PART II
GISMS1.0 (released in November 2008)

SECTION 1
Government Information Security Management System

- Drafted by Yusuke Tanaka, JICA Expert
- Edited by ICT Security Management Technical Team (iSMTT).

NiDA

Government
Information Security Management System

The Project of
Capacity Development on ICT Management at NiDA

H.E. CHEA MANIT, Deputy Secretary General
Mr. TANAKA YUSUKE, JICA Expert
November, 2008

Government

Information Security Management System

(GISMS)

Development Project

Introduction

GISMS

Government Information Security Management System (GISMS) is for Royal Government of Cambodia to secure information used in its business operations, to ensure the administration continuity in Royal Government of Cambodia and to minimize the risk of damage by preventing security incidents and reducing their potential impact. GISMS has the following characteristics;

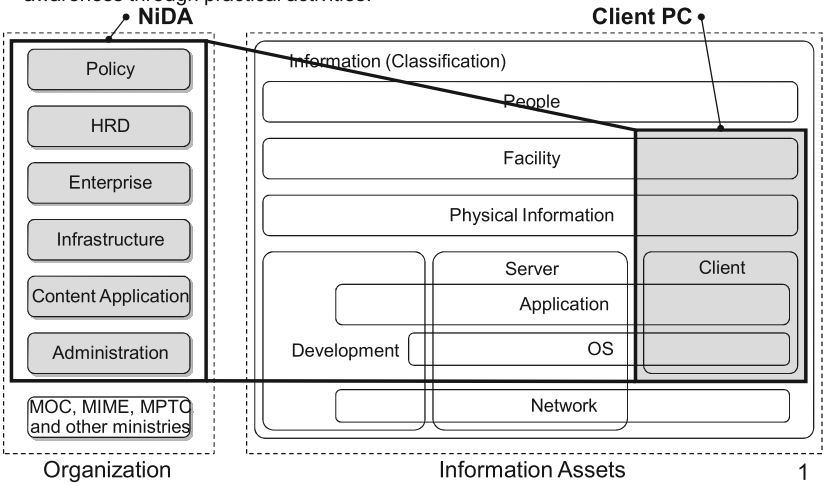
- Based on the best practices of global standard ISO/IEC27001
  - Accumulation of good practices and knowledge of information security
  - Ease of adoption of ISO/IEC27001 to any organization because of its applicability of tasks stipulated
  - Continuous revision

- Process-based
  - Applicable regardless of organization's structure
  - Applicable regardless of organization's size and/or nature
- PDCA approach
  - Plan/Do/Check/Action
  - Step by step and spiral evolution

2

GISMS Development Scope

The scope is carefully focused to realize PDCA cycle under the severe time constraint. The Client PC is selected due to its vulnerability and the ability to raise all officials awareness through practical activities.

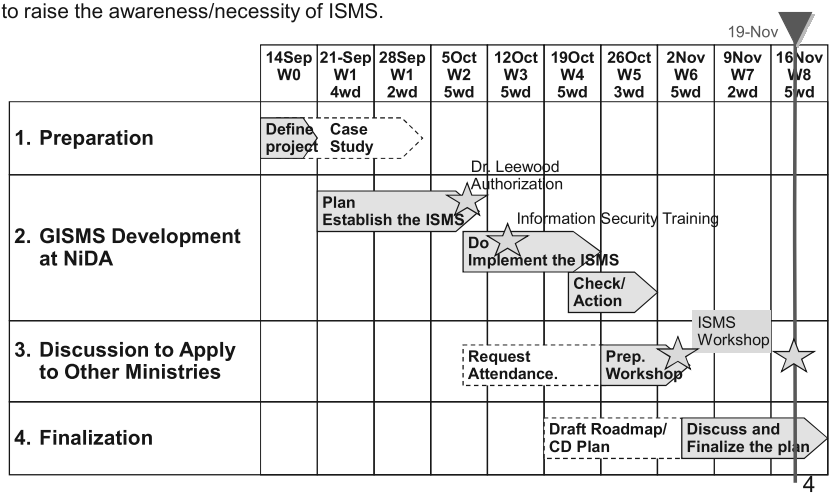


1

GISMS Development Project Schedule

It is scheduled to quickly realize PDCA cycle of ISMS.

