Topic 1. Establishing a Secure and Trustworthy ICT Environment

1.1 Establishing the Mechanism to Assure Security and Trust of ICT Infrastructure

Presented by
National Communications Commission (NCC)

2009 / 8 / 18

Agenda

- 1. Vision
- 2.Analysis of Current Status
- 3.Developement Trends
- 4. Strategies
- 5.Action Plan
- 6.Discussions

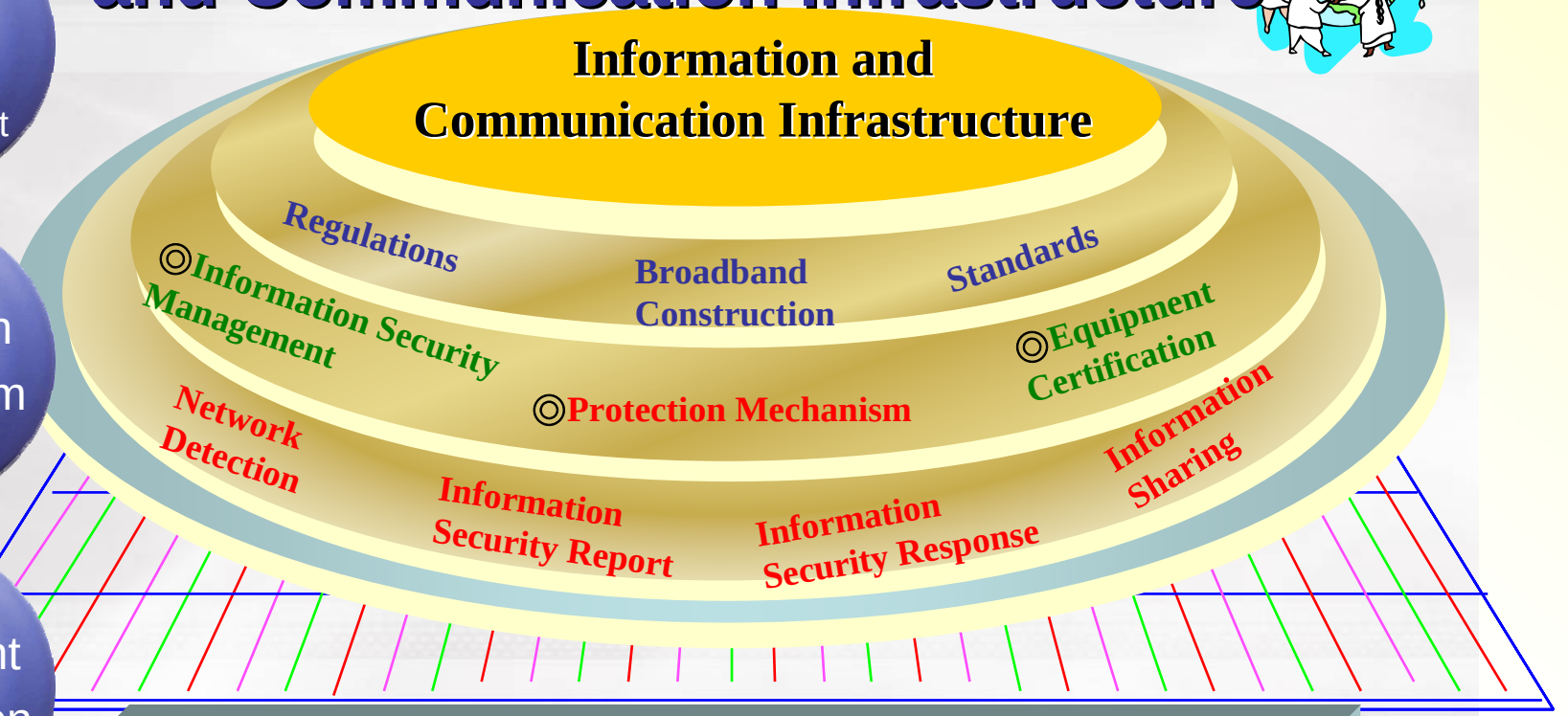
1. Vision

Trusted Mechanism of Information and Communication Infrastructure

Information and Security Management

Protection Mechanism

Equipment Certification

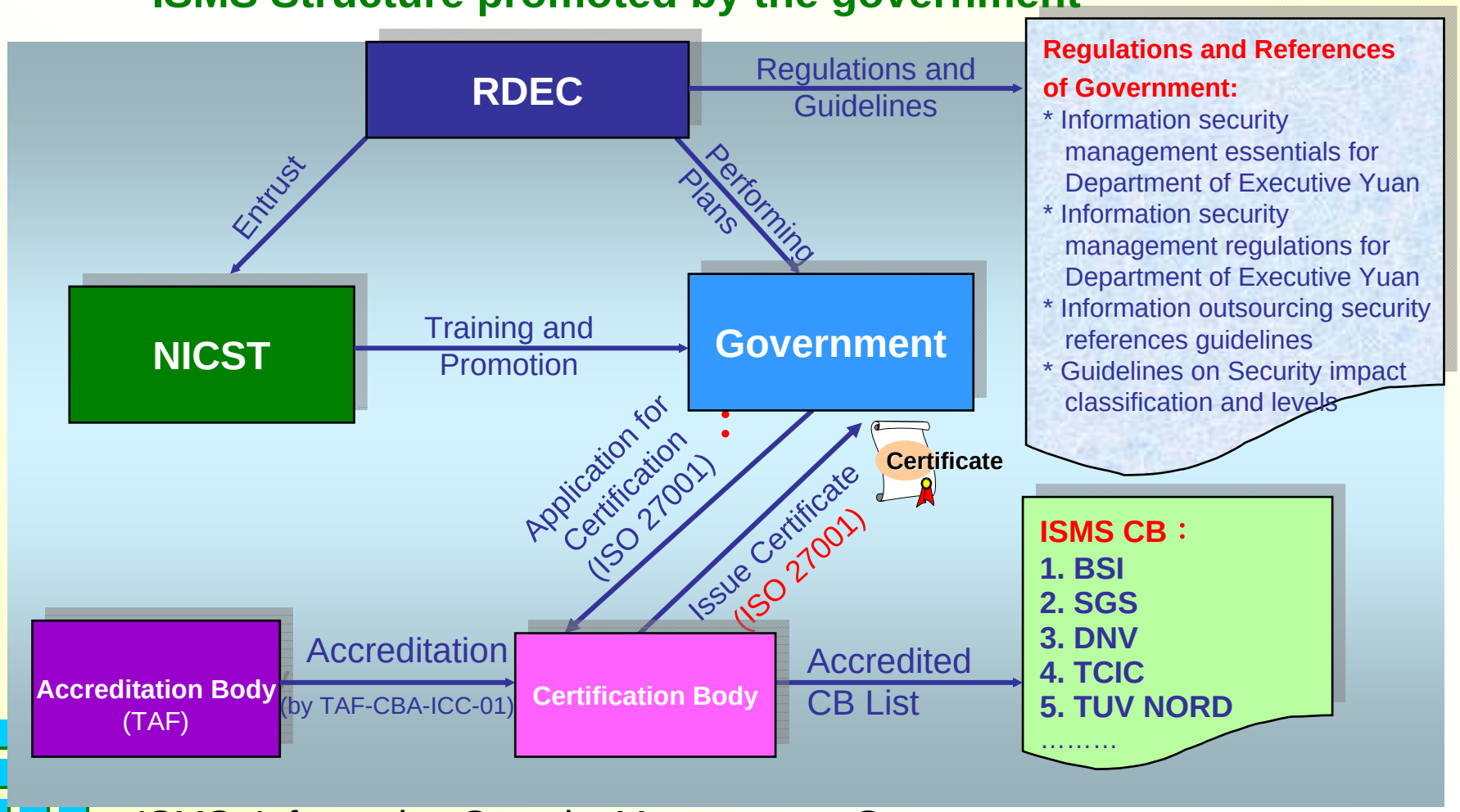


Use information and communication resources in a safe and secure environment

2. Analysis of Current Status(1/12)

1. Information Security System Management-1

ISMS Structure promoted by the government



ISMS: Information Security Management System

2. Analysis of Current Status(2/12)

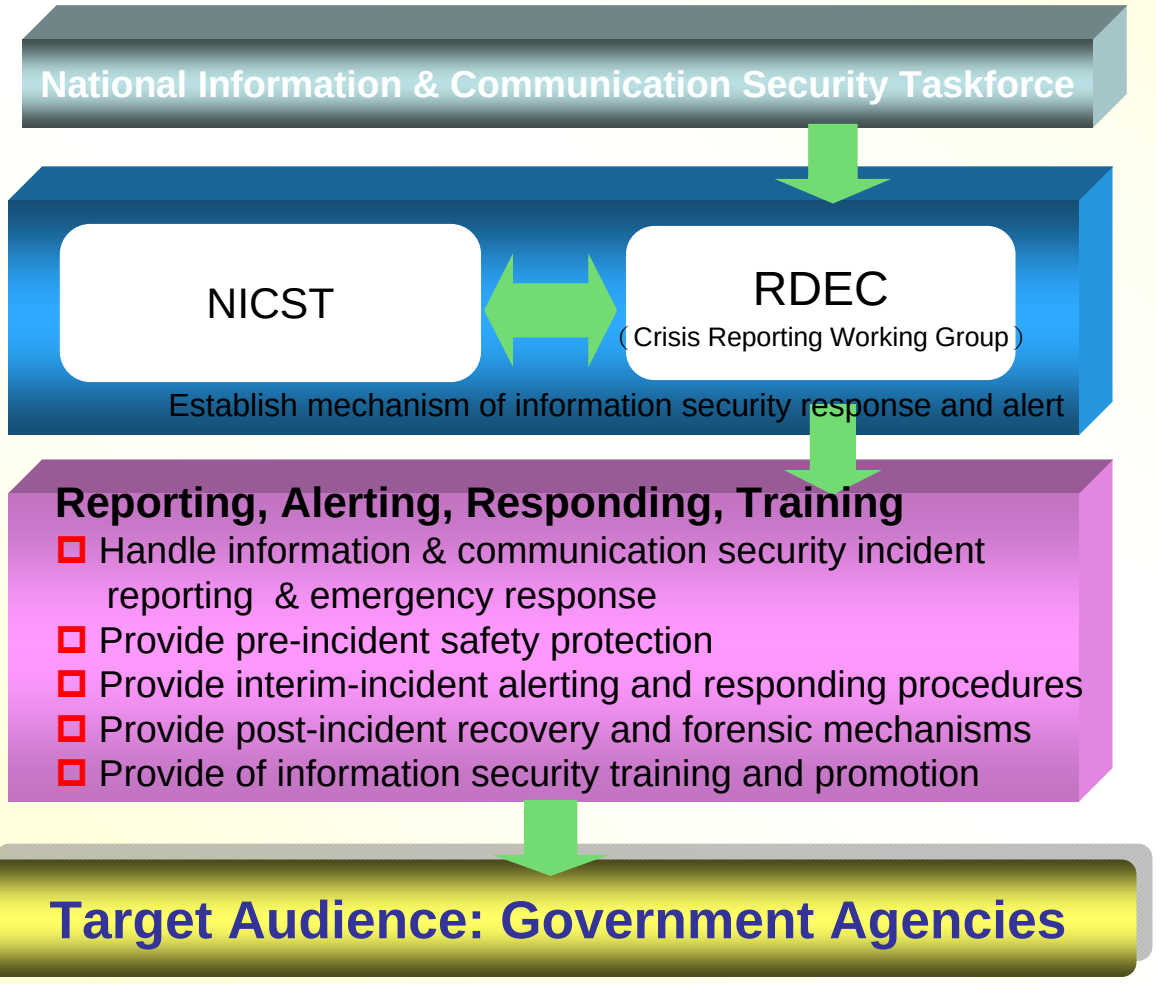
2. Information Security System Management-2

