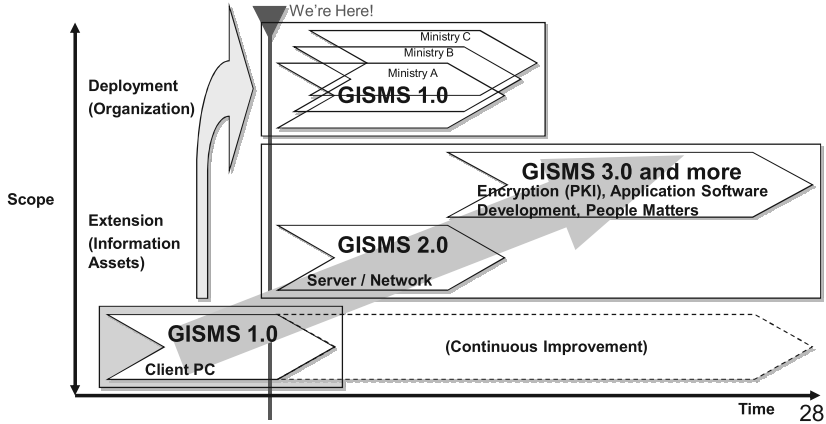


Next Step

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

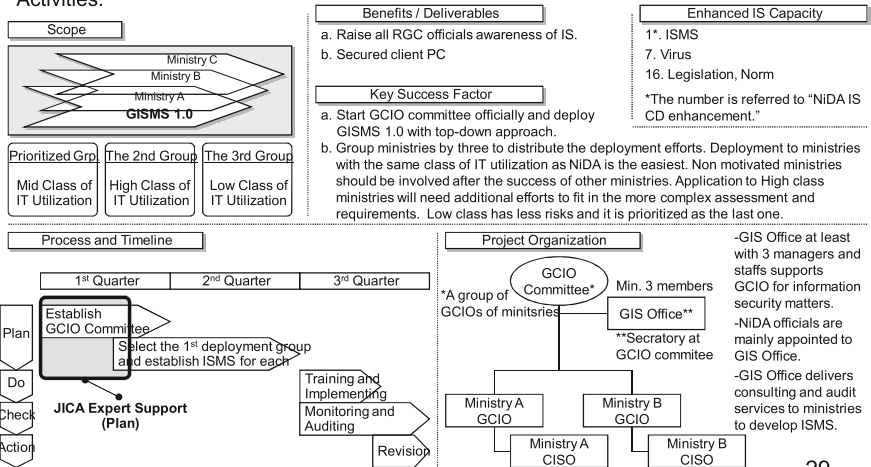
Then, Deployment to other ministries is its repeating actions.

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.



GISMS 1.0 Deployment

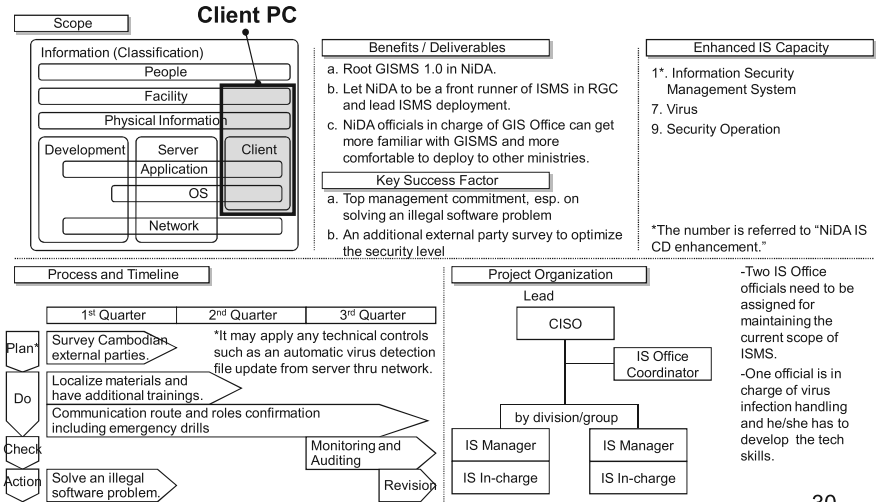
Succeeding the GISMS 1.0 implementation at NiDA, it is recommended to deploy the said GISMS 1.0 to all other ministries as part of GCIO (Government Chief Information Officer) Activities.



