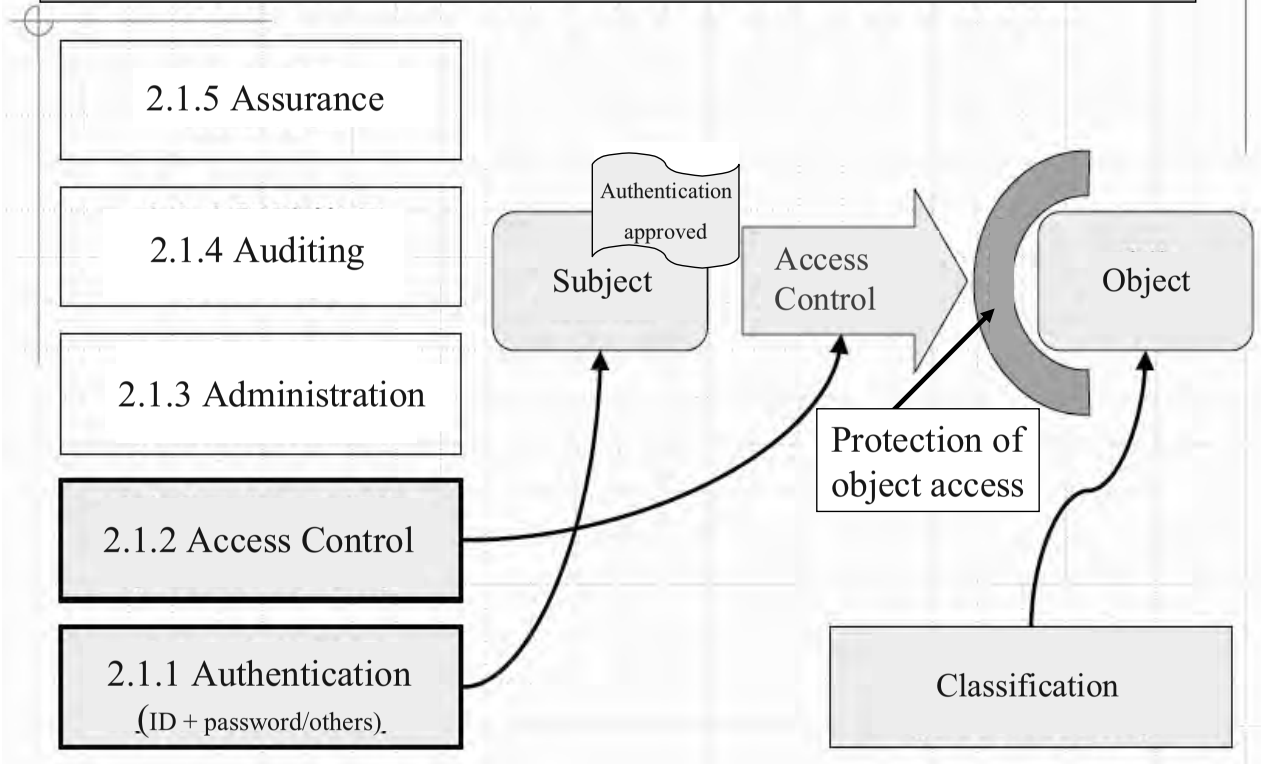
1.3.1.6 Data deletion

Information Evaluation（Handling Rules）



Measures for specifying information security requirements

- Information Security functions -



Government Information Security Standard Criteria

Information Processing System

2.1 Information Processing System

2.1.2 Information security threats

2.1.2.1 Measures for security holes

IS Managers of Information System should give good efforts to avoid any security holes both in their application software and communication equipments at installation. It is their duty to investigate security hole information constantly.

2.1.2.2 Measures for computer virus

It is duty for the IS Managers to install anti-virus software to all PCs and servers.