Problems

- ISMS are ready for government agencies, but ISMS has not been introduced in the telecom industry yet
- There is no regulations or laws to force telecom industry to implement ISMS; Need to revise the relative regulations of telecom industry

2. Analysis of Current Status(3/12)

2. Secure Protection of Information and Communication Infrastructure-1



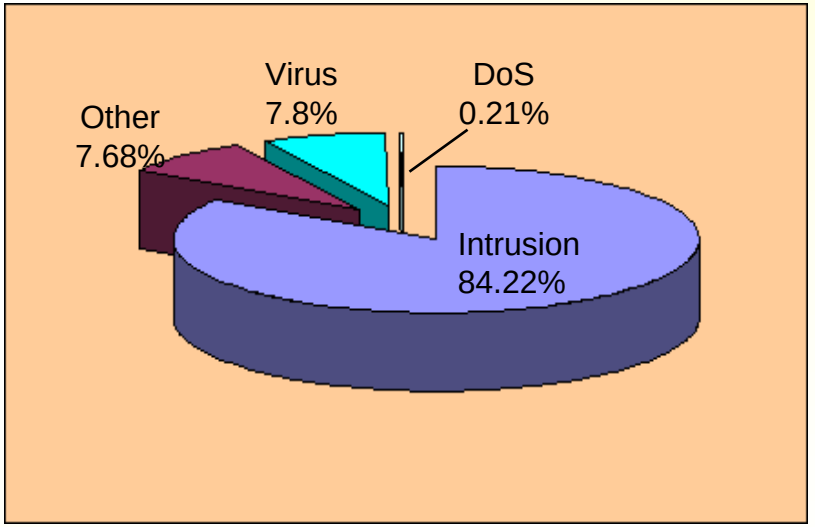
Ref. source:「如何提升政府資通安全通報應變能力」of RDEC

2. Analysis of Current Status(4/12)

2. Secure Protection of information and communication infrastructure-2

Security incidents reported by government agencies

- There are about 7,000 government organizations and15,000 information security contacts in National Information and Communication Security Center
- 963 incidents in 2008, and 368 of 963 were reported by ICST
- Numbers of each level
  - Level 4：0
  - Level 3：2
  - Level 2：87
  - Level 1：874



Ref. source：研考會「如何提升政府資通安全通報應變能力」之簡報資料

2. Analysis of Current Status(5/12)

2. Secure Protection of information and communication infrastructure-3

Loss caused by domestic information security incidents

- Tangible loss : time and money, intangible loss : goodwill
- Damage of information security incidents and recovery time:
  Recovery time was 12.52 hours in 2008, which is higher than that of 2007
- Financial loss of information security incidents: Most private enterprises in 2007 can control the loss money caused by information security incidents to 50,000 or less(70.2%); 243.2 thousands/event in average which is less than that of 2006(535.5 thousands/event)
- Loss of goodwill: The majority of private enterprises do not believe that the information security incidents will result in loss of goodwill or reputation; only 6.5% enterprises in 2008 believe that information security incidents will result in loss of goodwill, which is less than 7.4% in 2007

