Contents

Note:

All rights are reserved to National Information Communications Technology Development Authority (NiDA). The material in this publication is copyrighted. Copying and/or transmitting of portions or all of this publication may not be allowed without permission of NiDA.

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

1

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;

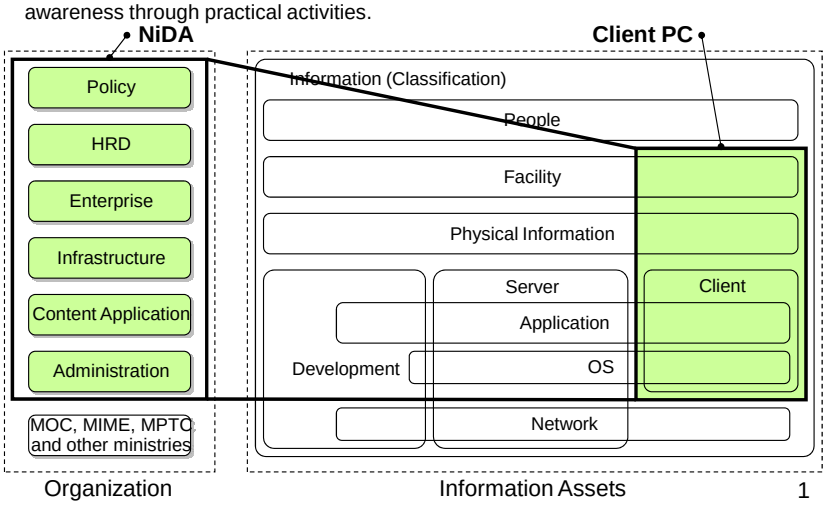
- Based on the best practices of global standard ISO/IEC27001
  - Accumulation of good practices and knowledge of information security
  - Ease of adoption of ISO/IEC27001 to any organization because of its applicability of tasks stipulated
  - Continuous revision

- 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

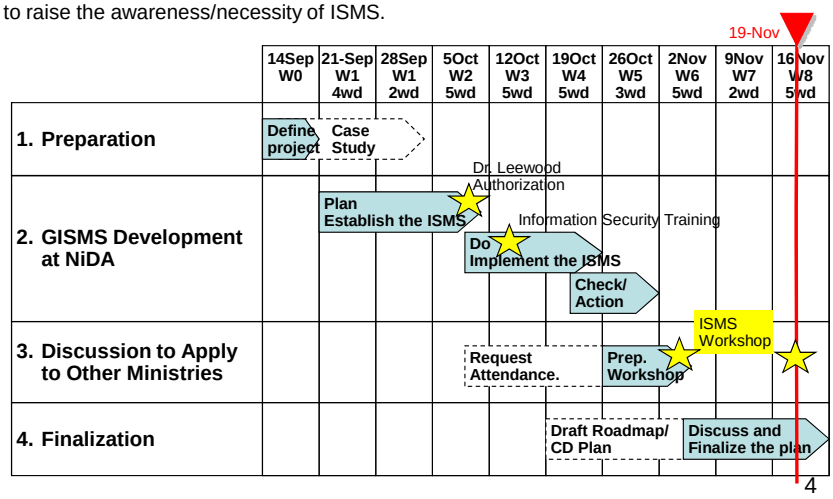
The scope is carefully focused to realize PDCA cycle under the severe time constraint. The Client PC is selected due to its vulnerability and the ability to raise all officials awareness through practical activities.



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.

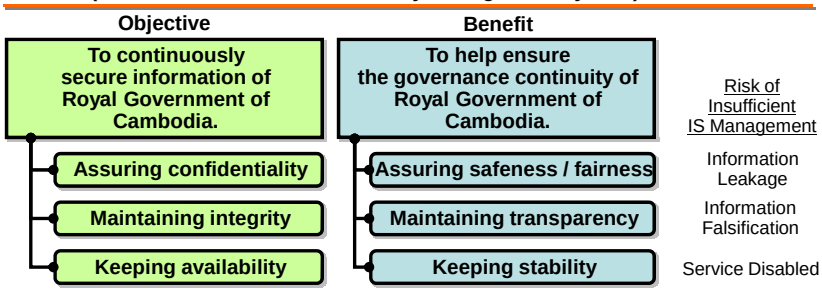


4

Government
Information Security Management System
(GISMS)

5

GISMS (Government Information Security Management System) in Brief



Characteristic

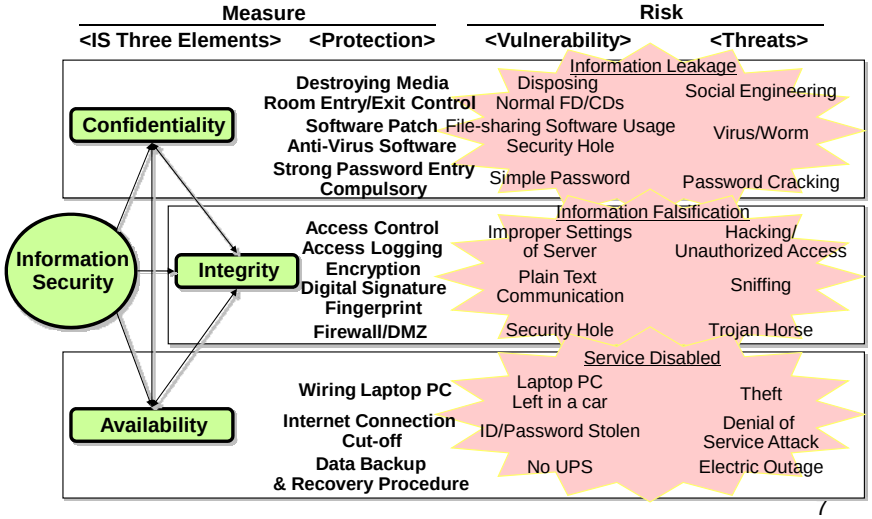
- GISMS is based on ISO27001, the global standard.
- Top-Down approach gets GISMS the most effective as the indispensable and mandatory business.
- PDCA (Plan-Do-Check-Action) cycles can gradually enhance information security step by step.
- Government unified ISMS can keep the better level of information 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%.

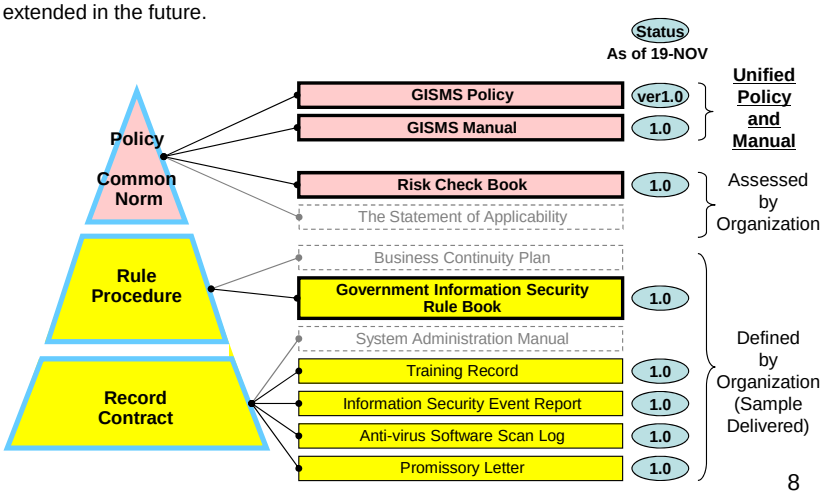
Risks and Measures Example

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



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.



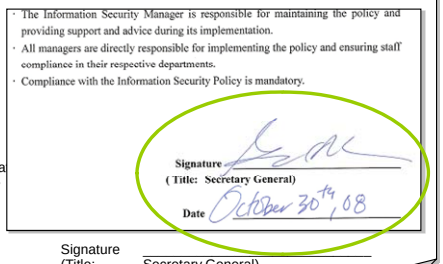
GISMS Policy

[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.


· The Information Security Manager is responsible for maintaining the policy and providing support and advice during its implementation.
· 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 October 30th, 08

Signature
(Title: Secretary General)

Date

GISMS Manual Contents

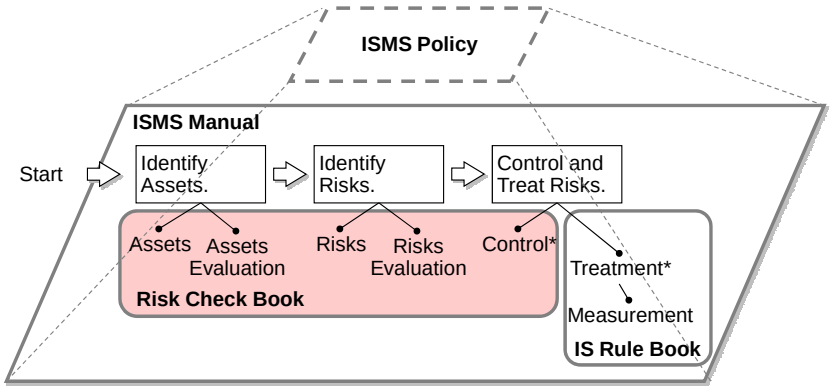
Government Information Security Management System (GISMS) Manual is defined only one among all ministries of Royal Government of Cambodia. The initial version of GISMS manual is focused on **Plan (Establish) ISMS**. (pink shaded part)

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.

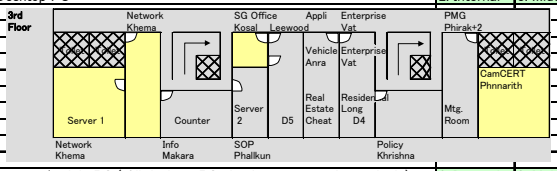


*Control and Treatment are also called Measure.

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 archiv	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					2: Internal			
54					1: General			
55					2: Internal			
56					5: Confidential			
57								
58								
59								
60								
61								
62								1: Low
63								
64								1: Low
65								
66								
67								1: Low
68								

1: Confidentiality evaluation

#	Class	Evaluation		Description
C1	1: General	1		Open information assets which go to public
C2	2: Internal	2		Information used only in a government business operation
C3	5: Confidential	5		Confidential among limited authorized people

2: Integrity evaluation

#	Class	Evaluation		Description
I1	1: Low	1		No impact on business continuity by falsification
I2	3: Middle	3		Operational cost impact by falsification
I3	5: High	5		Political impact by falsification

3: Availability evaluation

#	Class	Evaluation		Description
A1	1: Low	1		Out of service allowed over twenty four hours
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 archiv	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

Risk Check Book – Step4. Evaluate Risks

Evaluate Threat and Vulnerability to apply the criteria. Total Risk is automatically displayed.