29

GISMS 1.0 Continuous Improvement

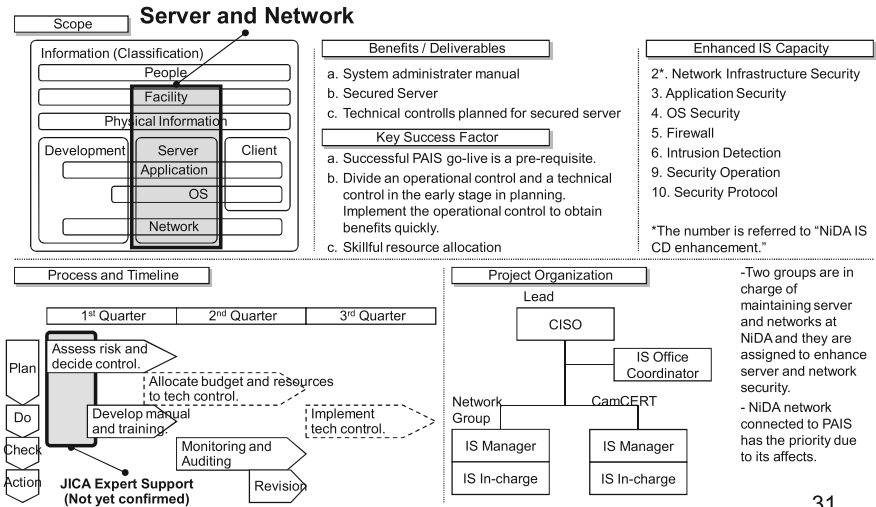
GISMS 1.0 at NiDA needs to be continuously improved as described formerly.



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.

<p>1. Information Security Management System Management Techniques, Risk Analysis Techniques, Information Security Policy, Information Security Audit, Relevant Knowledge</p>	<p>5. Firewall Firewall Installation and Operation, NAT(Network Address Translation), Network Access Control</p>
<p>2. Network Infrastructure Security Network Design Techniques, Network Access Protocol, VPN(Virtual Private Network), Wireless LAN</p>	<p>6. Intrusion Detection Intrusion Detection System Installation and Operation, Intrusion Detection System Function, Detection Algorithm, Detection Subject, Intrusion Detection System</p>
<p>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</p>	<p>7. Virus Communication Route, Policy after Infection, Policy for Prevention, Virus Attack, Detection and Cleansing, Infection, Virus Types</p>
<p>4. OS Security Log Control, Patch Application Control, Service Control, File System Control, Account Control</p>	

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.

8. Secured Programming Techniques Web Application, Database, Application Common, XML(Extensible Markup Language), PHP(HypertextPreprocessor), JAVA, Perl, VB/ASP, C/C++, UNIX, Compiler/VM(Virtual Machine), Windows	12. PKI(Public Key Infrastructure) Usage, Certificate and Authentication, Certificate Revocation, Trust Model, Contract Model, Key Description and Encoding, Norms, Certificate Repository, Certificate Authorities Establishment and Operation, Legal Scheme, PKI Elemental Technology, PKI Service
9. Security Operation Secured Operation at Normal Time, Abnormal Handling, Information Source for Operation	13. Cryptography Public Key Cryptography, Common Key Cryptography, Hashing Algorithm, Cryptic Random Number, Key Management, Zero Knowledge Proof, Other Cryptosystem, Cipher Breaking /Strength Evaluation
10. Security Protocol Application Layer, Transport Layer, Network Layer, Data Link Layer	14. Electronic Signature Usage, Elemental Technology, Mechanism, Benefits
11. Authentication Password Authentication, Biometric Authentication, Authentication Device, Authentication Protocol, Web Authentication, System Authentication, Single Sign-on	15. Unauthorized Access Remote Unauthorized Access, Denial of Service, Tapping, Surveilling, Information Collection, Classical Unauthorized Access
	16. Legislation, Norms Standard and Guideline, Law and Act, International Standard, International Guideline

*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.