  （Ref source:財團法人台灣經濟研究院委託調查）

2. Analysis of Current Status(6/12)

2. Secure Protection of information and communication infrastructure-4

Current information protection measures of major domestic IASP:

- Provide the latest version of anti-virus software, of which some are free of charge
- Provide anti-virus or detection services which collect fees; immediately issue information of specific virus, system flaws and hacker activities on website.
- Offer services for IPS (Intrusion Prevention System) and IDS (Intrusion Detection System)
- Inform all the potential BOT to consumers regarding fishing sites, relay station and the victim host announced by well-known institutions
- We will immediately deal with fishing websites, but it is difficult to handle botnet and Trojan problems due to the complexity. We do help users deal with harmful and analyzed malicious relay station

Problems:

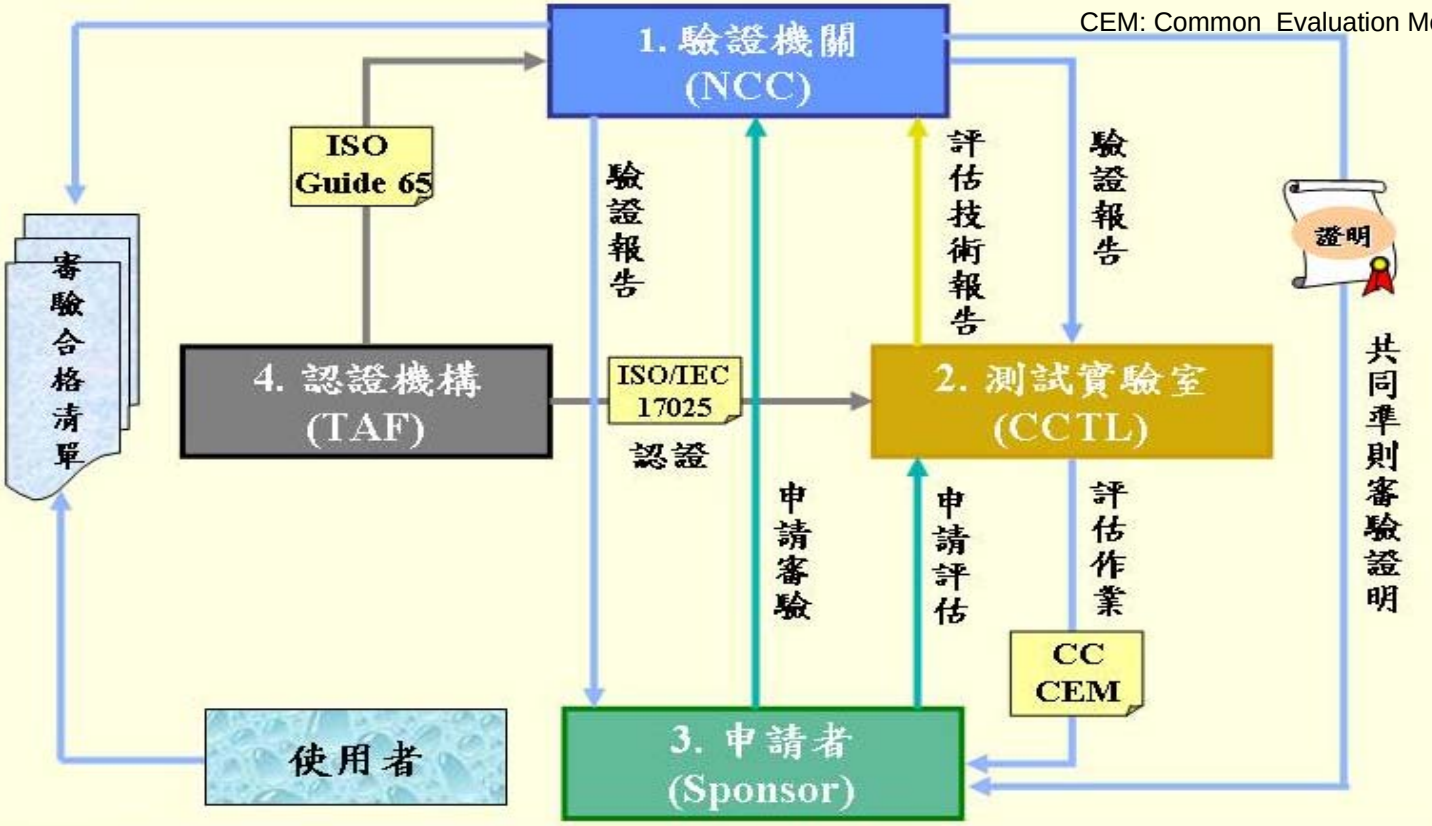
- **There are no integrated mechanisms of alerting, reporting, responding and information sharing for IASP**

2. Analysis of Current Status(7/12)

3. Information and Communication Equipment Certification-1

CC: Common Criteria

CEM: Common Evaluation Methodology



參與單位

1. 驗證機關 (Certification Body) ：國家通訊傳播委員會(NCC)
2. 測試實驗室 (Common Criteria Testing Laboratory)
3. 申請者(Sponsor/Developer)：設備供應商、開發者或政府機關（構）
4. 認證機構 (Accreditation Body) ：財團法人全國認證基金會(TAF)