8: Risk evaluation (Points = (Asset + Threat) * Vulnerability)

#	Class	Evaluation	Points	Description
R1	1: Low	1	2 to 6	Allowed Risk
R2	2: High	2	8 to 24	Non allowed risk which needs controlled

Risk Evaluation

	Threat	Comments on Threat	Vulnarability	Total Risk
51				
52	2: Middle	Unauthorized access, falsification, malfunction	3: Middle	2: High (9pt)
53	2: Middle	Unauthorized access, falsification, malfunction	3: Middle	2: High (9pt)
54	2: Middle	Unauthorized access, falsification, malfunction	3: Middle	2: High (9pt)
55	2: Middle	Unauthorized access, falsification, malfunction	3: Middle	2: High (9pt)
56	2: Middle	Unauthorized access, falsification, malfunction	3: Middle	2: High (9pt)
57	2: Middle	Unauthorized access, falsification, malfunction	3: Middle	2: High (9pt)
58	2: Middle	Unauthorized access, falsification, malfunction	3: Middle	2: High (9pt)
59	2: Middle	Unauthorized access, falsification, malfunction	3: Middle	2: High (9pt)
60	2: Middle	Circuit breaker down	3: Middle	2: High (9pt)
61	2: Middle	Information leak	3: Middle	2: High (9pt)
62				

automatic

6: Threat evaluation

#	Class	Evaluation		Description
T1	1: Low	1		Low probability of the threat
T2	2: Middle	2		Middle probability of the threat
T3	3: High	3		High probability of the threat

7: Vulnerability evaluation

#	Class	Evaluation		Description
V1	1: Low	1		Controlled enough to secure against a threat
V2	2: Fair	2		Controlled but opportunities to improve
V3	3: Middle	3		Controlled proportionally but needed to improve
V4	4: High	4		Non controlled against a threat

16

Risk Check Book – Step 5. Decide Controls

All check items evaluated as “High” risks are requested to control them. There are four types, mitigating risks, transferring risks, avoiding risks and (knowingly and objectively) accepting risks.

Generally, they needs to implement rules and procedures to mitigate risks. Therefore, it leads to develop Government Information Security Rule Book. (See the next section.)

After deciding controls and making treatments to risk items (e.g. define rules and procedures in GIS Rule Book), evaluate risks again and make sure all check items get evaluated as “Low”.

	Control		Risk Evaluation after Control		
	Control Contents	References	Threat	Vulnarability	Total Risk
51					
52	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
53	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
54	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
55	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
56	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
57	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
58	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
59	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
60	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
61	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
62					
63	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
64					
65	Implement Rule and Procedures..	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
66	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)
67					
68	Implement Rules.	GIS Rule Book	2: Middle	1: Low	1: Low (3pt)

17

Government Information Security (GIS) Rule Book Contents

GIS Rule Book is defined by ministry. The following introduces NiDA GIS Rule Book. It is the specific rule which needs to be done internally and it will be added in the future to get more secured environment. It can be copied and modified for each ministry GIS Rule Book. The initial version of Information Security Rule Book is focused on **client PC security**. (pink shaded part)

Client PC Security Rule – Desktop PC

This page is cited from Government Information Security Rule Book.

Desktop PC

Virus Protection

(a5) Viruses are a major threat to NiDA and client PCs are particularly vulnerable if their anti-virus software is not kept up-to-date. The virus definition file MUST be updated at least weekly. The easiest way of doing this is simply to log on to the LAN for the automatic update process to run. If you cannot log on for some reason, contact Information Security Office for advice on obtaining and installing anti-virus updates.

(a6) Always virus-scan any files downloaded to your computer from any source (FD/CD/DVD, USB hard disks and memory sticks, network files, e-mail attachments or files from the Internet). Virus scans must be set to happen automatically. It is also required to initiate scheduled scans at least weekly.

(a7) Report any information security events (such as virus infections) promptly to Information Security Office in order to minimize the damage.

(a8) Respond immediately to any virus warning message on your computer, or if you suspect a virus (e.g. by unusual file activity) by contacting Information Security Office. Do not forward any files or upload data onto the network if you suspect your PC might be infected.

Procedure

Virus Detection Handling

Step	Description	Owner	Records
b2.1	Detect an information security event such as virus detection.	Official	n/a
b2.2	Physically off-line from a network immediately.	Official	n/a
b2.3	Inform ISO immediately when the event happens.	Official	Information Security Event Report
b2.4	Analyze the effects of an event and take an appropriate action.	ISO	n/a
b2.5	Terminate any network/application services if necessary.	ISO	n/a
b2.6	Execute an emergent anti-virus protection procedure if necessary.	ISO	n/a
b2.7	Record an analysis and an action in a report.	ISO	(Updated) Information Security Event Report
b2.8	File a report and keep for the defined period.	IS In-charge	n/a

20

Records – Information Security Event Report

All information security events should be reported and handled appropriately by the in-charge personnel.

Information Security Event Report

Reporter

Name: [

Department: [

Contact (Cell/E-mail) **: [**

Event Type: Virus detection ☐
Inappropriate settings/installatio
Undesirable/unsavory e-mail de
Others ☐

Event Time: [
Situation:

Reported | Record Number:

Name: [ ]

Department: [ ]

Reported Time: [ ]

Action:

Lessons Learned

Name: [ ]

Department: [ ]

Recorded Time: [ ]

Lessons Learned:

21

Three Basic Rule to Secure Information

[Rule 1] Always consider whether you acquire, process or save confidential information. Do NOT expose information against any risks of leakage, falsification and inaccessibility.

[Rule 2] Lock up an office entrance, a cabinet and a desk drawer before walking away for any moment.

[Rule 3] Activate an auto-detection function of anti-virus software. Update a virus definition file at least weekly. Scan a storage device of your PC weekly and any external storage devices (e.g. FD, Memory Card/Stick and HDD) when to connect to your PC.

22

Information Security Management Example – Disciplinary Action

Details of Disciplinary Action taken in May 2007

TO: All XYZ Company People in Japan

Business ethics are critical for our company's success because they build trust and transparency. Trust and transparency, in turn, build the right envir... clients, our suppliers, our stakeholders and the communities in which we... throughout the world.

However unfortuna... ved here and there within the co...

To prever... ulation vi...

Considering insufficient working regulations in Royal Government of Cambodia, GIS Rule Book at the first stage takes no disciplinary actions.

								missal nder struction	Dismissal on disciplinary grounds
Acts of harassment									
Improper/fraudulent claims related to time report								1	
Information security violations	4	7	4		1				
Other		4							
Total	4	15	4		1			1	

23

Information Security Management Example – Software Installation Block

To:All XYZ Company People in Japan

Microsoft is expected to ion of its Internet Explorer browser, som f upgrade to IE7 on y client e ay not

I 7 E om getting in pdate, will be distribut October 25th.

This control requires a technical implementation, and GIS Rule Book at the first stage only defines a recommended rule to get an approval from IS Manager.

24

Information Security Management Example – USB Memory Usage Prohibition

To:All XYZ Company People in Japan

Below are the list of mai Security violations" and related global Security Committ

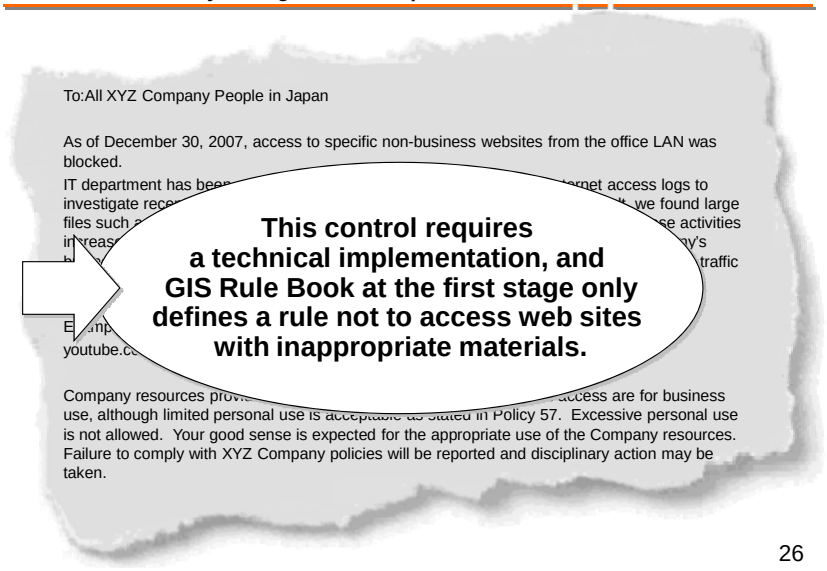
Loss o

This control requires a technical implementation, and GIS Rule Book at the first stage defines a rule to put a strap with a small external device.

Business use of USB me eral rule. However, the security administrator may permit such use as project policy if one of the following conditions is met. 1. If the USB memory has a password protection 2. If the USB memory has a biometric authentication function (fingerprint authentication, etc.) 3. If files are always encrypted or password protected when saved in USB memory.

25

Information Security Management Example – Web Site Access Block



26

Action Plan

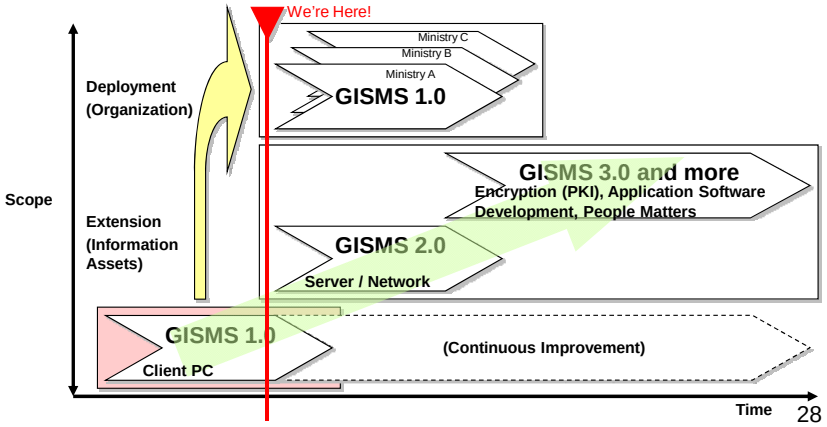
27

Next Step

This project covers only Client PC at NiDA. Call this project as GISMS 1.0.

Then, Deployment to other ministries is its repeating actions.