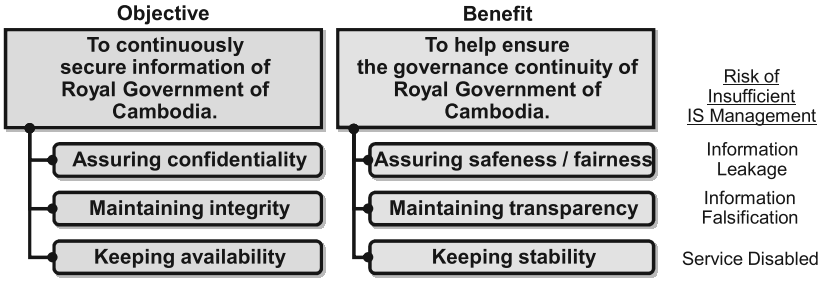
It is set up a workshop with other ministries to share the ISMS development experience, and to raise the awareness/necessity of ISMS.



Government
Information Security Management System
(GISMS)

5

GISMS (Government Information Security Management System) in Brief



Characteristic

- GISMS is based on ISO27001, the global standard.
- Top-Down approach gets GISMS the most effective as the indispensable and mandatory business.
- PDCA (Plan-Do-Check-Action) cycles can gradually enhance information security step by step.
- Government unified ISMS can keep the better level of information security, by researching private and public sectors in Cambodia and by considering the global trends, with the minimum power.

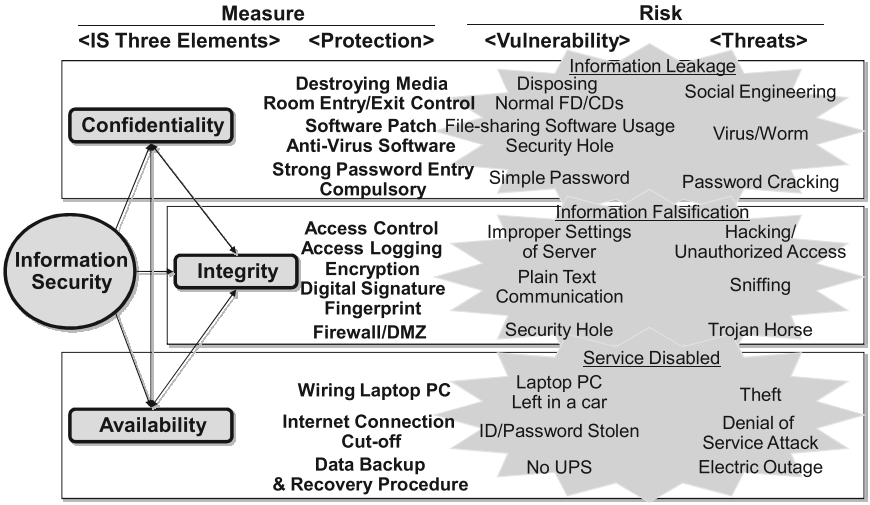
Risk Evidence

- RGC is being increasingly exposed to the cyber attacks of outsiders as it utilizes IT and internet more as identified the notably high ratio of virus infection reaching 35%.

6

Risks and Measures Example

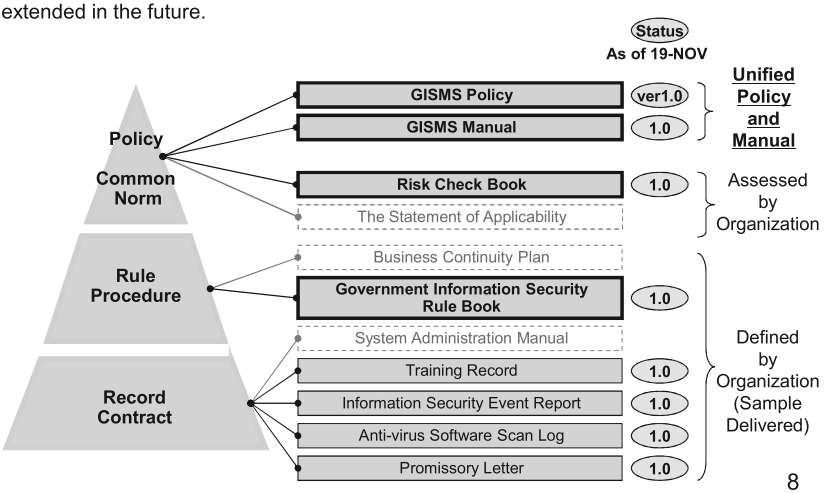
There exist present and clear dangers of information security and it needs to react proactively.



7

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.