2. Analysis of Current Status(8/12)

3. Information and Communication Equipment Certification-2

Evaluation energy of TTC (Telecom Technology Center)

- 14 evaluators are capable of CC evaluating
- Evaluation time estimation

Level / Time estimation	EAL 1	EAL 2	EAL 3	ELA 4
Evaluation time by Lab.	1-2 months	2-3 months	3-5 months	4-6 months
Document revision time by vendor	2-4 months	4-6 months	6-7 months	8-12 months
Total evaluation time	3-6 months	6-9 months	9-12 months	12-18 months
Verification by competent authority	< 1 months	< 1 months	1-2 months	1-2 months

- Total evaluation time = Evaluation time by Lab. + Document revision time by vendor
- Total evaluation time can be reduced if the vendor has evaluation experience
- Most cases are of EAL 2-3

2. Analysis of Current Status(9/12)

3. Information and Communication Equipment Certification-3

Evaluation cost comparison between TTC and other CC Lab.

Security Level	TTC		CCTL of Europe		CCTL of North American	
	Evaluation	Consultant	Evaluation	Consultant	Evaluation	Consultant
Protection Profile	0.9	1.8	4	6	1.8	3.6
EAL 1	0.9	1.8	4	6	1.8	3.6
EAL 2	1.5	3	6.5	10	3	6
EAL 3	2.4	4.8	10	15	4.8	9.6
EAL 4	4.5	9	15	22.5	9	18

Units: million

Although the cost of TTC are much less than other CC lab., it is still a huge budget for small companies or some low-cost products

2. Analysis of Current Status(10/12)

3. Information and Communication Equipment Certification-4

Information and communication equipment operating status of NCC

- Administrative rules and relative technique regulations has been accomplished by NCC
  - Information and communication security products and protection profile examination operating points
  - Information and communication security equipments, protection profile testing laboratory management examination operating points
  - Information technique security evaluation common criteria (CC) technical regulation(Ver.2.2, Ver.2.3 and Ver.3.1)
- CC certificates issued by NCC
  - 1 protection profile
  - 2 products

2. Analysis of Current Status(11/12)

3. Information and Communication Equipment Certification-5

De Facto Industry Standards

Test Lab	ICSA (International Computer Security Association) of USA	NSS Labs of France	NBL (Network Benchmarking Lab) of Taiwan
Test aspect	Functionality	Performance	Stability/Reliability
Major SUT	Anti-Spam, Anti-Spyware, Anti-Virus, Firewalls, IPSec	IPS, Anti-Malware, Next Generation Firewall, UTM, WAF, VA	Firewall, Anti-Virus, IPS, UTM, Anti-Malware
Vendor applied	International leading vendors: IBM, Symantec, Kaspersky Lab, Fortinet, McAfee, Microsoft, CA, F-Secure, Avira	International leading vendors: IBM, McAfee, Fortinet, Juniper, Symantec, 3Com, CA, Cisco	Local vendors: TrendMicro, D-Link, ZyXEL, Alpha, Broadbwd, Nusoft, Axtronics, L7 Networks, Billion, Abocom, Draytek, RetiCorp, Lionic, Box-Sol
Other	Founded for 20 years	Founded for 18 years	Founded for 7 years, served over 100 vendors and evaluated over 500 products

2. Analysis of Current Status(12/12)

3. Information and Communication Equipment Certification-6

Problems

- High cost and long evaluation time

  Vendors are too small to compete with other international equipment manufactures.
- Need suitable certification standards for information security equipment in Taiwan?
- Is it necessary to stipulate government organization to purchase information security equipment of domestic manufacturers?
- Lack of funding to encourage the investment by domestic manufacturers of information and security equipment

3. Development Trends(1/6)

1. ISMS- 1

ISO/IEC 27001
（Information Security Management System (ISMS) requirements standard ）