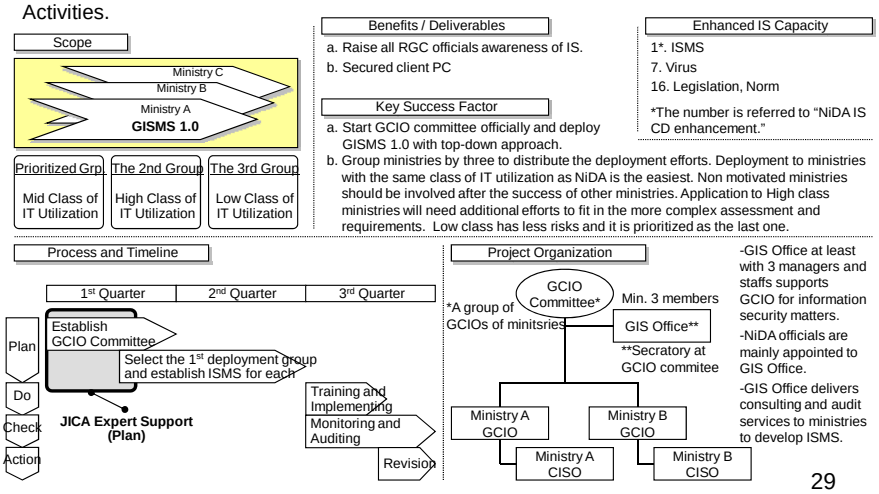
Extend the coverage of information assets such as Server / Network, Encryption (PKI), Application Software Development and People Matters. Business Continuity Plan is another set of actions to be followed later.



28

GISMS 1.0 Deployment

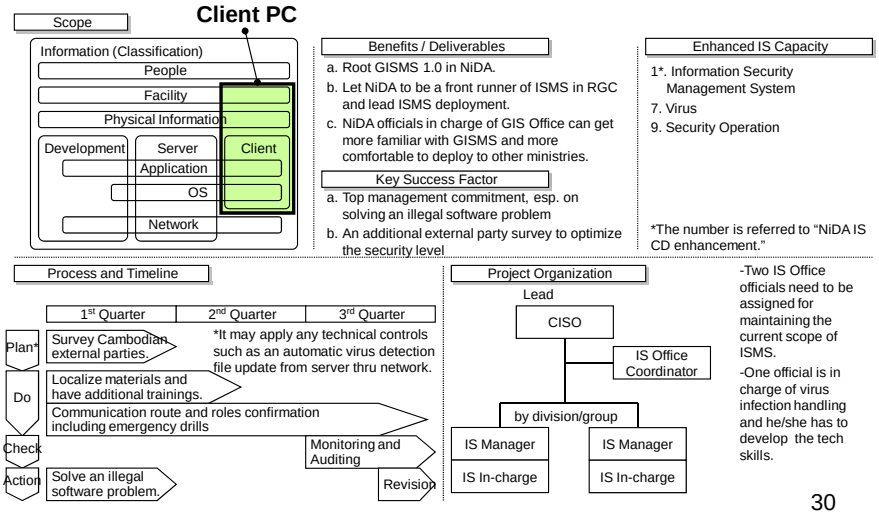
Succeeding the GISMS 1.0 implementation at NiDA, it is recommended to deploy the said GISMS 1.0 to all other ministries as part of GCIO (Government Chief Information Officer) Activities.



29

GISMS 1.0 Continuous Improvement

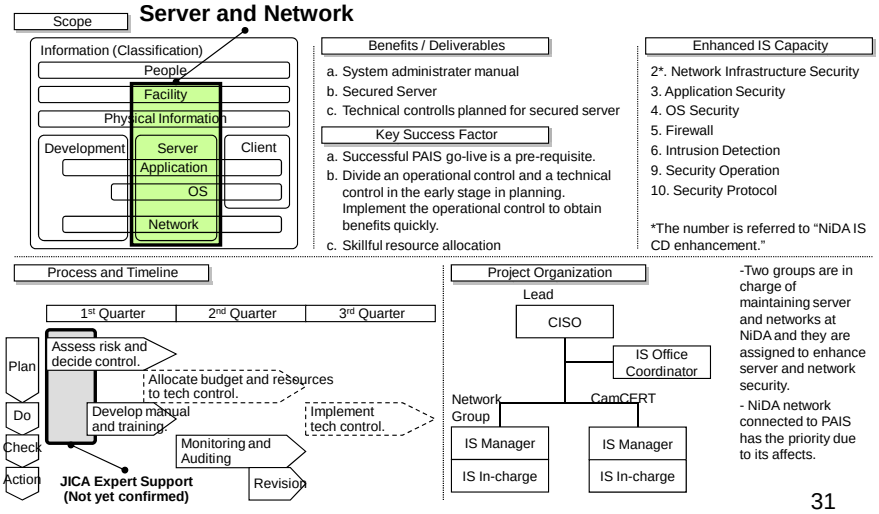
GISMS 1.0 at NiDA needs to be continuously improved as described formerly.



30

GISMS 2.0 Extension

The next PDCA cycle as GISMS 2.0 is recommended to target on Server and Network.



31

NiDA Information Security Capacity Development Enhancement

NiDA is to enhance information security capacity according to the defined actions.

	Capacity Category*	Before GISMS	GISMS 1.0 Develop.	GISMS 1.0 Deploy.	GISMS 2.0 Develop.	GISMS 3.0 Develop.
1	Information Security Management System	Level 1	Level 2	Level 3	Level 3	Level 3
2	Network Infrastructure Security	Level 1	Level 1	Level 1	Level 2	Level 2
3	Application Security	Level 0	Level 0	Level 0	Level 1	Level 1
4	OS Security	Level 0	Level 0	Level 0	Level 1	Level 1
5	Firewall	Level 1	Level 1	Level 1	Level 2	Level 2
6	Intrusion Detection	Level 1	Level 1	Level 1	Level 2	Level 2
7	Virus	Level 1	Level 1	Level 2	Level 2	Level 2
8	Secured Programming Techniques	Level 0	Level 0	Level 0	Level 0	Level 0
9	Security Operation	Level 1	Level 1	Level 1	Level 2	Level 2
10	Security Protocol	Level 0	Level 0	Level 0	Level 1	Level 1
11	Authentication	Level 0	Level 0	Level 0	Level 1	Level 2
12	PKI (Public Key Infrastructure)	Level 0	Level 0	Level 0	Level 1	Level 2
13	Encryption	Level 0	Level 0	Level 0	Level 1	Level 2
14	Electronic Signature	Level 0	Level 0	Level 0	Level 1	Level 2
15	Unauthorized Access	Level 1	Level 1	Level 1	Level 1	Level 1
16	Legislation, Norms	Level 1	Level 1	Level 2	Level 2	Level 2

*Capacity categories are defined in Information Security Skill Map Survey of IPA, Mar-2004.

32

NiDA Information Security Capacity Category and Level

Capacity category and level* are defined as below.

There are 16 categories and 102 sub categories.

1. Information Security Management System
Management Techniques, Risk Analysis Techniques, Information Security Policy, Information Security Audit, Relevant Knowledge

2. Network Infrastructure Security
Network Design Techniques, Network Access Protocol, VPN(Virtual Private Network), Wireless LAN

3. Application Security
Threats against Web Server, Security Measures of Web Server, Operation of Web Server, Web Application Design, Web Browser Security, Basic Knowledge of Web Related Protocol

4. OS Security
Log Control, Patch Application Control, Service Control, File System Control, Account Control

5. Firewall
Firewall Installation and Operation, NAT(Network Address Translation), Network Access Control

6. Intrusion Detection
Intrusion Detection System Installation and Operation, Intrusion Detection System Function, Detection Algorithm, Detection Subject, Intrusion Detection System

7. Virus
Communication Route, Policy after Infection, Policy for Prevention, Virus Attack, Detection and Cleansing, Infection, Virus Types

Level Description

Level 0: No knowledge, no experience,

Level 1: Understanding a basic knowledge, being able to acquire detailed technical contents through experience,

Level 2: Putting an acquired knowledge into practice under supervision, being able to explain a detailed technical content referring to an experience,

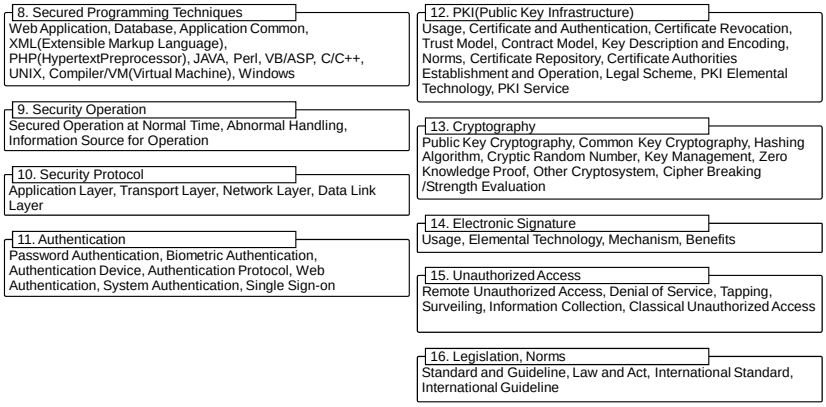
Level 3: Putting knowledge into practice autonomously, being able to use and advise technical know-hows referring to various experiences.

*Capacity category and level are defined in Information Security Skill Map Survey of IPA, Mar-2004.

33

NiDA Information Security Capacity Category and Level (Con.)

Capacity category and level* are defined as below.
There are 16 categories and 102 sub categories.



*Capacity category and level are defined in Information Security Skill Map Survey of IPA, Mar-2004.

34

Key Take-Away

Five points we should know in GISMS:

1. **Its documents include GISMS Policy, GISMS Manual, Risk Check Book, and GIS Rule Book.**
   a. **GISMS Policy** declares the top management commitment of implementing GISMS.
   b. **GISMS Manual** defines the unified approach of GISMS for all ministries concerned.
   c. **Risk Check Book** enables all ministries to assess their risks in the same criteria.
   d. **GIS Rule Book** implements GISMS at each ministry.
2. **Top management commitment**
   Top management commitment is indispensable to root ISMS in each ministry.
3. **All officials involvement**
   All officials are strongly expected to set their mindset to keep information security rules and procedures, and do information security related work in their daily operation.
4. **Technology utilization**
   Technology optimizes the information security risk mitigation and partly lessens officials hand work efforts. This will be challenged in the next cycle of ISMS.
5. **Continuous improvement**
   All managers and above are obliged to supervise the implementation of ISMS at their department/group completely with continuous improvement.