2.2 Measures for information system components

2.2.1 Facility and environment

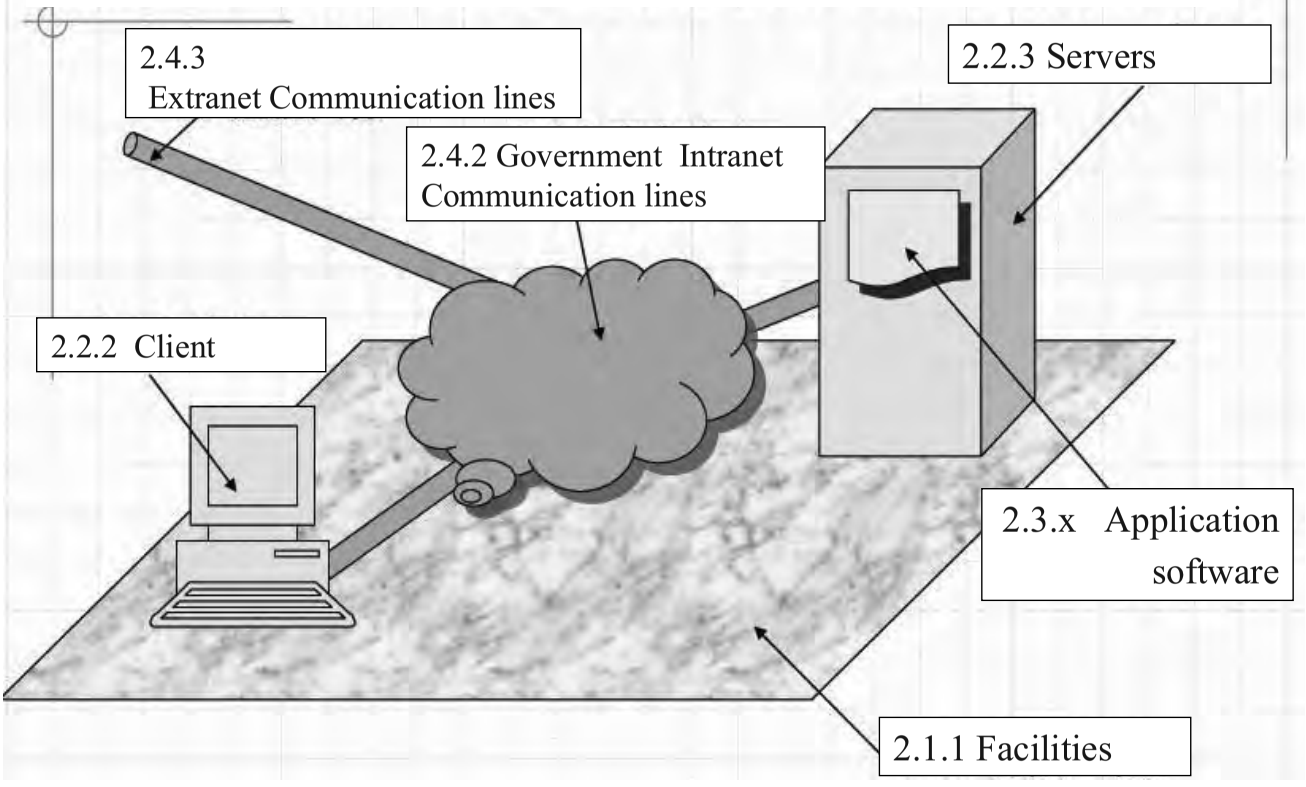
2.2.2 Computers

Common/Client/Servers/

2.2.3 Application Software

e-Mail/Web/DNS/Communication line/Intranet/Extranet

Five target Components of GISSC



Information Asset Classification

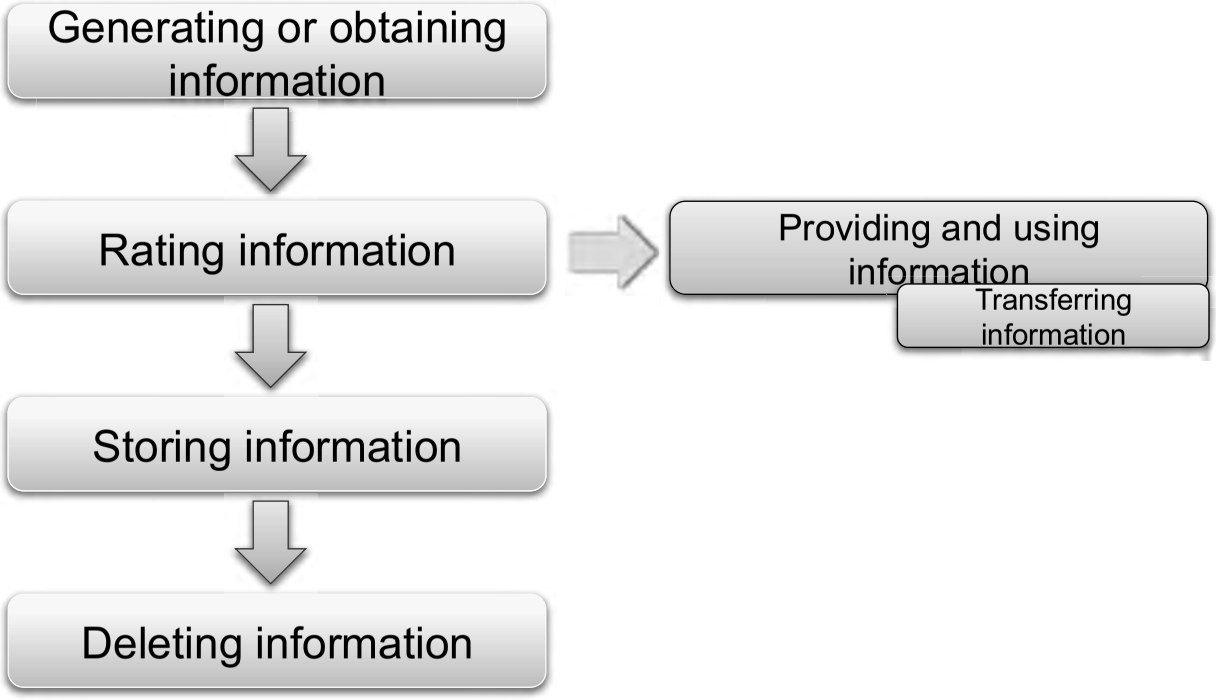
Keisuke Kamata, JICA Expert, 2009 Oct 1st@CJCC

Point of the Presentation

- **Introduces the classification, storage and disposal of information, focusing on the "Measures for Information"**
- From standard of National Information Security Center (NISC), Japan
- Standards for Information Security Measures for the Central Government Computer Systems

  http://www.nisc.go.jp/active/general/kijun01.html

Information Life Cycle



Thrash out information asset

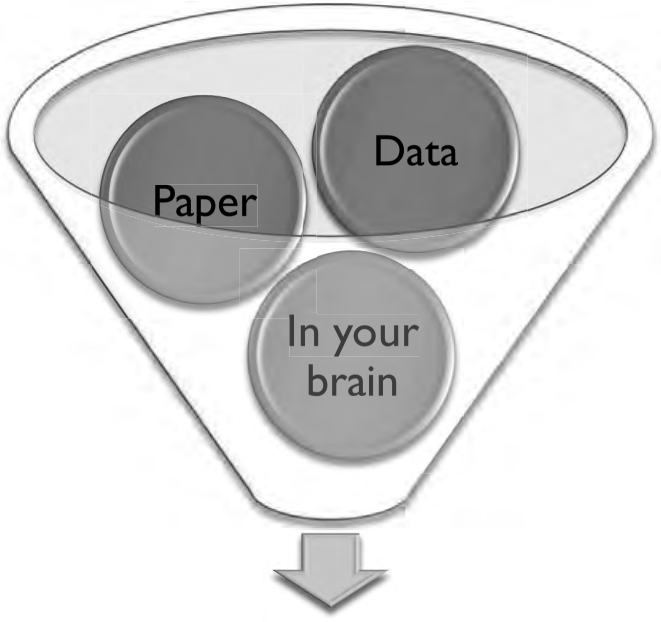
- What is information asset?
  - Documents: Memo, contract
  - Data: Personnel information, financial information, e-mail, database data
  - Hardware: Information system, network, server, PC
  - Software: Application software, OS
  - Intangible assets: Know-how, trust of society
- Management method is different
  - To each type of information

Information Asset Consideration

- To protect information asset from threat
  - What are you protecting from what ?
  - How will you protect ?

- Clarify the list of assets
  - Should recognize what you have
  - Or you Cannot rate, cannot protect

Where is the information asset?