8

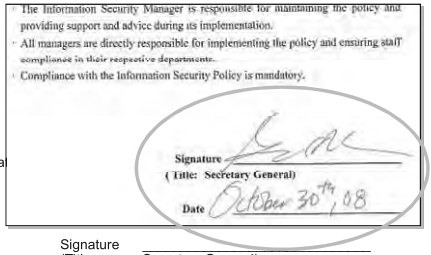
GISMS Policy

[Objective]

- The objective of information security is to ensure the administration continuity in the government of Kingdom of Cambodia and to minimize the risk of damage by preventing security incidents and reducing their potential impact.

[Policy]

- The goal of ISMS Policy is to protect the information assets in the government of Cambodia against all internal, external deliberate or accidental treats.
- The security policy ensures that
  - Information will be protected against any unauthorized access;
  - Confidentiality of information will be assured;
  - Integrity of information will be maintained;
  - Availability of information for administration processes will be maintained;
  - Legislative and regulatory requirements will met;
  - Information security training will be available for all government officials;
  - All actual or suspected information security breaches will be reported to the Information Security Manager and will be thoroughly investigated.
- Procedures exist and support the policy, including virus control treatments and passwords.
- Administrative requirements for availability of information and systems will be met.
- The Information Security Manager is responsible for maintaining the policy and providing support and advice during its implementa
- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.
- Compliance with the Information Security Policy is mandatory.



Signature _____
(Title: Secretary General)

Date _____

9

GISMS Manual Contents

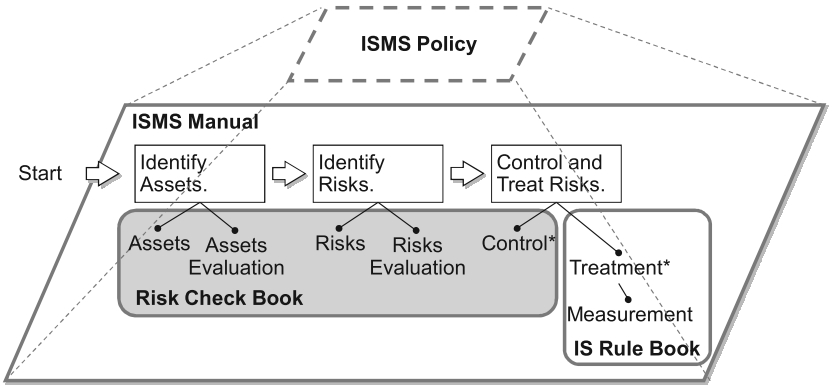
Government Information Security Management System (GISMS) Manual is defined only one among all ministries of Royal Government of Cambodia. The initial version of GISMS manual is focused on **Plan (Establish) ISMS**. (pink shaded part)

1. Introduction
2. Scope
3. Normative References, Terms and Definition
4. **Government Information Security Management System (GISMS)**
4.1. **Plan (Establish)**
4.1.1. **Walkthrough ISMS Policy and ISMS Manual**
4.1.2. **Define the Scope and Boundaries of the ISMS**
4.1.3. **Assess Risks**
4.1.4. **Define an Information Security Rule Book**
4.1.4.1. **Define the Scope of the ISMS of IS Rule Book**
4.1.4.2. **Identify the non-applicable rule /procedure in a sample rule book**
4.1.4.3. **Modify rules and procedures in a sample rule book**
4.1.5. **Obtain approvals**
4.2. Do (Implement and Operate)
4.3. Check (Monitor and Review)
4.4. Action (Maintain and Improve)
4.5. Document Control
4.6. Record Control
5. Management Responsibility
6. Controls and Treatment

10

Risk Check Book

Risk Check Book is applied to all government ministries when to assess their ISMS scope. It contains Assets evaluation, Risks evaluation and Controls.

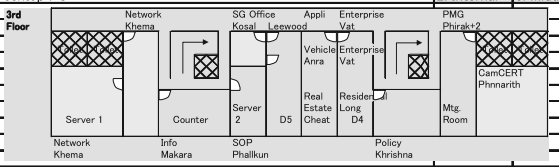


*Control and Treatment are also called Measure.

11

Risk Check Book – Step1. Identify Assets

Risk Check Book is applied to all government ministries when to assess their in-scope information assets. First of all, Identify assets. Risk Check Book has 6 default assets. 4 assets out of 6, Facility, Paper, Client PC, and Network & server assets are supposed to be defined by department for each to check by itself. Just copy and insert a group of rows (e.g. #50-68 is a group of rows for Client PC) and fill out whose assets they are. It is useful to prepare an office map for the later assessment.

