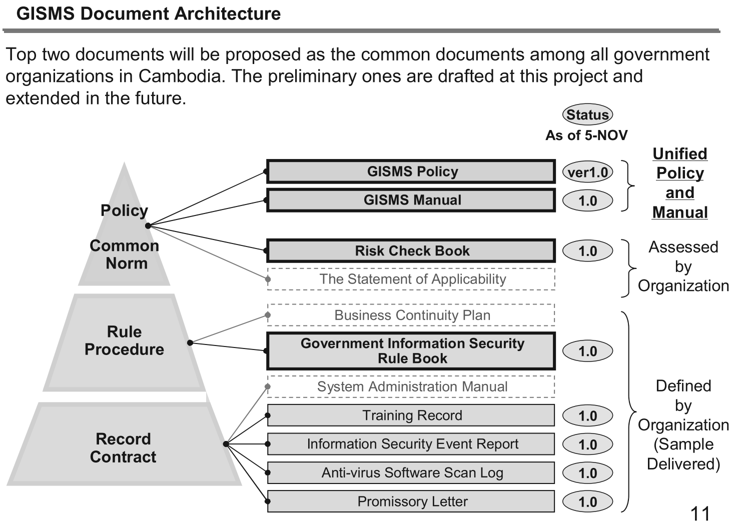

GISMS Document Architecture

Top two documents will be proposed as the common documents among all government organizations in Cambodia. The preliminary ones are drafted at this project and extended in the future.

Status
As of 5-NOV

Policy

Common
Norm

Rule
Procedure

Record
Contract

GISMS Policy — ver1.0

GISMS Manual — 1.0

Unified Policy and Manual

Risk Check Book — 1.0

The Statement of Applicability

Assessed by Organization

Business Continuity Plan

Government Information Security Rule Book — 1.0

System Administration Manual

Training Record — 1.0

Information Security Event Report — 1.0

Anti-virus Software Scan Log — 1.0

Promissory Letter — 1.0

Defined by Organization (Sample Delivered)

11

4) <u>GIS Rule Book</u>

This is defined by ministry. A sample GIS Rule Book, which is defined based on the default risk evaluation values of Risk Check Book blank form, is drafted by GIS Office. It has to be authorized by the top of ministry. Put the name of ministry on the document.

Other supplementary documents are defined and utilized by ministry.

4.5.2. <u>Document Revision, Distribution, Access and Keeping</u>

<u>Revision</u>

GISMS Policy shall be declared by the top of Royal Government of Cambodia. Hence, its revision procedure is defined by the other rules specified in RGC. (This needs to be specifically determined in a decree system in the future.)

GISMS Manual and Risk Check Book are revised yearly by GIS Office on the basis of comments/ requests from ministries implementing ISMS. The drafted documents are authorized with the same procedures defined in 4.5.1 Document Structure and Authorization.

All other GISMS documents revision is defined by ministry in accordance with PDCA cycle defined in 4.3 Check and 4.4 Action.

GISMS Manual, Risk Check Book and GIS Rule Book must have a revision history to assure which revision readers are referring.

<u>Distribution, Access and Keeping</u>

The confidentiality of GISMS documents varies by document, which is defined as follows;

1. GISMS Policy and GISMS Manual are classified as "general," which

means they can be got published and all Cambodian people can access and read them.

2. Non-assessed Risk Check Book contains no identified risks in a ministry and it is classified as "general." On the other hand, After-assessed Risk Check Book contains identified risks (threats and vulnerability), therefore, it is classified as "internal," which requires the careful distribution, access and keeping only in a government business operation.

3. GIS Rule Book contains the internal business rule and procedure and it is classified as "internal."

Copies of all revisions of after-assessed Risk Check Book, GIS Rule Book and defined records blank forms must be submitted to GIS Office and it keeps for five years.

All other GISMS documents distribution, access and keeping are defined by ministry. However, it is requested to take carefully deal with handling documents which contain confidential information (e.g. server IP address, personal privacy information).

4.6. Record Control

Records need to be managed for implementing rule and procedures. Control of authorization, revision, distribution, access and keeping of records blank form can be defined in GIS Rule Book.

Generally, records are submitted by the designated officials and filed and reserved by Information Security Office. Keep numbering those records uniquely identified. The period of keeping of all records is defined as one year, otherwise it is specifically defined.

Records often contain confidential information (e.g. server IP address, personal privacy information), and it is requested to take carefully deal with handling.

5. Management Responsibility

5.1. Management Commitment

The top management of Royal Government of Cambodia is responsible for establishing, implementing, monitoring and maintaining ISMS to ensure the administration continuity of Royal Government of Cambodia and to minimize the risk of damage by preventing security incidents and reducing their potential impact under the declaration of GISMS Policy.

Management people are directly responsible for implementing ISMS and especially for ensuring staff compliance in their respective departments.

5.2. Government Information Security Organization

The Ministers of Royal Government of Cambodia shall assign Government Chief Information Officer (GCIO) for each ministry. The top of Royal Government of Cambodia shall establish Government Chief Information Officer Committee (GCIO Committee). Government Information Security Office (GIS Office) is set up as a secretary at GCIO Committee and NiDA takes the role of GIS Office as part of its responsibility. *This clause is a draft. GCIO patronage will be settled in GCIO development project.*

The top management of each government organization shall assign Chief Information Security Officer (CISO) and he/she establishes Information Security Office (IS Office).

5.3. <u>Capacity Development</u>

Information security capacities are defined as follows and they are enhanced by the management of GIS Office as a center of excellence.

Information Security Capacity Categories:

1. Information Security Management System
2. Network Infrastructure Security
3. Application Security
4. OS Security
5. Firewall
6. Intrusion Detection
7. Virus
8. Secured Programming Techniques
9. Security Operation
10. Security Protocol
11. Authentication
12. PKI (Public Key Infrastructure)
13. Encryption
14. Electronic Signature
15. Unauthorized Access
16. Legislation, Norms

5.4. <u>Management Review</u>

GCIO is required to review all processes of ISMS of all government organizations and GIS Office is authorized to request all government organizations to report their ISMS status.

CISO and IS Office at each government organization is required to operate the equivalent review which fulfills the requirements of GIS Office and of 4.3 Check (Monitor and Review).

6. Control and Treatment

6.1. <u>Types of Control</u>

There are four types, mitigating risks, transferring risks, avoiding risks and (knowingly and objectively) accepting risks.

Mitigating risks is the major control to take against the revealed risks. A PC is vulnerable against a virus intrusion, for instance, Anti-virus software installation and activation is a control to be taken.

Transferring risks is the administratively possible way of control. Assume a PC contains valuable information and it is vulnerable against a fire disaster. Then, the data back up in a remote place is a control of mitigating risks, on the other hand, enrolling a fire insurance and insuring the damage of lost data is a control of transferring risks.

Avoiding risks is the alternative to vanish the source of risks. The previous research collected lots of privacy information which is irrelevant to the main business and it is vulnerable to information leakage, then, disposing the information safely is a control of avoiding risks.

(Knowingly and objectively) accepting risks is the last option. For example, it is widely applied to protect a LAN by setting up a firewall whereas a web server for external users is set up out of a firewall. It is accepted the web server might be attacked from outside although it needs some recovery efforts once an attack happens. Accepting risks has to be very carefully managed and the top management review and authorization is always required.

6.2. Control and Treatment by Information Asset

Most of controls and treatments is a type of mitigating risks. Major controls and treatments are seen in Risk Check Book and a sample GIS Rule Book, respectively. New controls and treatments are preferably in placement by ministry, and they must be clearly reported at the time of GIS Office approval.