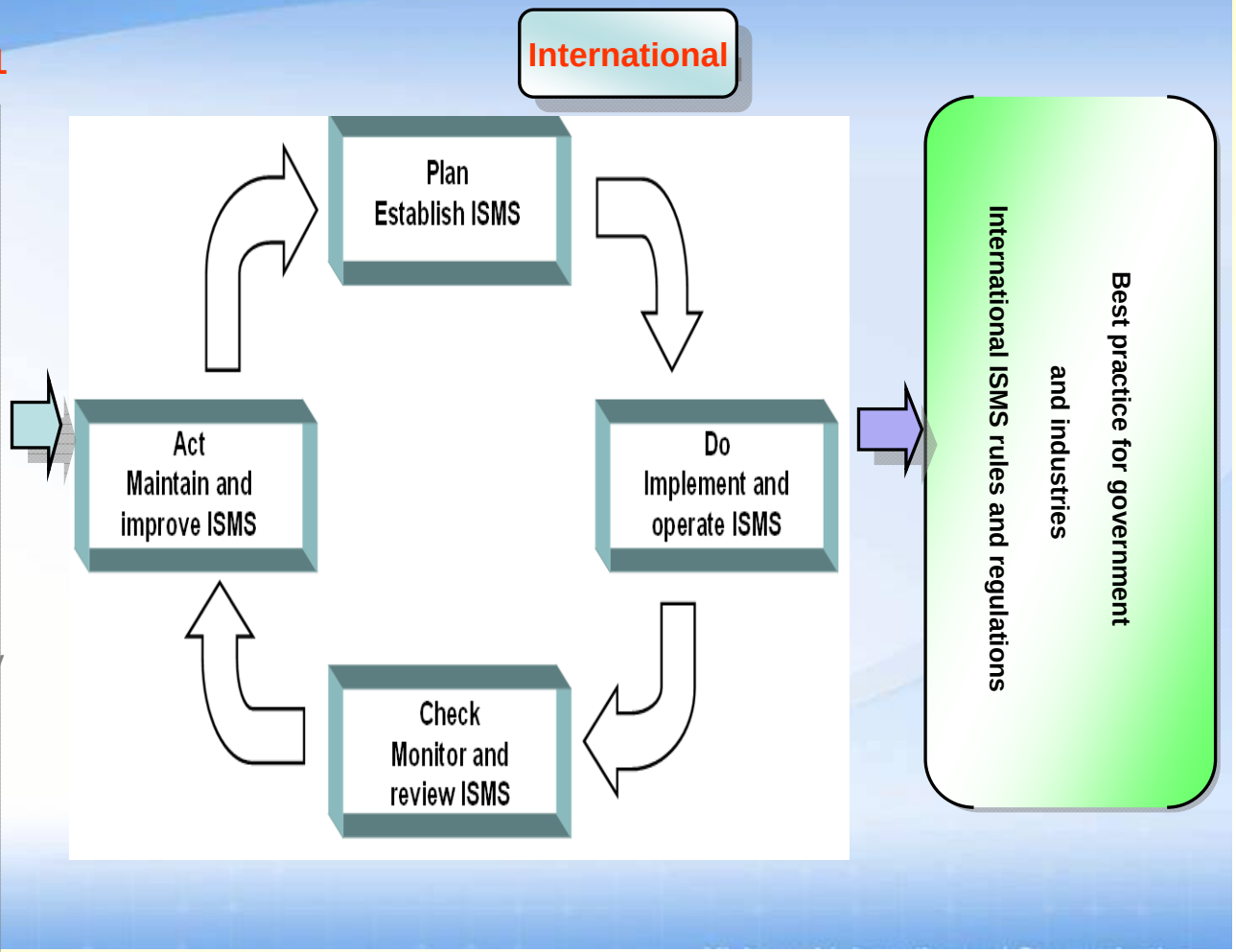
ISO/IEC 27002
（code of practice for information security management ）

ISO/IEC 27003
(ISMS implementation guide)

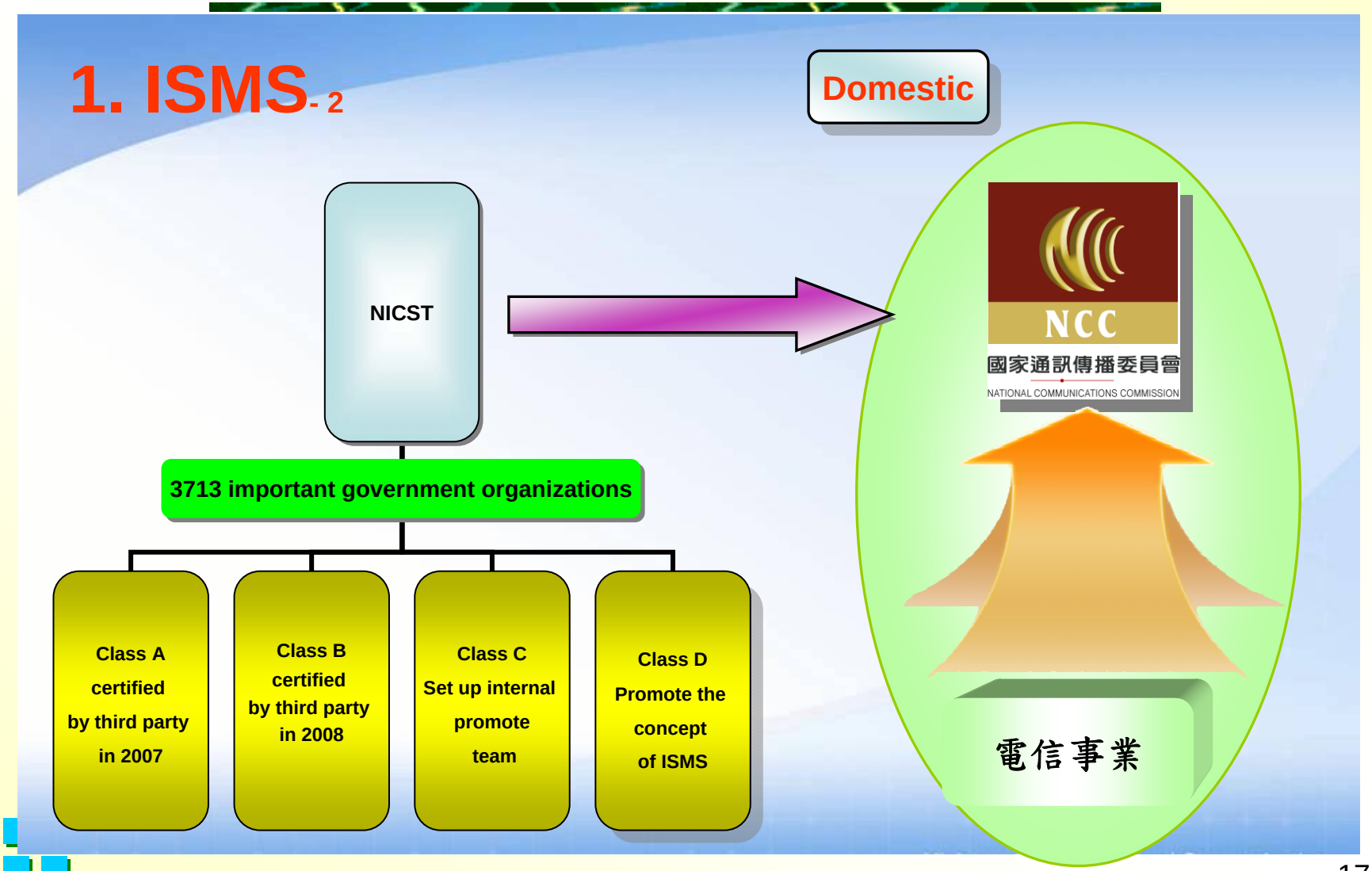
ISO/IEC 27004
(standard for information security management measurements)