35

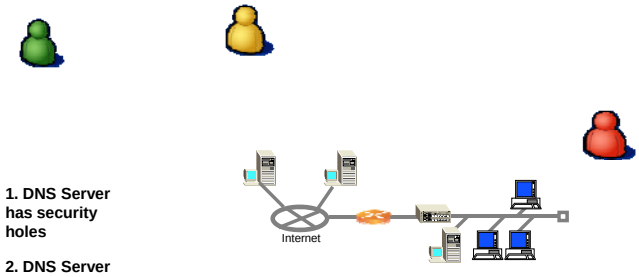
Appendix

36

Image of Vulnerable Servers Spreading Out Viruses

Nice to Have

Assume vulnerable DNS server hacked by unauthorized users from internet.



1. DNS Server has security holes

2. DNS Server hacked by ...

3. DNS cache table falsified ...

4. LAN user access to Internet

5. DNS designates wrong IP address (DNS Spoofing)

6. Malicious site sends malware in HTML.

7. Malware successfully hiding unless anti-virus software detects.

8. Malware search cookies with credit card id/password.

9. Malware sends the information to their sites.

10. Malware sends the information to xxx site.

11. The information is sold to other parties.

12. They buy goods paying by fraud credit card information.

13. LAN user gets financial damage.

37

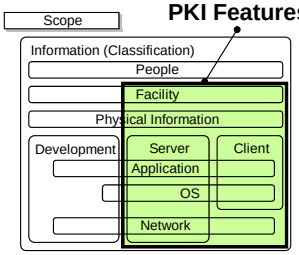
GISMS 3.0 Extension

Nice to Have

XXX

PKI Features

Scope



Benefits / Deliverables

a. XXX system
b. User manual

Key Success Factor

Enhanced IS Capacity

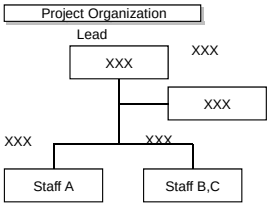
1. Information Security Management System
7. Virus
9. Security Operation

*The number is referred to "NiDA IS CD enhancement."

Process and Timeline*

*Timeline described on full time basis

Project Organization



- XXX

38

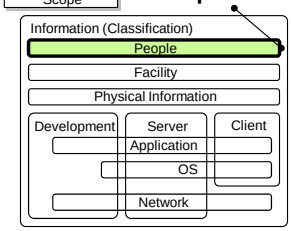
GISMS X.X Extension

Nice to Have

XXX

People Matters

Scope



Benefits / Deliverables

a. Hiring/Resigning procedure
b. Personal profiling related to information security

Key Success Factor

Enhanced IS Capacity

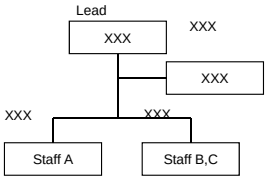
1. Information Security Management System
9. Security Operation
(NA) General Administration related to information security

*The number is referred to "NiDA IS CD enhancement."

Process and Timeline*

*Timeline described on full time basis

Project Organization



- XXX

39

SECTION 2
Government Information Security Management System Policy

Kingdom of Cambodia
Government Information Security Management System 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 implementation.
- 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 October 30th, 08

SECTION 3
Government Information Security Management System Manual

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

1. Introduction

The Government Information Security Management System Manual (GISMS Manual) is defined that Royal Government of Cambodia establishes, implements, checks and takes actions as a body of Government Information Security Management System, under the Government Information Security Management System Policy (GISMS Policy) declared by its Prime Minister, the chief of the government.

2. Scope

GISMS Manual covers all thirty-one government organizations stated as follows;

1. The Office of the Council of Ministers,
2. Ministry of Agriculture Forestry and Fisheries,
3. Ministry of Commerce,
4. Ministry of Culture and Fine Arts,
5. Ministry of Economy and Finance,
6. Ministry of Education Youth and Sports,
7. Ministry of Environment,
8. Ministry of Foreign Affairs and International Cooperation,
9. Ministry of Health,
10. Ministry of Industry Mines and Energy,
11. Ministry of Information,
12. Ministry of Interior,
13. Ministry of Justice,
14. Ministry of Labor and Vocational Training,
15. Ministry of Land Management, Urban Planning & Construction,
16. Ministry of National Defense,
17. Ministry of Parliamentary Affairs and Inspection,
18. Ministry of Planning,
19. Ministry of Post and Telecommunication,
20. Ministry of Public Works and Transport,
21. Ministry of Religions and Cults,
22. Ministry of Rural Development,
23. Ministry of Social Affairs Veteran and Youth Rehabilitation,
24. Ministry of Tourism,
25. Ministry of Water Resources and Meteorology,
26. Ministry of Women Affairs,
27. Municipality of Phnom Penh,
28. Secretariat of Public Service,
29. Secretariat of Civil Aviation,
30. National Information Communications Technology Development Authority (NiDA) and
31. Permanent Mission of the Kingdom of Cambodia to the United Nations.

3. Normative References, Terms and Definition

3.1. Normative References

The following referred documents are indispensable for the application of this document.

ISO/ISE 27001: 2005 Information technology – Security techniques – Information security management systems – Requirements

3.2. Terms and Definition

The followings are the terms and their definitions specifically used in GISMS.

Government Information Security Management System (GISMS):
It is ISMS for Royal Government of Cambodia in this manual. ISMS is referred to ISO/ISE 27001.

Government Information Security Office (GIS Office):
It is set up as a secretary at GCIO Committee and NiDA takes the role of GIS Office as part of its responsibility. It is responsible for setting up the policy, standards and guidelines of GISMS and is also responsible for all ISMS related topics in Royal Government of Cambodia. *This definition is a draft. GCIO patronage will be settled in GCIO development project.*

Chief Information Security Officer (CISO):
It is assigned to one official by ministry. Responsibilities are explicitly defined in GISMS Manual and Information Security Rule Book.

Information Security Manager (IS Manager):
It is assigned by ministry. Responsibilities are explicitly defined in GISMS Manual and Information Security Rule Book.

Risk Check Book:
It is a check book which identifies information assets, evaluates information assets, checks potential risks, identifies risks and evaluates risks.

Government Information Security Rule Book (GIS Rule Book):
It defines rule and procedures which secures each information asset. It is defined by ministry whereas its sample is developed by NiDA and the sample is highly recommended to apply as the minimum level as required to secure information.

4. Government Information Security Management System (GISMS)

GISMS takes the plan, do, check and action (PDCA) cycle as ISO27001 defines. This chapter defines these processes of GISMS.
It also defines document control and record control.

4.1. Plan (Establish)

Plan process consists of 5 sub processes; walkthrough policy and manual, define the scope of GISMS, assessing risks, develop GIS manual and obtain approvals.

4.1.1. Walkthrough GISMS Policy and GISMS Manual

First of all, read GISMS Policy, which declares the objective and policy of Kingdom of Cambodia GISMS. Walkthrough GISMS Manual (this document), which is applied to all government organizations of Kingdom of Cambodia, and which defines the unified rules to mobilize GISMS.

4.1.2. Define the Scope of the ISMS

When a ministry starts developing ISMS, it needs to define the scope for one cycle of PDCA. It is generally applicable to define the scope by physical facilities, such as a land boundary/building. It is also possible to define the

scope by information system network to effectively decide controls and treatments against threats. It needs careful to scope by organization chart, because it sometimes makes difficult to implement. The initial version of GISMS focuses only on Client PC as the minimum subset of fully-scoped ISMS developed in the future.

4.1.3. Assess Risks

Assess Risks procedure consists of five steps; Identify Information Assets, Evaluate Information Assets, Check Potential Risks, Identify Risks and Evaluate risks. The detailed procedure is defined in Risk Check Book. Please refer to an instruction in Risk Check Book. (See Appendix.1 Risk Check Instruction)

Step.1 Identify Assets

Identify assets. Risk Check Book has 6 default assets. 4 assets out of 6, such as Facility, Paper, Client PC, and Network & server assets are supposed to be defined by department for each to check by itself.

Step.2 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 shown below.

1: Confidentiality evaluation				
#	Class	Evaluation		Description
C1	1: General	1		Open information assets which go to public
C2	2: Internal	2		Information used only in a government business operation
C3	5: Confidential	5		Confidential among limited authorized people
2: Integrity evaluation				
#	Class	Evaluation		Description
I1	1: Low	1		No impact on business continuity by falsification
I2	3: Middle	3		Operational cost impact by falsification
I3	5: High	5		Political impact by falsification
3: Availability evaluation				
#	Class	Evaluation		Description
A1	1: Low	1		Out of service allowed over twenty four hours
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

The total evaluation of an asset determines 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.

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

Step.3 Check Assets

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

(Sample check items of Desktop PC)

- ✓ Assign one main user at minimum to all PCs.
- ✓ Use a robust password and change one periodically.
- ✓ Prohibit share user ID and password with several people.
- ✓ Clear a display screen by setting screen saver function with password.
- ✓ Scan a local storage with anti-virus software periodically.
- ✓ Use an automatic virus detection function usually.
- ✓ Update a virus definition file periodically.
- ✓ Keep records of scanning and updating virus definitions.
- ✓ Connect UPS for all desktop PCs.
- ✓ Execute a physical formatting of a storage, or scrap it physically.

Step.4 Evaluate Risks

Evaluate Threat and Vulnerability to apply the criteria. Each check item has an example of threat in a comment column to easily identify the specific threats.

6: Threat evaluation				
#	Class	Evaluation		Description
T1	1: Low	1		Low probability of the threat
T2	2: Middle	2		Middle probability of the threat
T3	3: High	3		High probability of the threat
7: Vulnerability evaluation				
#	Class	Evaluation		Description
V1	1: Low	1		Controlled enough to secure against a threat
V2	2: Fair	2		Controlled but opportunities to improve
V3	3: Middle	3		Controlled proportionally but needed to improve
V4	4: High	4		Non controlled against a threat

The total risk evaluation is determined by the following calculation.

8: Risk evaluation (Points = (Asset + Threat) * Vulnerability)				
#	Class	Evaluation	Points	Description
R1	1: Low	1	2 to 6	Allowed Risk
R2	2: High	2	8 to 24	Non allowed risk which needs controlled

Step.5 Decide Controls

All check items evaluated as “High” risks are requested to control them. Generally, they need to implement rules and procedures to mitigate risks. Therefore, it leads to develop Government Information Security Rule Book. After deciding controls and making treatments to risk items (e.g. define rules and procedures in GIS Rule Book), evaluate risks again and make sure all check items get evaluated as “Low”.