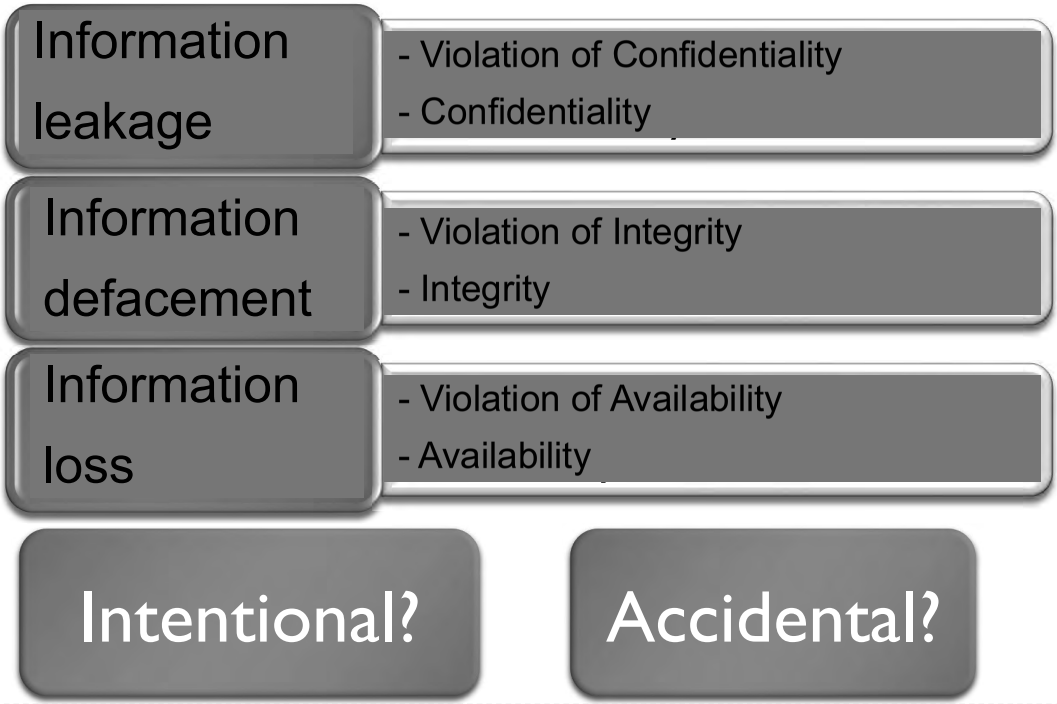


Information Asset

Damage to Information

Information leakage	- Disclosed to a third party - Opened to the public
Information defacement	- Unable to provide adequate information
Information loss	-Unable to use information when it is necessary

Damage to Information



Owner of Information

- Owner of Information
  - Who is the owner of information ?
    - Who's "problem" if the information is unprotected?
    - What we need to think when providing information

  - Things to consider when providing information
    - Do you have approval from the information owner?
    - Can the person who receives the information handle it appropriately?
    - What are the differences in information handling standards between the person providing the information (you) and the person receiving the information?
    - The information owner should control the information

Necessity of Information Management

- Why is it necessary to manage information?
  - To ensure the three major elements of information security
    - Confidentiality, Integrity, Availability
    - Measures for leakage, defacement and loss
  - Classifying and managing information based on its importance enables to ensure security with consideration of priority and cost

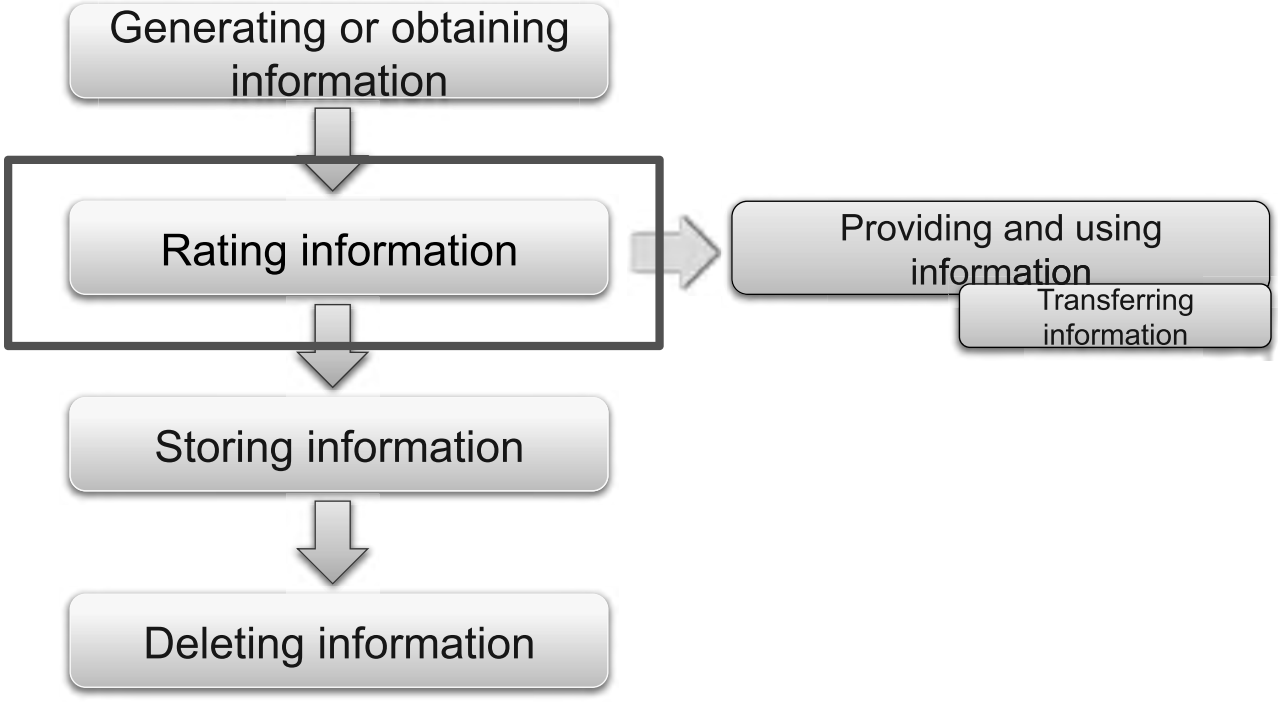
Problems of Information Management

- Information classification is primarily to reduce the cost of information management
  - Apply the adequate management cost to each information by "classifying" the information appropriately

57

- Over management leads to over cost
  - The more confidential the information, the more management cost it takes/should take further
  - Draws apart from the original objective
  - Happens in organizations in reality

Information Rating



Information Rating

- For information handled in the government office, it is necessary to rate information to ensure security
- Have to develop rules and regulations for information rating

- Basic points of information rating
  - Electromagnetic record (data)
    - Confidentiality
    - Integrity
    - Availability
  - Documents
    - Confidentiality

Requires to develop rules and regulations in the above perspectives

Information Rating
Information Rating by Confidentiality

Rating	Classification Criteria	Handling Limits
Confidentiality level 3	Information handled by the government office which require confidentiality level equivalent to classified documents	Ex） Prohibit to reproduce Prohibit to redistribute Mandatory to encrypt
Confidentiality level 2	Information handled by the government office which do not require confidentiality level equivalent to classified documents, however that has the possibility of infringing citizen's rights, or interfering with government office	
Confidentiality level 1	Information other than confidentiality level 2 and 3	