ISO/IEC 27005
(designed to assist the satisfactory implementation of information Security based on a risk management approach)

ISO/IEC 27011
（information security Management guideline for telecommunications organizations ）



3. Development Trends(2/6)



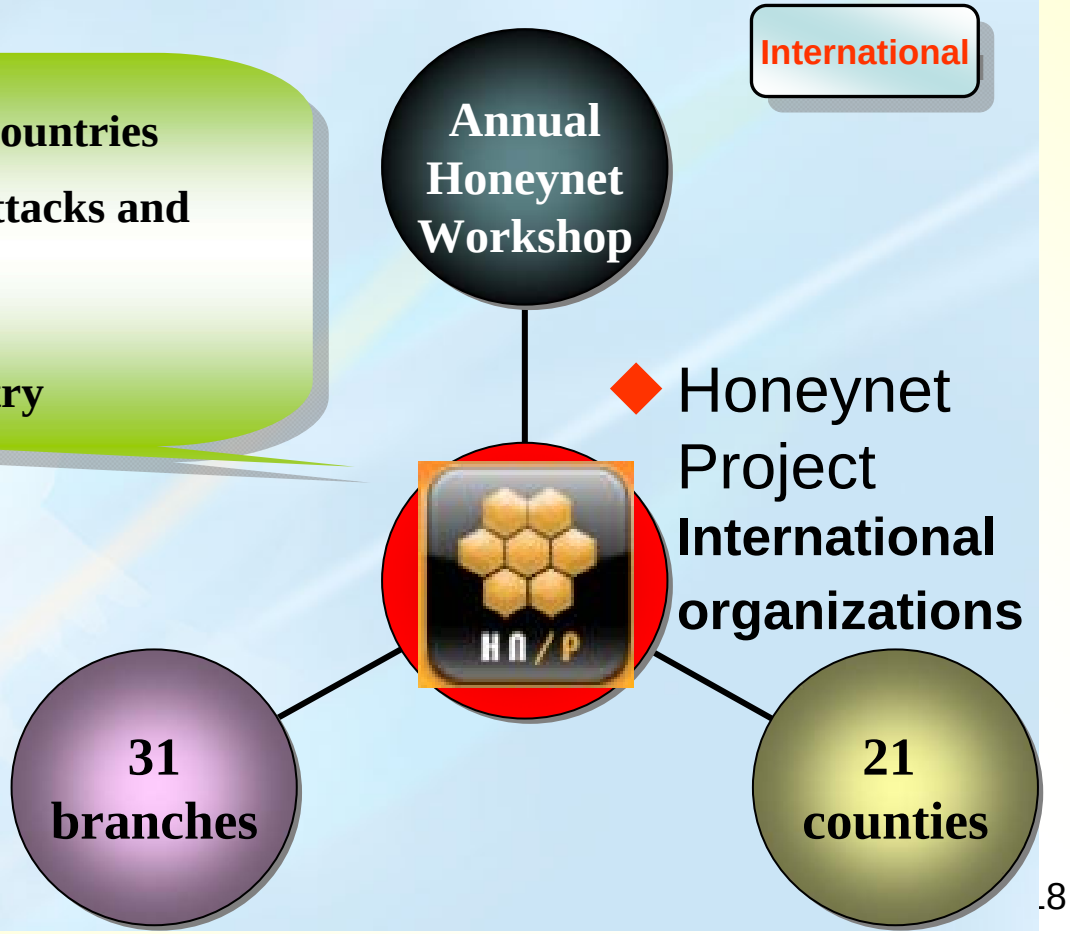
3. Development Trends(3/6)