4.1.4. Develop a Government Information Security Rule Book

GIS Rule Book is defined by ministry. Based on the results of a risk assessment, the major treatment is to define rule and procedures to mitigate revealed risks. GIS Rule Book must contain the following five components; Scope defined at Scetion.4.1.2 Define the Scope of ISMS, Information Security Organization, Rule and Procedures, Information Security Training, and Measurement for Check and Action. A sample GIS Rule Book for a

ministry is obliged to use, which is issued by GIS office whose role will be described in Chapter.5 Management Responsibility. The following three steps explain the tips to develop GIS Rule Book.

4.1.5. Define the Scope of the ISMS in GIS Rule Book

The scope of ISMS defined at Section.4.1.2 is documented in GIS Rule Book where it is recommended to clarify the information assets and their related physical locations /organizations /officials as their example can be shown in a sample rule book.

4.1.5.1. Identify the non-applicable rule /procedure in a sample rule book

The rules and procedures depend on the information assets and their confidentiality in scope of each ministry. They do not need to be defined unless the targeted information assets exist in the scope.

4.1.5.2. Modify rules and procedures in a sample rule book.

They need to define more secured if the information dealt in a ministry is more confidential according to the results of a risk assessment. They need to add to be defined if a sample rule book does not contain the in-scoped information assets. In the latter case, it is recommended to discuss with GIS Office before starting to define rules and procedures, in order to decide who defines the standard of newly in-scoped information assets of RGC.

4.1.6. Obtain approvals

There are two steps of approvals; one is approved by the top management of ministry and the other is done by GIS office.

Once all steps from section.4.1.1 to 4.1.4 are completed and the risk check book and GIS rule book which includes CISO and IS manager assignment are fully documented, those planning process and documents shall be reviewed and approved by GIS Office first in order to assure the compliance with GISMS.

The very exceptional case allows accepting a risk as a residual risk although it exceeds the accepted level in the automated risk evaluation in Risk Check Book. It needs a well organized reasons and decision making to get an approval of GIS Office.

The approval of the top management of ministry is a MUST to implement fully and effectively at the ministry.

4.2. Do (Implement and Operate)

The first thing to do when implementing ISMS at a ministry is to establish ISO. Then, CISO assigns some of ISO members to prepare for and conduct an information security training. The ISMS is a “management” system, therefore, it is recommended higher ranked people get training first, get familiar with ISMS and lead their officials to implement ISMS.

4.3. Check (Monitor and Review)

It needs a long way to go that ISMS is rooted in an organization. Continuous efforts and improvements are required.

In order to grasp the objective status and to discuss any improvements, the

measurement must be installed which are defined in GIS Rule Book.
An internal audit to survey on the effectiveness of implemented ISMS is also requested to find issues to achieve the level of risks in the planning process and/or to review the accepted level of risks. The results of risk evaluation must be updated in Risk Check Book.
The frequency of Check and Action must be defined in GIS Rule Book, however, it has to be at least once a year or more.

4.4. Action (Maintain and Improve)

The results of the measurement and the internal audit lead to decide actions to improve the effectiveness of ISMS and optimize the accepted level of risks. Those actions are not only enhancements of rule and procedure but also treatments to install new software/hardware to protect a network/system. The actions may contain to abolish some rule and procedure to match with the change of a ministry role and business operation.

4.5. Document Control

This section defines GISMS document structure, authorization, revision, distribution, access and keeping.

4.5.1. Document Structure and Authorization

GISMS has four major documents;

1) GISMS Policy
2) GISMS Manual

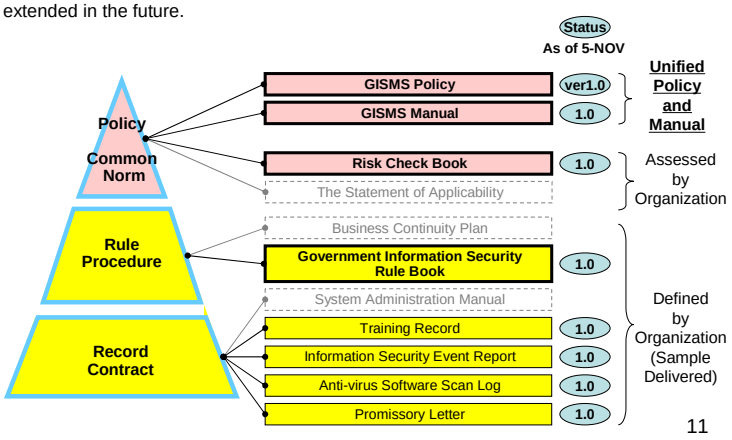
These are drafted by GIS Office, reviewed by GCIO Committee (tentative name until officially established) and authorized by GCIO Chairman (tentative name until officially established). GISMS Policy shall be declared by the top of Royal Government of Cambodia. *The initial version 1.0 is tentatively defined by NiDA with an assistance of JICA.*

3) Risk Check Book

The check items are drafted by GIS Office, reviewed and authorized by GCIO Committee (tentative name until officially established). Risk Check Book blank form contains the default risk evaluation values and controls to be taken. They are assessed and updated by ministry. Put the name of ministry on the document after assessed.

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.



4) GIS Rule Book

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. Document Revision, Distribution, Access and Keeping

Revision

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.

Distribution, Access and Keeping

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. Capacity Development

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. Management Review

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. Types of Control

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.

Appendix.1 Risk Check Instruction

Risk Check Book Instruction	
Risk Check Book is used in a plan phase of ISMS. Follow the instruction below step by step.	
Step 1	Identify assets.
Step 1.1	Walkthrough the assets listed at column C in Risk Check sheet. It defines six types of asset; Information, People, Facility, Paper, Client hardware and software, and Network and server.
Step 1.2	Divide assets according to the organization structure.
	Information and People assets are supposed to be defined at ministry level in accordance with the usual governance .
	Facility, Paper, Client hardware and software, Network and server assets are supposed to be defined by department for each to check by itself.
Step 1.3	Edit column C & D according to the division you made at Step 1.2.
	You can copy & paste an asset by row in order to check by department. However, an asset has multiple check items to identify risks. Be careful to copy a group of rows to include all items.
Step 2	Evaluate assets.
Step 2.1	Evaluate confidentiality, integrity and availability to apply the criteria described in Evaluation Table sheet.
	You can select one from a pull down menu in each field at column G, H and I.
	Use a default value if you feel difficult to evaluate.
Step 2.2	Risk Check sheet automatically display the total evaluation of an asset at column J.
	Review the result and check with the criteria listed in Evaluation Table sheet. Revise confidentiality, integrity and availability evaluation if you feel a total asset value is different from actual.
Step 3	Check assets.
Step 3.1	Read column L and M, and choose just yes or no at column N.
Step 4	Evaluate risks.
Step 4.1	Evaluate threat and vulnerability to apply the criteria described in Evaluation Table sheet.
	You can select one from a pull down menu in each field at column P and R.
	Read the description of each threat at column Q for assistance to decide threat evaluation.
	Use a default value if you feel difficult to evaluate.
Step 4.2	Risk Check sheet automatically display the total evaluation of a risk at column T.
	Review the result and check with the criteria listed in Evaluation Table sheet. Revise threat and vulnerability evaluation if you feel a total risk value is different from actual.
	Go to Step 5 if the total risk is High. Consider the consistency of ISMS if the total risk is Low and make an arrangement if any (e.g. update the existing rulebook or update the control reference at column V.)
Step 5	Decide controls.
Step 5.1	Read the description of default control contents at column U.
Step 5.2	Read the description of sample information security rulebook referred at column V.
Step 5.3	Decide the applicability of implementing the rule and procedures in the sample information security rulebook. Decide the alternatives if not applicable.
Step 5.4	Update the control contents at column U, reference at column V, and the rule and procedures which is applicable and can be implemented to the organization.
Step 6	Evaluate risks after control.
Step 6.1	Evaluate threat and vulnerability to apply the criteria described in Evaluation Table sheet.
	You can select one from a pull down menu in each field at column W and Y.
	Use a default value if you do not change the controls and the rule and procedures in the sample IS handbook.
Step 6.2	Risk Check sheet automatically display the total evaluation of a risk at column AA.
	Review the result and check with the criteria listed in Evaluation Table sheet. Revise threat and vulnerability valuation if you feel a total risk value is different from actual.
Step 6.3	Make sure it is preferable to get each total risk classified as Low. Decide take additional actions to lessen risks, or describe a residual risk statement to accept.

SECTION 4
Government Information Security Management System Risk Check

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

Risk Check

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidentiel	Integrity	Availability	Total	Check Item Check Type	Check Item	Check results	Comments on Check Results
1	Basic Check List								Basic			
2	NIDA: CISO											
3		Information										
4			Classification		5: Confident	3: High	5: High	3: High				
5									Classification	Define the security classification of information.	1: No	
6									Control	Define information control according to the classification.	1: No	
7									Protection	Define how to save and protect information against unauthorized access.	1: No	
8									Record	Define how to keep a record (a media and a keeping period).	1: No	
9			Privacy information		5: Confident	5: High	5: High	3: High				
10									Classification	Classify privacy information always as confidential.	1: No	
11		People										
12			Information security organization		5: Confident	5: High	5: High	3: High				
13									Organization	Define and name information security manager (IS manager).	1: No	
14			Government officials						-to be defined and implemented in the future.			
15									Hiring	Evaluate information security factors when selecting candidates.	0: Yes / NA	
16									Orientation	Get trained information security and state the nondisclosure obligation.	0: Yes / NA	
17									Termination	Check ...	0: Yes / NA	
18			External parties						-to be defined and implemented in the future.			
19									Accessible area	Define an accessible area for each external party.	0: Yes / NA	
20			Purchasing equipments						-to be defined and implemented in the future.			
21			Outsourcing						-to be defined and implemented in the future.			
22									Contractor selection	Evaluate information security factors when selecting contractors.	0: Yes / NA	
23									Contract	Define the nondisclosure obligation clearly in a contract.	0: Yes / NA	
24			Software development						-to be defined and implemented in the future.			
25		Facility										
26			Office building		2: Internal	5: High	5: High	2: Middle				
27									User definition	Define those who can enter the facility/room.	1: No	
28									Key system	Implement an appropriate key system for an entrance of the facility/room.	1: No	
29									Zoning	Separate an office space and the other accessible common space.	1: No	
30									Outsiders	Get outsiders with an insider attendant.	1: No	
31									Entry / exit record	Record an entry and exit.	1: No	
32									Goods shipping record	Keep records of courier service.	1: No	
33			Cabinet		2: Internal	5: High	5: High	2: Middle				
34									Cabinet lock-up	Store information assets with confidential information and lock up cabinets.	1: No	
35			Fax machines and printers		2: Internal	5: High	5: High	2: Middle				
36									Disposal	Dispose printed materials/faxed materials with care.	1: No	
37									Faxing record	Keep record of faxing (sending/receiving).	1: No	
38			Desk		2: Internal	5: High	5: High	2: Middle				
39									Desk lock-up	Lock up desk drawers when leaving.	1: No	
40									Desktop clean-up	Leave nothing on a desktop, especially confidential information.	1: No	
41		Physical information										
42			Paper		2: Internal	5: High	5: High	2: Middle				
43									Classification	Identify confidential information within each paper/document.	1: No	
44									Protection	Save confidential paper/documents in safe against unauthorized access.	1: No	
45									Disposal	Use a paper shredder when disposing confidentials. Or burn it by official.	1: No	
46			Digital Archives (DVDs/CDs/FDs/Tapes)		2: Internal	3: Middle	1: Low	1: Low				
47									Classification	Identify confidential information within each archive.	1: No	
48									Protection	Save confidential archives in safe against unauthorized access.	1: No	
49									Disposal	Scrap a media (Tape/FD/CD/DVD) physically.	1: No	