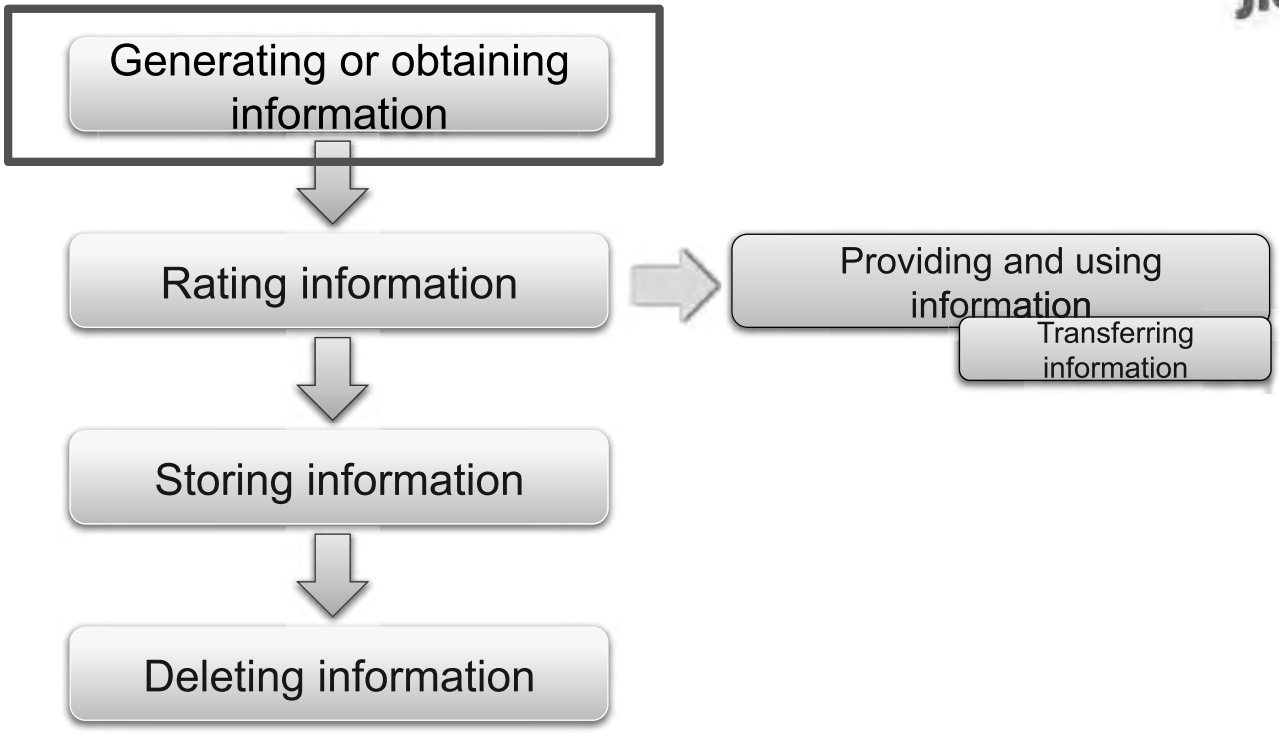
Information Rating
Information Rating by Integrity

Rating	Classification Criteria	Handling Limits
Integrity level 2	Information handled by the government office (excluding documents) that have the possibility of infringing citizen's rights or interfering with government office (excluding minor cases) through defacement, error or corruption	Ex) Store until Day/ Month/Year
Integrity level 1	Information other than integrity level 2 (excluding documents)	

Information Rating
Information Rating by Availability

Rating	Classification Criteria	Handling Limits
Availability level 2	Information handled by the government office (excluding documents) that have the possibility of infringing citizen's rights or interfering with government office (excluding minor cases) through damage, loss or non-availability of the information	Ex) Restoration within one hour
Availability level 1	Information other than availability level 2 (excluding documents)	

Information Handling
Generating and obtaining information



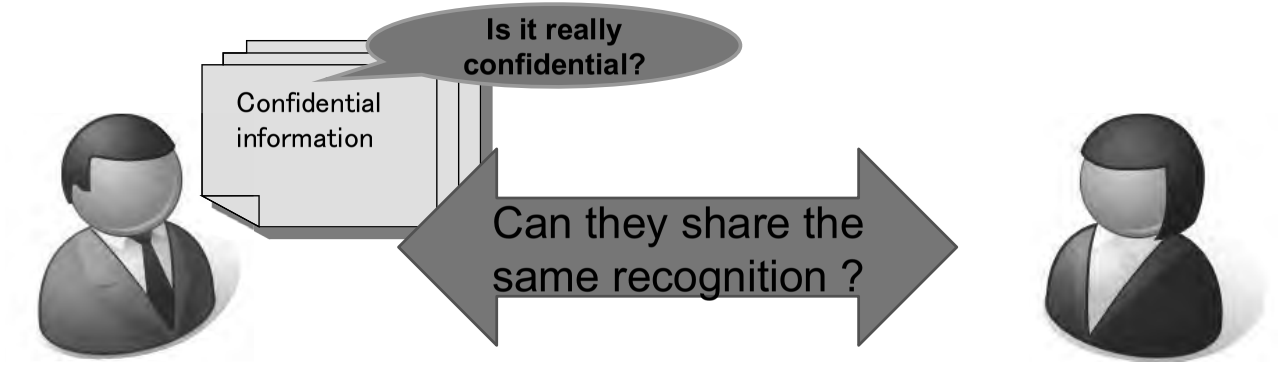
Information Handling
Generating and obtaining information

- Items that describe about generating and obtaining information
- You should not generate or obtain information other than for the purpose of government office work
  - You should not use operational information for private use
- Rate the information when it is generated or obtained
  - Rate the information by confidentiality, integrity and availability, when it is generated or obtained
    - Information rating should be "easy to see" (Ex. on the cover in red, etc.)
    - Consider the rate of the source when quoting information
  - If you need to change information rating, consult with the person who generated or obtained it
    - Necessary to review the rate