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidentiality	Integrity	Availability	Total
1	Basic Check List							
2	**NiDA, CISO**							
50				Client PC (hardware and software)				
51				Desktop PC	2: Internal	3: Middle	1: Low	1: Low
52								
53								
54								
55								
56								
57								
58								
59								
60								
61								
62				Laptop /mobile PC (All desktop PC check items must be applied.)	2: Internal	3: Middle	1: Low	1: Low
63								
64				Storage devices (Portable HDDs /Memory sticks /Memory cards)	2: Internal	3: Middle	1: Low	1: Low
65								
66								
67				Personal asset (Personally owned PC, storage devices and digital archives)	2: Internal	3: Middle	1: Low	1: Low
68								

12

Risk Check Book – Step2. Evaluate Assets

Next step is to evaluate assets. There are 3 elements of evaluation, Confidentiality, Integrity and Availability. Select one class of each according to the criteria. Just select one from the pull down menu. Use a default value if you feel difficult to evaluate.

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidentiality	Integrity	Availability	Total
1	Basic Check List							
2	**NiDA, CISO**							
50				Client PC (hardware and software)				
51				Desktop PC	2: Internal	3: Middle	1: Low	1: Low
52								
53				**1: Confidentiality evaluation**				
54				# / Class / Evaluation / Description				
55				C1 / 1: General / 1 / Open information assets which go to public				
56				C2 / 2: Internal / 2 / Information used only in a government business operation				
57				C3 / 5: Confidential / 5 / Confidential among limited authorized people				
58								
59				**2: Integrity evaluation**				
60				# / Class / Evaluation / Description				
61				I1 / 1: Low / 1 / No impact on business continuity by falsification				
62				I2 / 3: Middle / 3 / Operational cost impact by falsification				1: Low
63				I3 / 5: High / 5 / Political impact by falsification				
64								1: Low
65				**3: Availability evaluation**				
66				# / Class / Evaluation / Description				
67				A1 / 1: Low / 1 / Out of service allowed over twenty four hours				1: Low
68				A2 / 3: Middle / 3 / Out of service allowed up to twenty four hours				
				A3 / 5: High / 5 / Out of service allowed up to four hours				

13

Risk Check Book – Step2. Evaluate Assets

Then, the spreadsheet automatically display the total evaluation of an asset according to the total points of 3 elements. Review and revise confidentiality, integrity and availability evaluation if you feel a total asset value is different from actual.

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidentiality	Integrity	Availability	Total
1	Basic Check List							
2	**NiDA , CISO**							
50				Client PC (hardware and software)				
51				Desktop PC	2: Internal	3: Middle	1: Low	1: Low
52								
53								
54								
55								
56								
57								
58								
59								
60								
61								
62				Laptop /mobile PC (All desktop PC check items must be applied.)	2: Internal	3: Middle	1: Low	1: Low
63								
64				Storage devices (Portable HDDs /Memory sticks /Memory cards)	2: Internal	3: Middle	1: Low	1: Low
65								
66								
67				Personal asset (Personally owned PC, storage devices and digital archives)	2: Internal	3: Middle	1: Low	1: Low
68								

4: Asset evaluation (Points = Confidentiality + Integrity + Availability)

#	Class	Evaluation	Points	Description
As1	1: Low	1	3 to 6	Assets to impact moderately on an operation
As2	2: Middle	2	7 to 12	Assets to impact enormously on an operation
As3	3: High	3	13 to 15	Assets to impact enormously on an governing

automatic

Risk Check Book – Step3. Check Assets

Check assets. Just select Yes or No for each check item.

5: Check results

#	Class	Evaluation		Description
Ch1	0: Yes / NA	0		Correct operation
Ch2	1: No	1		Risk implication

	Check item Check Type	Check item	Check results
51			
52	Assignment	Assign one main user at minimum to all PCs.	1: No
53	User ID and password	Use a robust password and change one periodically.	1: No
54	User ID sharing	Prohibit share user ID and password with several people.	1: No
55	Cleared screen	Clear a display screen by setting screen saver function with password.	1: No
56	Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No
57	Anti-virus protection	Use an automatic virus detection function usually.	1: No
58	Anti-virus protection	Update a virus definition file periodically.	1: No
59	Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No
60	UPS	Connect UPS for all desktop PCs.	1: No
61	Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No
62			
63	Security wire	Wire all laptop /mobile PCs physically to desks or store at a locked facility.	1: No
64			
65	Anti-virus protection	Scan storage devices with anti-virus software periodically.	1: No
66	Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No
67			
68	Permission	Get a permission from IS manager to take in/out a personal asset to/from an office.	1: No