Risk Check

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidential	Integrity	Availability	Total	Check item Check Type	Check item	Check results	Comments on Check Results
50				Client PC (hardware and software)								
51				Desktop PC	2: Internal	3: Middle	1: Low	1: Low				
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				Laptop /mobile PC (All desktop PC check items must be applied.)	2: Internal	3: Middle	1: Low	1: Low				
63									Security wire	Wire all laptop /mobile PCs physically to desks or store at a locked facility.	1: No	
64				Storage devices (Portable HDDs /Memory sticks /Memory cards)	2: Internal	3: Middle	1: Low	1: Low				
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				Personal asset (Personally owned PC, storage devices and digital archi	2: Internal	3: Middle	1: Low	1: Low				
68									Permission	Get a permission from IS manager to take in/out a personal asset to/from an office	1: No	
69				Software	2: Internal	3: Middle	1: Low	1: Low				
70									Installation	Install software explicitly allowed by IS manager.	1: No	
71									Software configuration	Configure software according to IS managers' instruction.	1: No	
72									Patch application	Apply patches according to IS managers' request.	1: No	
73									Mail encryption	Encrypt to send an e-mail.	1: No	
74									Miss-addressing mails	Report and take appropriate actions when miss-addressing mails.	1: No	
75									Integrity consideration	Consider the integrity of a document and deliver one in PDF format when copying.	1: No	
76									Web downloading	Download a web browser executable only which has an electronic signature.	1: No	

Risk Check

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidential	Integrity	Availability	Total	Check item Check Type	Check item	Check results	Comments on Check Results
77	NDA: CamCERT											
78		Facility										
79			Office building	2: Internal	5: High	5: High	2: Middle					
80									User definition	Define those who can enter this facility/room.	1: No	
81									Key system	Implement an appropriate key system for an entrance of the facility/room.	1: No	
82									Zoning	Separate an office space and the other accessible common space.	1: No	
83									Outsiders	Get outsiders with an insider attendent.	1: No	
84									Entry / exit record	Record an entry and exit.	1: No	
85									Goods shipping record	Keep records of courier service.	1: No	
86			Cabinet	2: Internal	5: High	5: High	2: Middle					
87									Cabinet lock-up	Store information assets with confidential information and lock up cabinets.	1: No	
88			Fax machines and printers	2: Internal	5: High	5: High	2: Middle					
89									Disposal	Dispose printed materials/faxed materials with care.	1: No	
90									Faxing record	Keep record of faxing (sending/receiving).	1: No	
91			Desk	2: Internal	5: High	5: High	2: Middle					
92									Desk lock-up	Lock up desk drawers when leaving.	1: No	
93									Desktop clean-up	Leave nothing on a desktop, especially confidential information.	1: No	
94		Physical information										
95			Paper	2: Internal	5: High	5: High	2: Middle					
96									Classification	Identify confidential information within each paper/document.	0: Yes / NA	
97									Protection	Save confidential paper/documents in safe against unauthorized access.	1: No	
98									Disposal	Use a paper shredder when disposing confidentials. Or burn it by offcial.	1: No	
99			Digital Archives (DVDs/CDs/FDs/Tapes)	2: Internal	3: Middle	1: Low	1: Low					
100									Classification	Identify confidential information within each archive.	1: No	
101									Protection	Save confidential archives in safe against unauthorized access.	1: No	
102									Disposal	Scrap a media (Tape/FD/CD/DVD) physically.	1: No	
103		Client PC (hardware and software)										
104			Desktop PC	2: Internal	3: Middle	1: Low	1: Low					
105									Assignment	Assign one main user at minimum to all PCs.	1: No	
106									User ID and password	Use a robust password and change one periodically.	1: No	
107									User ID sharing	Prohibit share user ID and password with several people.	1: No	
108									Cleared screen	Clear a display screen by setting screen saver function with password.	1: No	
109									Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No	
110									Anti-virus protection	Use an automatic virus detection function usually.	1: No	
111									Anti-virus protection	Update a virus definition file periodically.	1: No	
112									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
113									UPS	Connect UPS for all desktop PCs.	1: No	
114									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
115			Laptop /mobile PC (All desktop PC check items must be applied)	2: Internal	3: Middle	1: Low	1: Low					
116									Security wire	Wire all laptop /mobile PCs physically to desks or store at a locked facility.	1: No	
117			Storage devices (Portable HDDs /Memory sticks /Memory cards)	2: Internal	3: Middle	1: Low	1: Low					
118									Anti virus protection	Scan storage devices with anti-virus software periodically.	1: No	
119									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
120			Personal asset (Personally owned PC, storage devices and digital arch	2: Internal	3: Middle	1: Low	1: Low					
121									Permission	Get a permission from IS manager to take in/out a personal asset to/from an office.	1: No	
122			Software	2: Internal	3: Middle	1: Low	1: Low					
123									Installation	Install software explicitly allowed by IS manager.	1: No	
124									Software configuration	Configure software according to IS managers' instruction.	1: No	
125									Patch application	Apply patches according to IS managers' request.	1: No	
126									Mail encryption	Encrypt to send an e-mail.	1: No	
127									Miss-addressing mails	Report and take appropriate actions when miss-addressing mails.	1: No	
128									Integrity consideration	Consider the integrity of a document and deliver one in PDF format when copying.	1: No	
129									Web downloading	Download a web browser executable only which has an electronic signature.	1: No	

Risk Check

	Assets			Asset Evaluation				Check item			
#	L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Confidential	Integrity	Availability	Total	Check Type	Check item	Check results	Comments on Check Results
130				Network and server								
131				LAN and Internet	2: Internal	3: Middle	1: Low	1: Low				
132									Firewall	Disconnect an internal network from an external network.	1: No	
133									Record	Record a network access.	1: No	
134									Audit and action	Audit records, detect unauthorized access and take actions promptly.	1: No	
135									UPS	Connect UPS for all network devices.	1: No	
136				Server common	2: Internal	3: Middle	1: Low	1: Low				
137									Zoning control	Segregate a server room and lock up the room usually.	1: No	
138									Physical installation	Install servers physically in safe from destruction.	1: No	
139									Physical protection	Lock up a server rack from unauthorized access.	1: No	
140									User definition	Define those who can enter the server room.	1: No	
141									User ID and password	Use a robust password and change one periodically.	1: No	
142									User ID sharing	Prohibit share user ID and password with several people.	1: No	
143									Operation manual	Document an operation manual and lessen human errors.	1: No	
144									Data access control	Control data access appropriately with the access control functions of file/data systems.	1: No	
145									Data protection	Encrypt data appropriately in case of a forced attack.	1: No	
146									Data back-up	Back up data periodically.	1: No	
147									Archive protection	Save confidential archives in safe against unauthorized access.	1: No	
148									Data recovery	Have a capacity to recover data defined in a service level agreement.	1: No	
149									Record	Record a data access and keep it for the defined period of time.	1: No	
150									Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No	
151									Anti-virus protection	Use an automatic virus detection function usually.	1: No	
152									Anti-virus protection	Update a virus definition file periodically.	1: No	
153									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
154									Audit and action	Audit records, detect unauthorized access /execution and take actions promptly.	1: No	
155									Information gathering	Gather external security information to take actions proactively.	1: No	
156									Patch application	Apply patches depending on its emergency and stability.	1: No	
157									UPS	Connect UPS for all servers.	1: No	

Risk Check

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidential	Integrity	Availability	Total	Check Item Check Type	Check Item	Check results	Comments on Check Results
158	GAIS											
159		Network and server			2: Internal	3: Middle	3: Middle	2: Middle				
160									Firewall	Disconnect an internal network from an external network.	1: No	Suspended until PAIS integrating GAIS
161									Record	Record a network access.	1: No	
162									Audit and action	Audit records, detect unauthorized access and take actions promptly.	1: No	
163									UPS	Connect UPS for all network devices.	1: No	
164		Server common			2: Internal	3: Middle	3: Middle	2: Middle				
165									Zoning control	Segregate a server room and lock up the room usually.	1: No	
166									Physical installation	Install servers physically in safe from destruction.	1: No	
167									Physical protection	Lock up a server rack from unauthorized access.	1: No	
168									User definition	Define those who can enter the server room.	1: No	
169									User ID and password	Use a robust password and change one periodically.	1: No	
170									User ID sharing	Prohibit share user ID and password with several people.	1: No	
171									Operation manual	Document an operation manual and lessen human errors.	1: No	
172									Data access control	Control data access appropriately with the access control functions of file/data systems.	1: No	
173									Data protection	Encrypt data appropriately in case of a forced attack.	1: No	
174									Data backup	Back up data periodically.	1: No	
175									Archive protection	Save confidential archives in safe against unauthorized access.	1: No	
176									Data recovery	Have a capacity to recover data defined in a service level agreement.	1: No	
177									Record	Record a data access and keep it for the defined period of time.	1: No	
178									Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No	
179									Anti-virus protection	Use an automatic virus detection function usually.	1: No	
180									Anti-virus protection	Update a virus definition file periodically.	1: No	
181									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
182									Audit and action	Audit records, detect unauthorized access /execution and take actions promptly.	1: No	
183									Information gathering	Gather external security information to take actions proactively.	1: No	
184									Patch application	Apply patches depending on its emergency and stability.	1: No	
185									UPS	Connect UPS for all servers.	1: No	