64

Information Handling
Generating and obtaining information

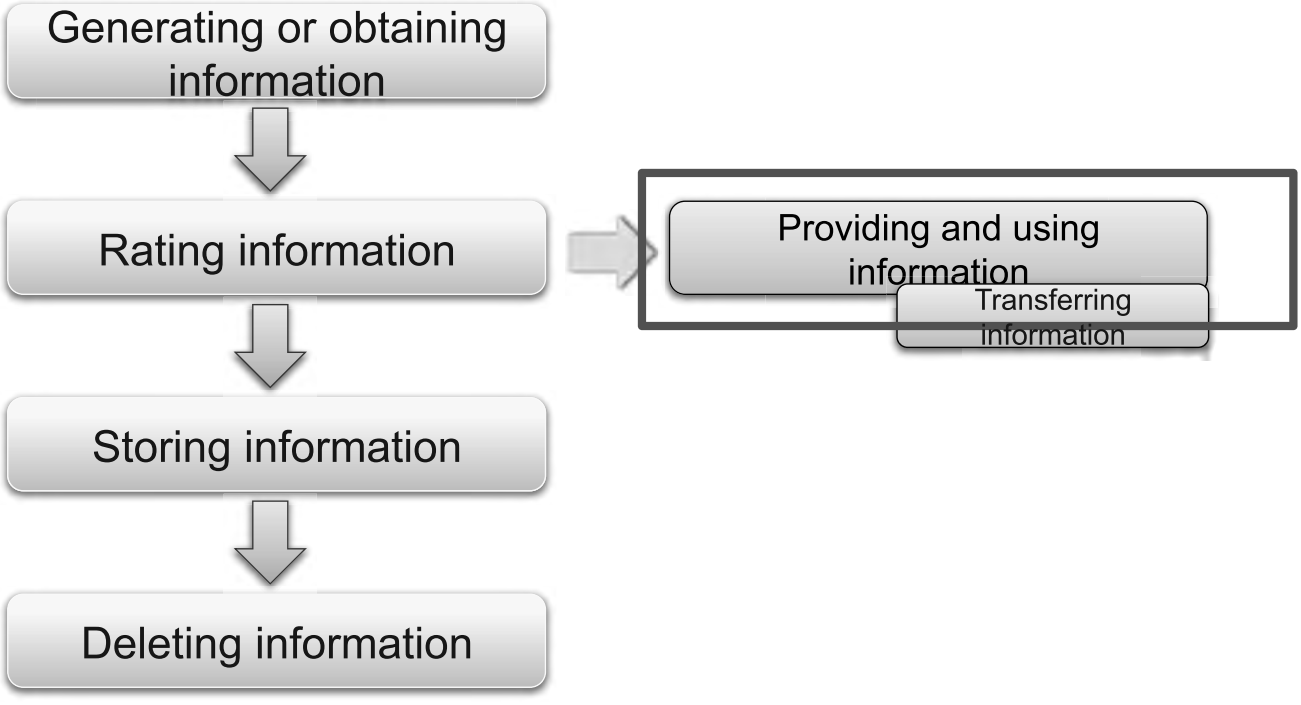
- Precautions for generating information
  - Need to consider the perception gap between the person generating the information and the person using the information
    - Need information rating –> Do not rate higher than necessary



Mr. A
(Person generating the information)

Ms. B
(Person using the information)

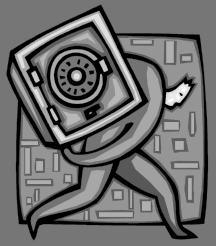
Using information



Using information

Examples of Inappropriate Use of Information

Taking out information



Reproducing information

Providing information

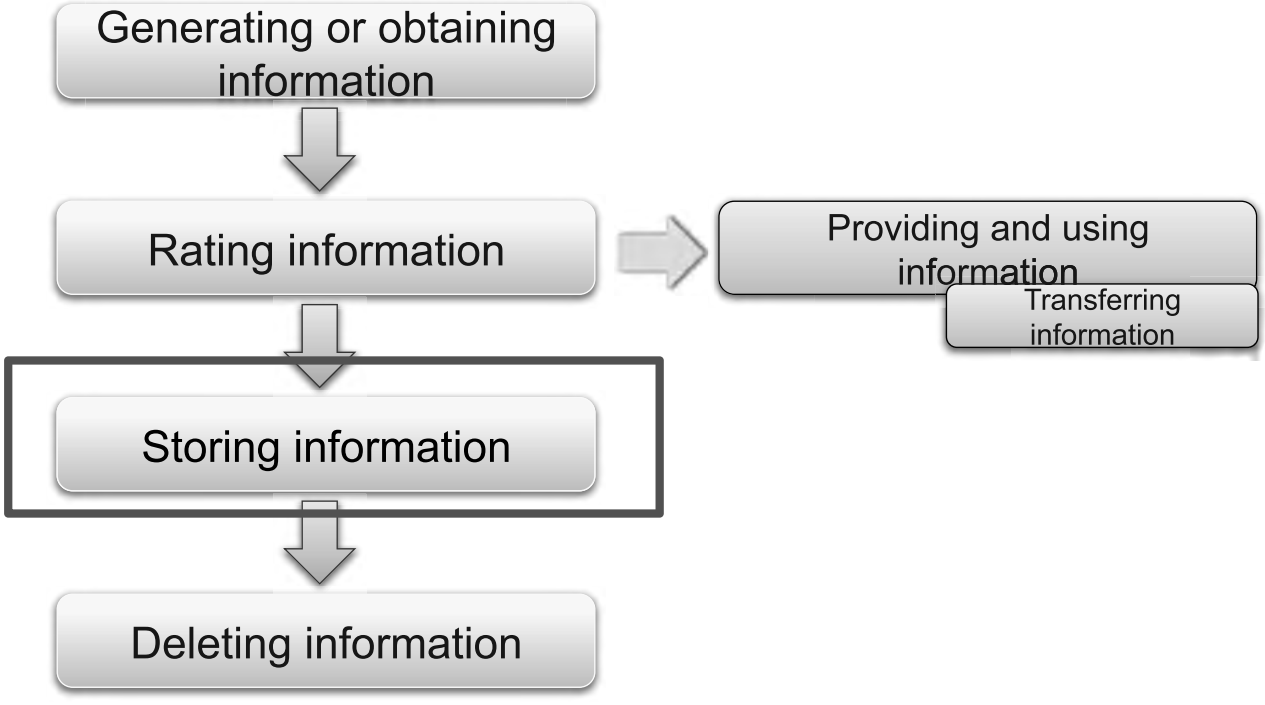
Leaving information

Information Handling
Using information

- Inadequate information handling due to the information user‘s lack of recognition results in risks such as information leakage

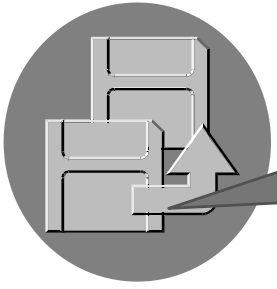
  → Need to ensure that the information is handled based on its rating
- Prohibit the use of information other than for operational use
- Require information handling based on its rating and handling limits
- Handling information that needs high protection
  - Do not take out from the governmental office
  - Do not leave information that needs high protection
  - Do not copy Confidentiality level 3 information more than necessary (Ex. Put copy prohibited tag)
  - Do not distribute highly confidential information more than necessary (Ex. Put information passing prohibited tag)
  - Others: Require to attach a sequence number consisted of a clear notification of the handling term and Confidentiality level 3, as well as to clarify the location, etc.