- GISMS Policy** declares the top management commitment of implementing GISMS.
- GISMS Manual** defines the unified approach of GISMS for all ministries concerned.
- Risk Check Book** enables all ministries to assess their risks in the same criteria.
- 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

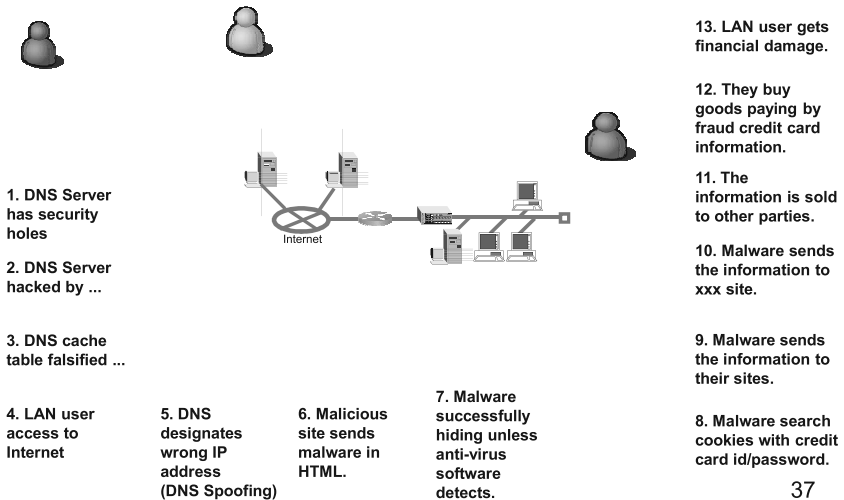
Appendix

36

Image of Vulnerable Servers Spreading Out Viruses

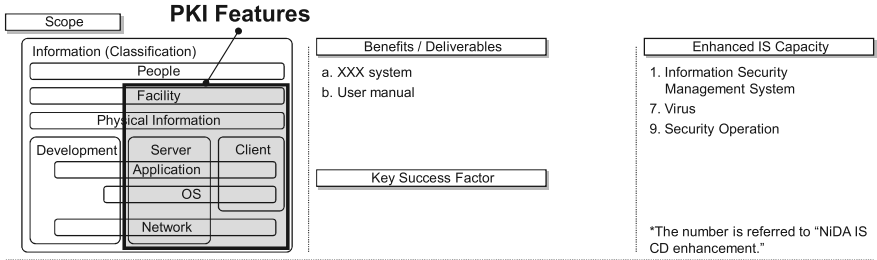
Nice to Have

Assume vulnerable DNS server hacked by unauthorized users from internet.

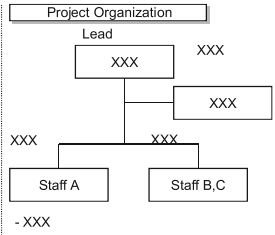


37

XXX

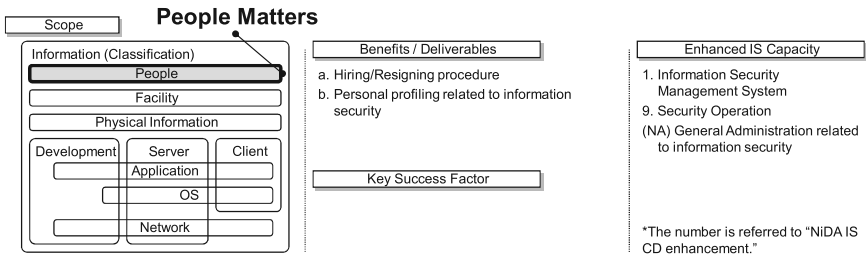


Process and Timeline*
*Timeline described on full time basis

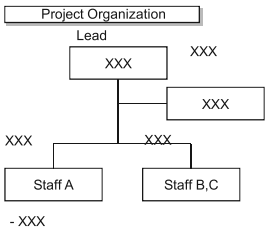


38

XXX



Process and Timeline*
*Timeline described on full time basis



39

SECTION 2
Government Information Security
Management System Policy

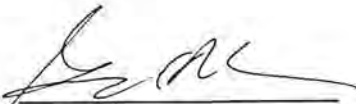
Kingdom of Cambodia
Government Information Security Management System Policy

[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