Risk Check

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidential	Integrity	Availability	Total	Check item Check Type	Check Item	Check results	Comments on Check Results
185	Secretary General Office											
187		Facility										
188			Office building	2: Internal	5: High	5: High	2: Middle					
189									User definition	Define those who can enter the facility/room.	0: Yes / NA	
190									Key system	Implement an appropriate key system for an entrance of the facility/room.	0: Yes / NA	
191									Zoning	Separate an office space and the other accessible common space.	0: Yes / NA	
192									Outsiders	Get outsiders with an insider attendant.	0: Yes / NA	
193									Entry /exit record	Record an entry and exit.	1: No	
194									Goods shipping record	Keep records of courier service.	1: No	
195			Cabinet	5: Confident	5: High	5: High	3: High					
196									Cabinet lock-up	Store information assets with confidential information and lock up cabinets.	1: No	
197			Fax machines and printers	2: Internal	5: High	5: High	2: Middle					
198									Disposal	Dispose printed materials/faxed materials with care.	0: Yes / NA	
199									Faxing record	Keep record of faxing (sending/receiving).	1: No	
200			Desk	5: Confident	5: High	5: High	3: High					
201									Desk lock-up	Lock up desk, drawers when leaving.	0: Yes / NA	
202									Desktop clean-up	Leave nothing on a desktop, especially confidential information.	0: Yes / NA	
203		Physical information										
204			Paper	5: Confident	5: High	5: High	3: High					
205									Classification	Identify confidential information within each paper/document.	0: Yes / NA	
206									Protection	Save confidential paper/documents in safe against unauthorized access.	0: Yes / NA	
207									Disposal	Use a paper shredder when disposing confidentials. Or burn it by official.	0: Yes / NA	
208			Digital Archives (DVDs/CDs/FDs/Tapes)	2: Internal	3: Middle	1: Low	1: Low					
209									Classification	Identify confidential information within each archive.	1: No	
210									Protection	Save confidential archives in safe against unauthorized access.	1: No	
211									Disposal	Scrap a media (Tape/FD/CD/DVD) physically.	1: No	
212		Client PC (hardware and software)										
213			Desktop PC	5: Confident	3: Middle	3: Middle	2: Middle					
214									Assignment	Assign one main user at minimum to all PCs.	0: Yes / NA	
215									User ID and password	Use a robust password and change one periodically.	1: No	
216									User ID sharing	Prohibit share user ID and password with several people.	1: No	
217									Cleared screen	Clear a display screen by setting screen saver function with password.	1: No	
218									Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No	
219									Anti-virus protection	Use an automatic virus detection function usually.	0: Yes / NA	
220									Anti-virus protection	Update a virus definition file periodically.	0: Yes / NA	
221									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
222									UPS	Connect UPS for all desktop PCs.	1: No	
223									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
224			Laptop /mobile PC (All desktop PC check items must be applied.)	2: Internal	3: Middle	1: Low	1: Low					
225									Security wire	Wire all laptop /mobile PCs physically to desks or store at a locked facility.	1: No	
226			Storage devices (Portable HDDs /Memory sticks /Memory cards)	2: Internal	3: Middle	1: Low	1: Low					
227									Anti virus protection	Scan storage devices with anti-virus software periodically.	1: No	
228									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
229			Personal asset (Personally owned PC, storage devices and digital archi	2: Internal	3: Middle	1: Low	1: Low					
230									Permission	Get a permission from IS manager to take in/out a personal asset to/from an office.	1: No	
231			Software	2: Internal	3: Middle	1: Low	1: Low					
232									Installation	Install software explicitly allowed by IS manager.	1: No	
233									Software configuration	Configure software according to IS managers' instruction.	1: No	
234									Patch application	Apply patches according to IS managers' request.	1: No	
235									Mail encryption	Encrypt to send an e-mail.	1: No	
236									Miss-addressing mails	Report and take appropriate actions when miss-addressing mails.	1: No	
237									Integrity consideration	Consider the integrity of a document and deliver one in PDF format when copying.	1: No	
238									Web downloading	Download a web browser executable only which has an electronic signature.	1: No	
239												
240												

Risk Check

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidential	Integrity	Availability	Total	Check item Check Type	Check item	Check results	Comments on Check Results
241	Extended								Extended			
242		Network and Server										
243			LAN and Internet						-to be defined and implemented in the future.			
244										Protection of network	0: Yes / NA	
245										Security measure of network equipment	0: Yes / NA	
246									Remote access	Limit an access capacity from external networks considering its risks.	0: Yes / NA	
247									Wireless LAN	Consider its risks to...	0: Yes / NA	
248			Server common						-to be defined and implemented in the future.			
249									Security holes treatment		0: Yes / NA	
250									Malware treatment		0: Yes / NA	
251									DOS treatment		0: Yes / NA	
252									Stepping stone treatment		0: Yes / NA	
253									Domain name		0: Yes / NA	
254			Server application common						-to be defined and implemented in the future.			
255									Authentication		0: Yes / NA	
256									Access control		0: Yes / NA	
257									Administration		0: Yes / NA	
258									Audit trail		0: Yes / NA	
259									Assurance		0: Yes / NA	
260									Encryption		0: Yes / NA	
261												

Risk Check

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidential	Integrity	Availability	Total	Check item Check Type	Check item	Check results	Comments on Check Results
262	Network											
263		Facility										
264			Office building		2: Internal	5: High	5: High	2: Middle				
265									User definition	Define those who can enter the facility/room.	0: Yes / NA	
266									Key system	Implement an appropriate key system for an entrance of the facility/room.	1: No	
267									Zoning	Separate an office space and the other accessible common space.	0: Yes / NA	
268									Outsiders	Get outsiders with an insider attendant.	1: No	
269									Entry / exit record	Record an entry and exit.	1: No	
270									Goods shipping record	Keep records of courier service.	1: No	
271			Cabinet		2: Internal	5: High	5: High	2: Middle				
272									Cabinet lock-up	Store information assets with confidential information and lock up cabinets.	1: No	
273			Fax machines and printers		2: Internal	5: High	5: High	2: Middle				
274									Disposal	Dispose printed materials/faxed materials with care.	1: No	
275									Faxing record	Keep record of faxing (sending/receiving).	1: No	
276			Desk		2: Internal	5: High	5: High	2: Middle				
277									Desk lock-up	Lock up desk drawers when leaving.	1: No	
278									Desktop clean-up	Leave nothing on a desktop, especially confidential information.	1: No	
279		Physical information										
280			Paper		2: Internal	5: High	5: High	2: Middle				
281									Classification	Identify confidential information within each paper/document.	1: No	
282									Protection	Save confidential paper/documents in safe against unauthorized access.	1: No	
283									Disposal	Use a paper shredder when disposing confidentials. Or burn it by official.	1: No	
284			Digital Archives (DVDs/CDs/FDs/Tapes)		2: Internal	5: High	5: High	2: Middle				
285									Classification	Identify confidential information within each archive.	1: No	
286									Protection	Save confidential archives in safe against unauthorized access.	1: No	
287									Disposal	Scrap a media (Tape/FD/CD/DVD) physically.	1: No	
288		Client PC (hardware and software)										
289			Desktop PC		2: Internal	5: High	5: High	2: Middle				
290									Assignment	Assign one main user at minimum to all PCs.	1: No	
291									User ID and password	Use a robust password and change one periodically.	1: No	
292									User ID sharing	Prohibit share user ID and password with several people.	0: Yes / NA	
293									Cleared screen	Clear a display screen by setting screen saver function with password.	0: Yes / NA	
294									Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No	
295									Anti-virus protection	Use an automatic virus detection function usually.	0: Yes / NA	
296									Anti-virus protection	Update a virus definition file periodically.	0: Yes / NA	
297									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
298									UPS	Connect UPS for all desktop PCs.	1: No	
299									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
300			Laptop /mobile PC (All desktop PC check items must be applied.)		2: Internal	5: High	5: High	2: Middle				
301									Security wire	Wire all laptop /mobile PCs physically to desks or store at a locked facility.	1: No	
302			Storage devices (Portable HDDs /Memory sticks /Memory cards)		2: Internal	5: High	5: High	2: Middle				
303									Anti-virus protection	Scan storage devices with anti-virus software periodically.	1: No	
304									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
305			Personal asset (Personally owned PC, storage devices and digital archi		2: Internal	5: High	5: High	2: Middle				
306									Permission	Get a permission from IS manager to take in/out a personal asset to/from an office.	1: No	
307			Software		2: Internal	5: High	5: High	2: Middle				
308									Installation	Install software explicitly allowed by IS manager.	1: No	
309									Software configuration	Configure software according to IS managers' instruction.	1: No	
310									Patch application	Apply patches according to IS managers' request.	1: No	
311									Mail encryption	Encrypt to send an e-mail.	1: No	
312									Mis-addressing mails	Report and take appropriate actions when miss-addressing mails.	1: No	
313									Integrity consideration	Consider the integrity of a document and deliver one in PDF format when copying.	1: No	
314									Web downloading	Download a web browser executable only which has an electronic signature.	1: No	