Storing information



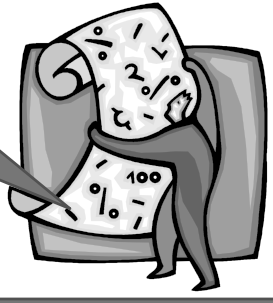
Information Handling
Storing information

Appropriate storage and management of documents and data



Backup of information

Protecting information with encryption or passwords



Electronic signatures to data

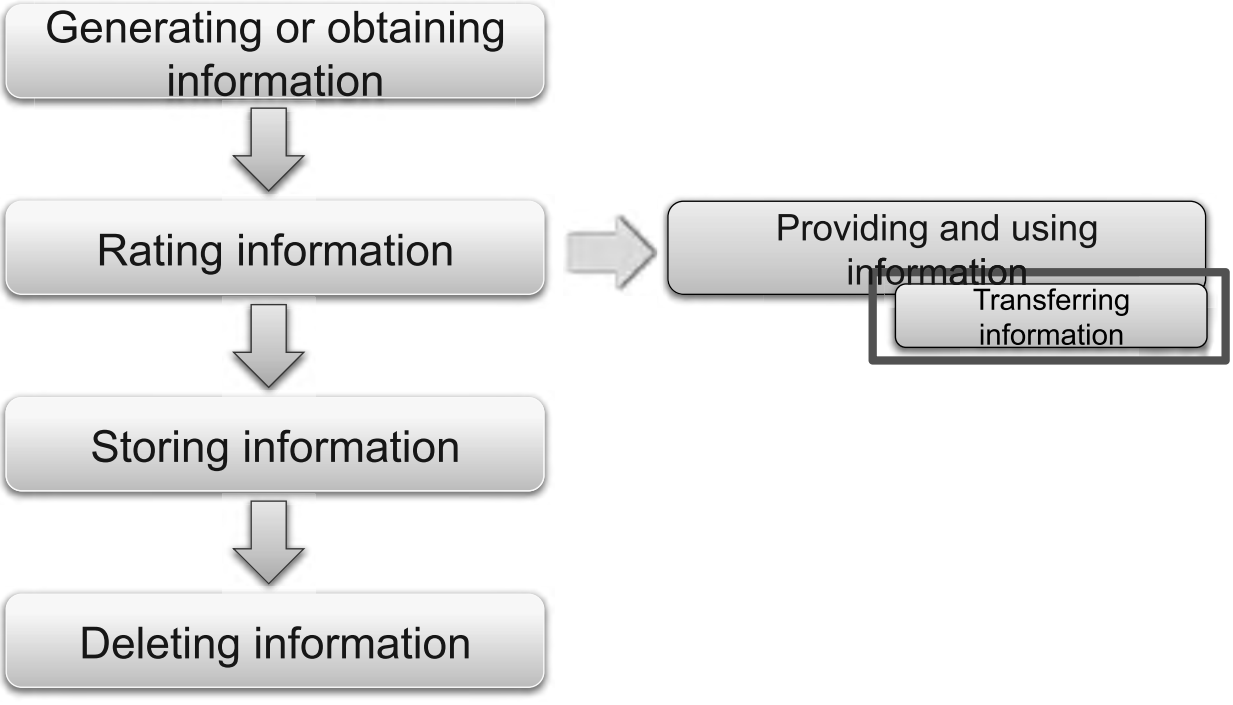
Access control: Who can access to the information?

70

Information Handling
Storing information

- Possibility of leakage remains as long as the information is stored
- Storing information based on its rating
  - Apply appropriate access control to the information
    - Apply in units such as electronic computers, OS, applications, files, etc.
- Electromagnetic recording media storing information should be managed appropriately
- When recording the information electromagnetically, you should consider and execute the followings
  - Necessity of encryption: Ensuring the confidentiality
  - Necessity of electronic signature: Ensuring the integrity
- Consider and execute the necessity of backing up (or copying) the info
  - Need to consider the procedure, time required and restoration method
- Consider the possibility of disaster for backup storage
- Storage term of the information, and data erasure after the storage term

Transferring Information



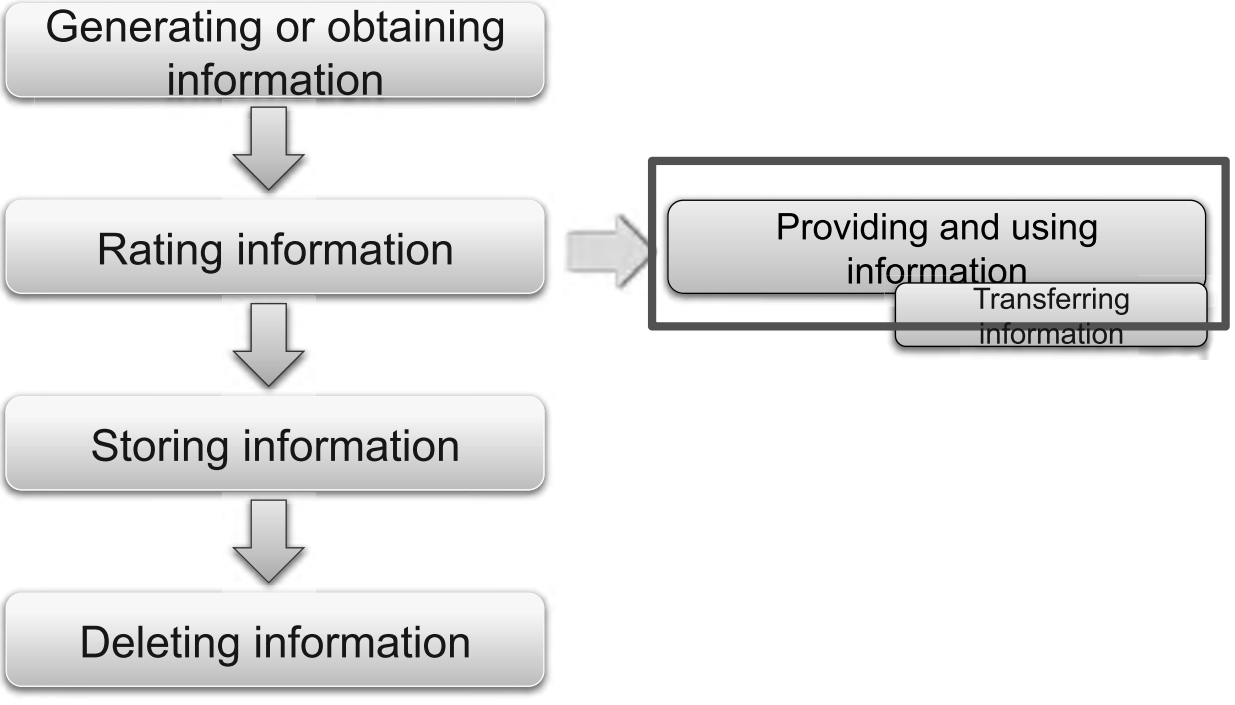
Information Handling
Transferring information

- Need to consider the possibility of information leakage, etc. through information transfer from e-mails and media that store information
- Obtain an approval, or report when transferring important information
  - Confidentiality level 3, Integrity level 2, Availability level 2 are subject to important specification
  - Confidentiality level 2, Integrity level 1, electromagnetic record of Availability level 1, or documented information of Confidentiality level 2
  - Need approval from the information security manager
  - Recommended to establish the procedures
- Select information sending or information transferring
  - Transferring electromagnetic record information that require high protection is subject
  - Select either information sending or transferring, and report to the information security manager
  - Need risk assessment

Information Handling
Transferring Information

- Deciding the method to transfer information
  - Select the appropriate method to transfer information, among the wide variety of transferring methods
  - Consider the communication pathway or encryption, for transfer via the Internet
    - Using VPN, S/MIME or reliable ISPs
- Protection Measures for Documents
  - Apply adequate measures based on the information rating when transferring important information
- Protection measures for transferring electromagnetic record
  - Consider use of passwords (ex. zip passwords)
  - Consider the necessity of encryption
  - Consider the necessity of electronic signature
  - Consider the necessity of backup
  - Consider the possibility of loss during the transfer and consider to transfer the same information in multiple pathways
  - In addition to encryption, divide the information in multiple pieces and transfer them in different pathways

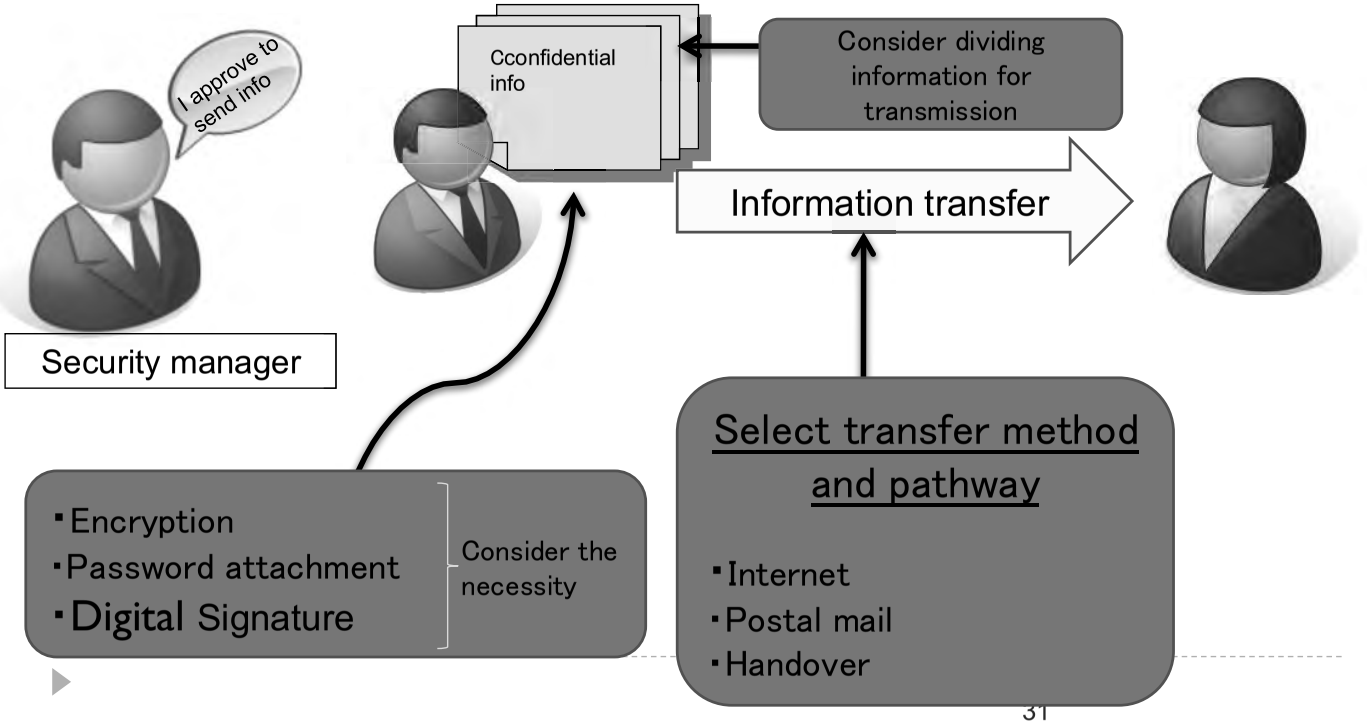
Providing Information



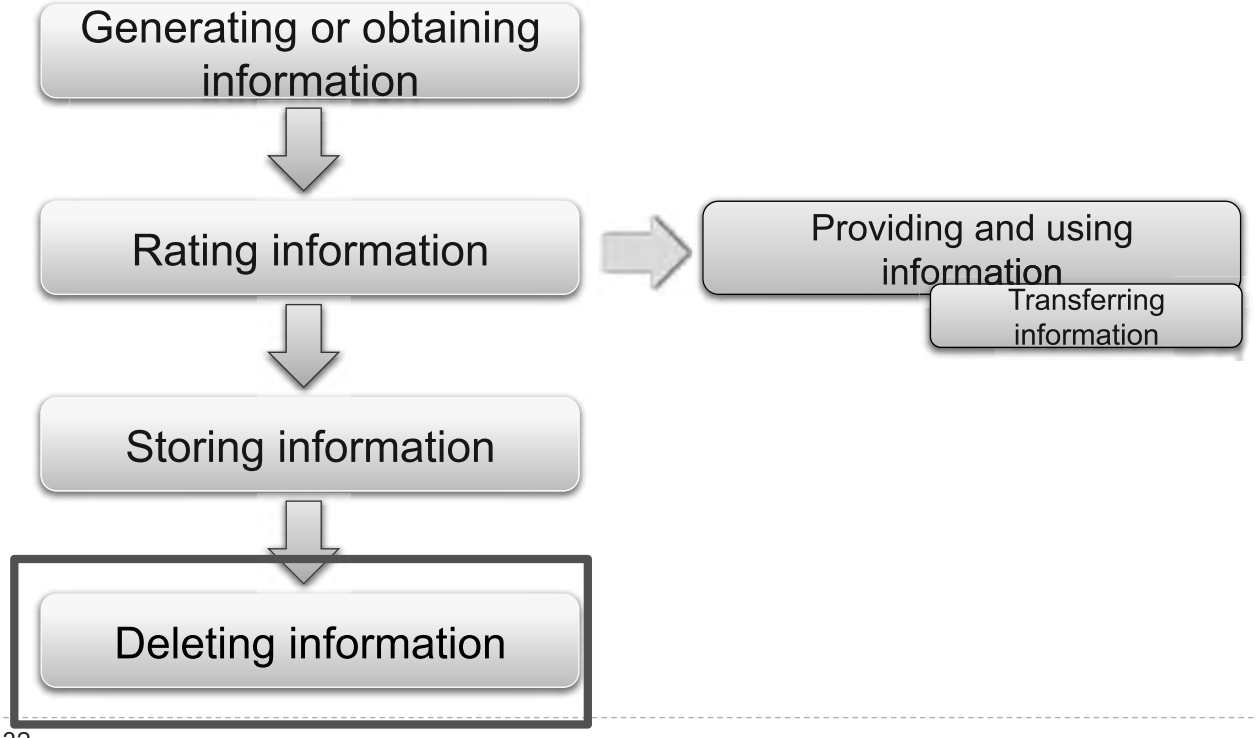
Information Handling
Providing information