Risk Check

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidential	Integrity	Availability	Total	Check item Check Type	Check_Item	Check results	Comments on Check Results
315	Enterprise											
316		Facility										
317				Office building	2: Internal	5: High	5: High	2: Middle				
318									User definition	Define those who can enter the facility/room.	0: Yes / NA	
319									Key system	Implement an appropriate key system for an entrance of the facility/room.	1: No	
320									Zoning	Separate an office space and the other accessible common space.	0: Yes / NA	
321									Outsiders	Get outsiders with an insider attendant.	0: Yes / NA	
322									Entry /exit record	Record an entry and exit.	1: No	
323									Goods shipping record	Keep records of courier service.	1: No	
324				Cabinet	2: Internal	5: High	5: High	2: Middle				
325									Cabinet lock-up	Store information assets with confidential information and lock up cabinets.	1: No	
326				Fax machines and printers	2: Internal	5: High	5: High	2: Middle				
327									Disposal	Dispose printed materials/faxed materials with care.	1: No	
328									Faxing record	Keep record of faxing (sending/receiving).	1: No	
329				Desk	2: Internal	5: High	5: High	2: Middle				
330									Desk lock-up	Lock up desk drawers when leaving.	1: No	
331									Desktop clean-up	Leave nothing on a desktop, especially confidential information.	0: Yes / NA	
332		Physical information										
333				Paper	2: Internal	5: High	5: High	2: Middle				
334									Classification	Identify confidential information within each paper/document.	0: Yes / NA	
335									Protection	Save confidential paper/documents in safe against unauthorized access.	1: No	
336									Disposal	Use a paper shredder when disposing confidentials. Or burn it by official.	1: No	
337				Digital Archives (DVDs/CDs/tDs/Tapes)	2: Internal	5: High	5: High	2: Middle				
338									Classification	Identify confidential information within each archive.	1: No	
339									Protection	Save confidential archives in safe against unauthorized access.	1: No	
340									Disposal	Scrap a media (Tape/FD/CD/DVD) physically.	1: No	
341		Client PC (hardware and software)										
342				Desktop PC	2: Internal	5: High	5: High	2: Middle				
343									Assignment	Assign one main user at minimum to all PCs.	1: No	
344									User ID and password	Use a robust password and change one periodically.	1: No	
345									User ID sharing	Prohibit share user ID and password with several people.	1: No	
346									Cleared screen	Clear a display screen by setting screen saver function with password.	1: No	
347									Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No	
348									Anti-virus protection	Use an automatic virus detection function usually.	0: Yes / NA	
349									Anti-virus protection	Update a virus definition file periodically.	0: Yes / NA	
350									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
351									UPS	Connect UPS for all desktop PCs.	1: No	
352									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
353				Laptop /mobile PC (All desktop PC check items must be applied)	2: Internal	5: High	5: High	2: Middle				
354									Security wire	Wire all laptop /mobile PCs physically to desks or store at a locked facility.	1: No	
355				Storage devices (Portable HDDs /Mamory sticks /Memery cards)	2: Internal	5: High	5: High	2: Middle				
356									Anti-virus protection	Scan storage devices with anti-virus software periodically.	1: No	
357									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
358				Personal asset (Personally owned PC, storage devices and digital archi	2: Internal	5: High	5: High	2: Middle				
359									Permission	Get a permission from IS manager to take in/out a personal asset to/from an office.	1: No	
360				Software	2: Internal	5: High	5: High	2: Middle				
361									Installation	Install software explicitly allowed by IS manager.	0: Yes / NA	
362									Software configuration	Configure software according to IS managers' instruction.	0: Yes / NA	
363									Patch application	Apply patches according to IS managers' request.	1: No	
364									Mail encryption	Encrypt to send an e-mail.	1: No	
365									Miss-addressing mails	Report and take appropriate actions when miss-addressing mails.	1: No	
366									Integrity consideration	Consider the integrity of a document and deliver one in PDF format when copying.	1: No	
367									Web downloading	Download a web browser executable only which has an electronic signature.	1: No	

Risk Check

#	Assets L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Asset Evaluation Confidentiality	Integrity	Availability	Total	Check Item Check Type	Check item	Check results	Comments on Check Results
368	Content & Applications											
369		Facility										
370			Office building	2: Internal	5: High	5: High	2: Middle					
371								User definition	Define those who can enter the facility/room.	0: Yes / NA		
372								Key system	Implement an appropriate key system for an entrance of the facility/room.	0: Yes / NA		
373								Zoning	Separate an office space and the other accessible common space.	0: Yes / NA		
374								Outsiders	Get outsiders with an insider attendant.	0: Yes / NA		
375								Entry / exit record	Record an entry and exit.	1: No		
376								Goods shipping record	Keep records of courier service.	1: No		
377			Cabinet	2: Internal	5: High	5: High	2: Middle					
378								Cabinet lock-up	Store information assets with confidential infomation and lock up cabinets.	1: No		
379			Fax machines and printers	2: Internal	5: High	5: High	2: Middle					
380								Disposal	Dispose printed materials/faxed materials with care.	1: No		
381								Faxing record	Keep record of faxing (sending/receiving).	1: No		
382			Desk	5: Confident	5: High	5: High	3: High					
383								Desk lock-up	Lock up desk drawers when leaving.	0: Yes / NA		
384								Desktop clean-up	Leave nothing on a desktop, especially confidential information.	0: Yes / NA		
385		Physical information										
386			Paper	2: Internal	5: High	5: High	2: Middle					
387								Classification	Identify confidential information within each paper/document.	1: No		
388								Protection	Save confidential paper/documents in safe against unauthorized access.	0: Yes / NA		
389								Disposal	Use a paper shredder when disposing confidentials. Or burn it by official.	1: No		
390			Digital Archives (DVDs/CDs/FDs/Tapes)	5: Confident	5: High	5: High	3: High					
391								Classification	Identify confidential information within each archive.	0: Yes / NA		
392								Protection	Save confidential archives in safe against unauthorized access.	0: Yes / NA		
393								Disposal	Scrap a media (Tape/FD/CD/DVD) physically.	1: No		
394		Client PC (hardware and software)										
395			Desktop PC	5: Confident	5: High	5: High	3: High					
396								Assignment	Assign one main user at minimum to all PCs.	0: Yes / NA		
397								User ID and password	Use a robust password and change one periodically.	0: Yes / NA		
398								User ID sharing	Prohibit share user ID and password with several people.	0: Yes / NA		
399								Cleared screen	Clear a display screen by setting screen saver function with password.	0: Yes / NA		
400								Anti-virus protection	Scan a local storage with anti-virus software periodically.	0: Yes / NA		
401								Anti-virus protection	Use an automatic virus detection function usually.	0: Yes / NA		
402								Anti-virus protection	Update a virus definition file periodically.	0: Yes / NA		
403								Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No		
404								UPS	Connect UPS for all desktop PCs.	1: No		
405								Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No		
406			Laptop /mobile PC (All desktop PC check items must be applied.)	2: Internal	5: High	5: High	2: Middle					
407								Security wire	Wire all laptop /mobile PCs physically to desks or store at a locked facility.	1: No		
408			Storage devices (Portable HDDs /Memory sticks /Memory cards)	2: Internal	5: High	5: High	2: Middle					
409								Anti -virus protection	Scan storage devices with anti-virus software periodically.	0: Yes / NA		
410								Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No		
411			Personal asset (Personally owned PC, storage devices and digital arch	2: Internal	5: High	5: High	2: Middle					
412								Permission	Get a permission from IS manager to take in/out a personal asset to/from an office.	1: No		
413			Software	2: Internal	5: High	5: High	2: Middle					
414								Installation	Install software explicitly allowed by IS manager.	1: No		
415								Software configuration	Configure software according to IS managers' instruction.	1: No		
416								Patch application	Apply patches according to IS managers' request.	1: No		
417								Mail encryption	Encrypt to send an e-mail.	1: No		
418								Miss-addressing mails	Report and take appropriate actions when miss-addressing mails.	1: No		
419								Integrity consideration	Consider the integrity of a document and deliver one in PDF format when copying.	0: Yes / NA		
420								Web downloading	Download a web browser executable only which has an electronic signature.	1: No		

	Assets			Asset Evaluation				Check item			
	L1	L2	L3	Description (Attributes, Location, Manager in charge, # of Assets)	Confidentiality	Integrity	Availability	Total	Check Type	Check item	Check results	Comments on Check Results
512	HRD & FOSS (only the training team room was assessed)											
513		Facility										
514			Office building		2: Internal	5: High	5: High	2: Middle				
515									User definition	Define those who can enter the facility/room.	0: Yes / NA	
516									Key system	Implement an appropriate key system for an entrance of the facility/room.	1: No	
517									Zoning	Separate an office space and the other accessible common space.	0: Yes / NA	
518									Outsiders	Get outsiders with an insider attendant.	0: Yes / NA	
519									Entry / exit record	Record an entry and exit.	1: No	
520									Goods shipping record	Keep records of courier service.	1: No	
521			Cabinet		2: Internal	5: High	5: High	2: Middle				
522									Cabinet lock-up	Store information assets with confidential information and lock up cabinets.	1: No	
523			Fax machines and printers		2: Internal	5: High	5: High	2: Middle				
524									Disposal	Dispose printed materials/faxed materials with care.	1: No	
525									Faxing record	Keep record of faxing (sending/receiving).	1: No	
526			Desk		2: Internal	5: High	5: High	2: Middle				
527									Desk lock-up	Lock an desk drawers when leaving.	1: No	
528									Desktop clean-up	Leave nothing on a desktop especially confidential information.	0: Yes / NA	
529		Physical information										
530			Paper		2: Internal	5: High	5: High	2: Middle				
531									Classification	Identify confidential information within each paper/document.	1: No	
532									Protection	Save confidential paper/documents in safe against unauthorized access.	1: No	
533									Disposal	Use a paper shredder when disposing confidentials. Or burn it by official.	1: No	
534			Digital Archives (DVDs/CDs/FDs/Tapes)		2: Internal	5: High	5: High	2: Middle				
535									Classification	Identify confidential information within each archive.	0: Yes / NA	
536									Protection	Save confidential archives in safe against unauthorized access.	0: Yes / NA	
537									Disposal	Scrap a media (Tape/FD/CD/DVD) physically.	1: No	
538		Client PC (hardware and software)										
539			Desktop PC		2: Internal	5: High	5: High	2: Middle				
540									Assignment	Assign one main user to minimum to all PCs.	1: No	
541									User ID and password	Use a robust password and change one periodically.	1: No	
542									User ID sharing	Prohibit share user ID and password with several people.	1: No	
543									Cleared screen	Clear a display screen by setting screen saver function with password.	1: No	
544									Anti-virus protection	Scan a local storage with anti-virus software periodically.	1: No	
545									Anti-virus protection	Use an automatic virus detection function usually.	0: Yes / NA	
546									Anti-virus protection	Update a virus definition file periodically.	0: Yes / NA	
547									Anti-virus protection	Keep records of scanning and updating virus definitions.	1: No	
548									UPS	Connect UPS for all desktop PCs.	1: No	
549									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
550			Laptop /mobile PC (All desktop PC check items must be applied)		2: Internal	5: High	5: High	2: Middle				
551									Security wire	Wire all laptop /mobile PCs physically to desks or store at a locked facility.	1: No	
552			Storage devices (Portable HDDs /Memory sticks /Memory cards)		2: Internal	5: High	5: High	2: Middle				
553									Anti-virus protection	Scan storage devices with anti-virus software periodically.	1: No	
554									Disposal	Execute a physical formatting of a storage, or scrap it physically.	1: No	
555			Personal asset (Personally owned PC, storage devices and digital archi		2: Internal	5: High	5: High	2: Middle				
556									Permission	Get a permission from IS manager to take in/out a personal asset to/from an office.	1: No	
557			Software		2: Internal	5: High	5: High	2: Middle				
558									Installation	Install software explicitly allowed by IS manager.	1: No	
559									Software configuration	Configure software according to IS manager's instruction.	1: No	
560									Patch application	Apply patches according to IS managers' request.	1: No	
561									Mail encryption	Encrypt to send an e-mail.	1: No	
562									Mis-addressing mails	Report and take appropriate actions when mis-addressing mails.	1: No	
563									Integrity consideration	Consider the integrity of a document and deliver one in PDF format when copying.	1: No	
564									Web downloading	Download a web browser executable only which has an electronic signature.	1: No	