- Concern of inappropriate information handling resulting in information leakage, in cases of providing information to non-governmental officers for operational purposes.
- Confirm that the information is "Confidentiality level 1" when publishing it
- Pay attention to the "attachment information" when publishing the information
  - Property section of Word (Creator, Date, Time and so on)
- Should receive approval from the security manager when providing important information to non-governmental officers
  - Classified in details based on the information rating
- Should apply measures for appropriate information handling when providing important information to non-governmental officers
- Pay attention to the "attachment information" when providing important information to non-governmental officers

Information Handling
Transferring information and Providing Information



Information Handling
Deleting information

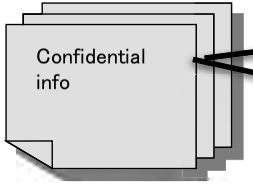


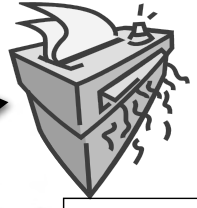
Information Handling
Deleting information

If you leave unnecessary information it may be lost or stolen

Documents

Unnecessary information





Destroy the data electrically and magnetically

Request to professional companies (melting, etc.)

Electronic data

Media storing unnecessary information

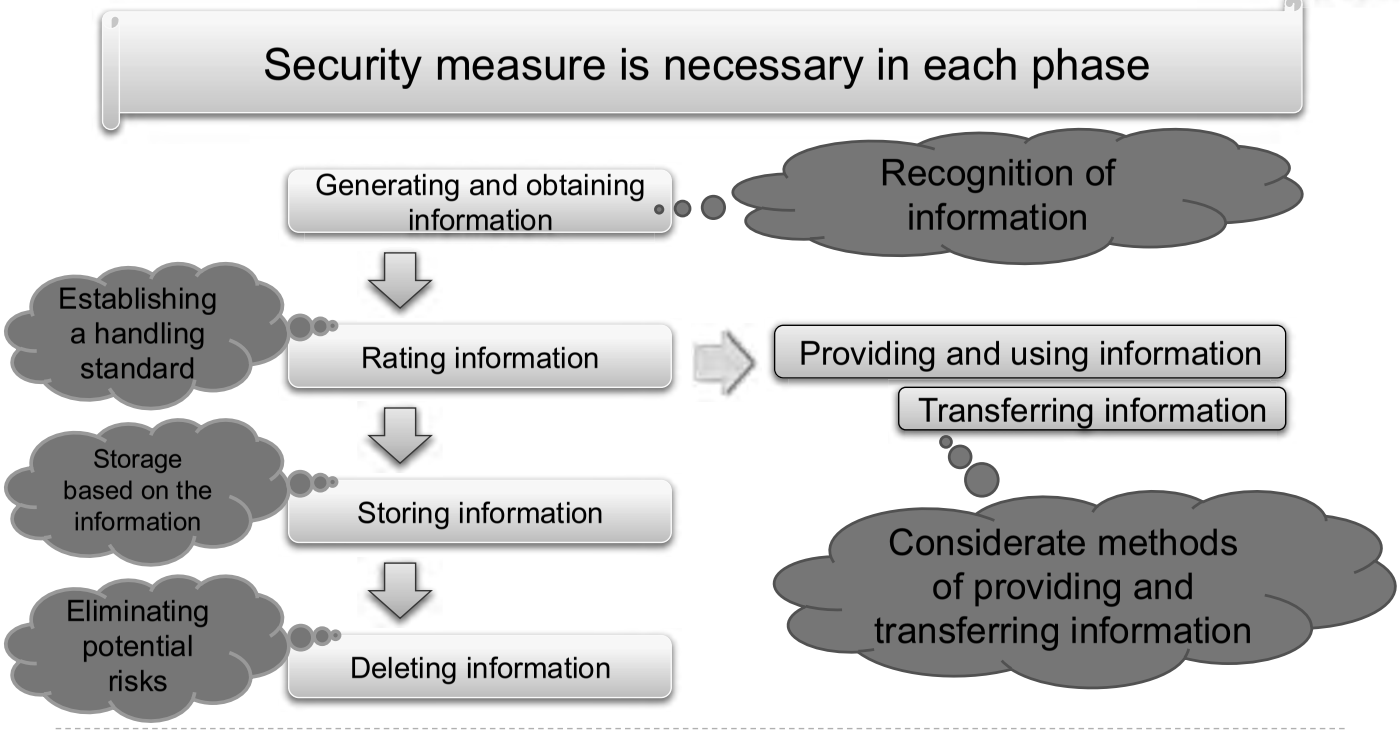
- "Ensure" to delete the data
- Destroy the data magnetically
- Destroy the whole media physically
- Melt the whole media
- Request professional companies (delete, destruct, etc.)

Information Handling
Deleting information

- Concern about unnecessary information being left without appropriate disposal, resulting in information leakage. Also, if appropriate measures are not taken when deleting the information, it is possible to restore the data.

- Method of deleting electromagnetic record
  - When disposing electromagnetic record media, you need to ensure that all information is "difficult to restore"
    - In Windows, simply "deleting the file" leaves it easy to restore
    - Applies also to digital cameras
- Precautions of providing electronic record media to others
  - Erase confidential information
- Erase confidential information based on the setup conditions of the electromagnetic record media
- When disposing documents of highly confidential information, ensure that it is difficult to restore

Summary 1


Security measure is necessary in each phase
Generating and obtaining information
Recognition of information
Establishing a handling standard
Rating information
Providing and using information
Transferring information
Storage based on the information
Storing information
Considerate methods of providing and transferring information
Eliminating potential risks
Deleting information

Summary 2

- Information changes the status after time pass
  - Change of rating may happen
    - From confidential information to public information
    - From handle with care information to confidential information
  - Review the rating
  - Information that becomes unnecessary
    - Keeping unnecessary information will cause managing cost
- Need a standard as an organization (or as government)
  - Cannot establish a uniform measure if individuals evaluate according to each information
  - By applying standardized handling according to the organization policy, you can smoothly send and receive information between organizations and ensure information security
  - Organization standards also need review along time