2. Secure Protection of Information and Communication Infrastructure

☆Share attacks data in their countries

☆Analyze the new trends of attacks and threats

☆Understand the information security status in each country



3. Development Trends(4/6)

2. Secure Protection of Information and Communication Infrastructure

Plan of System Security Assurance and Anti-hacker Control Techniques Research
(STAG)

Domestic

Establish a Plan of Internet Anti-hacker Detection and Information Security Reporting System
(NCC)

Collect and analyze hackers' behavior

Alerting, reporting and responding the information security incidents

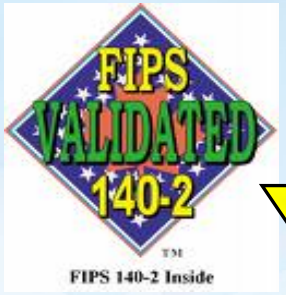
Avoid the expansion of information security incidents
Reduce the threat and attack from the internet
Improve overall information and communication infrastructure protection ability

3. Development Trends(5/6)

3. Information and Communication Equipment Certification-1

International

FIPS 140



CC part 1
CC part 2
CC part 3

International Organization for Standardization

ISO/IEC 19790

ISO/IEC 15408-1
ISO/IEC 15408-2
ISO/IEC 15408-3

3. Development Trends(6/6)

3. Information and Communication Equipment Certification-2

International

- International organization of CCRA:

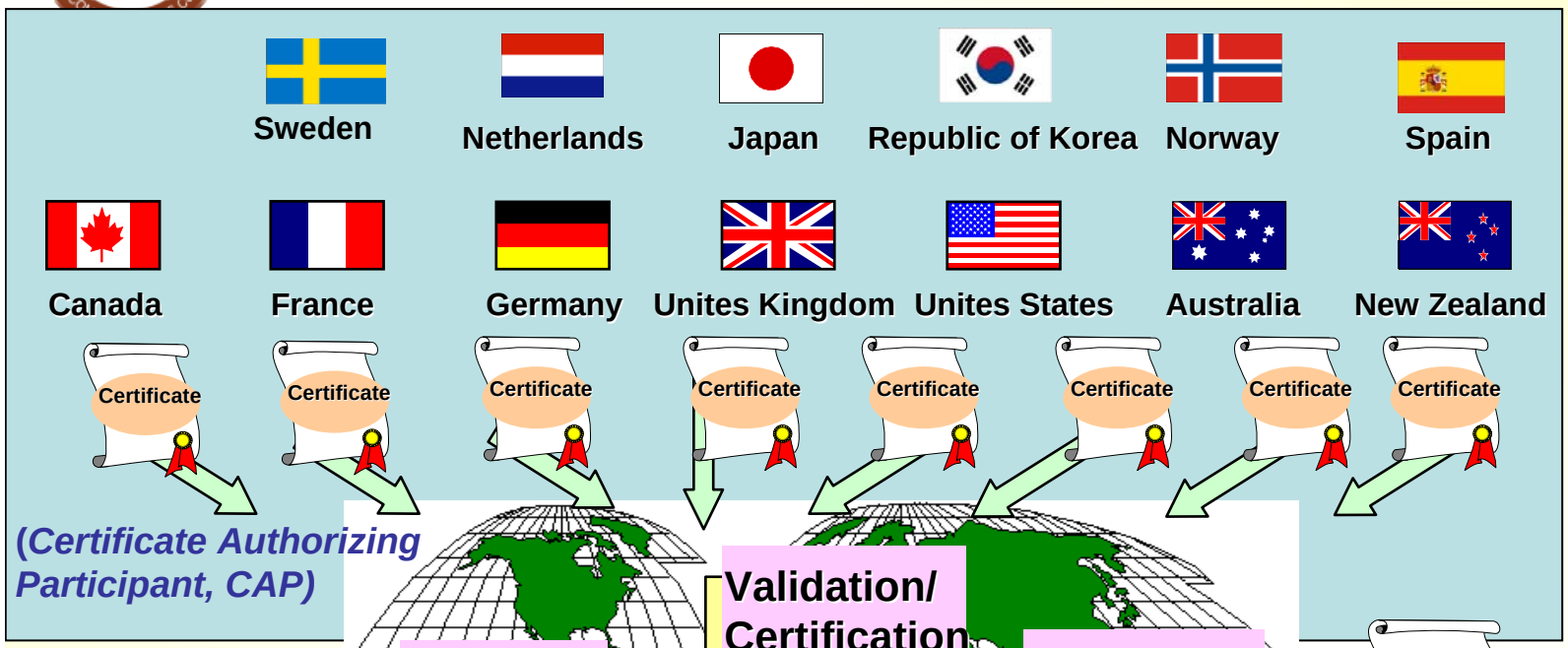
Responsible for promoting the common criteria for information technology related security standards

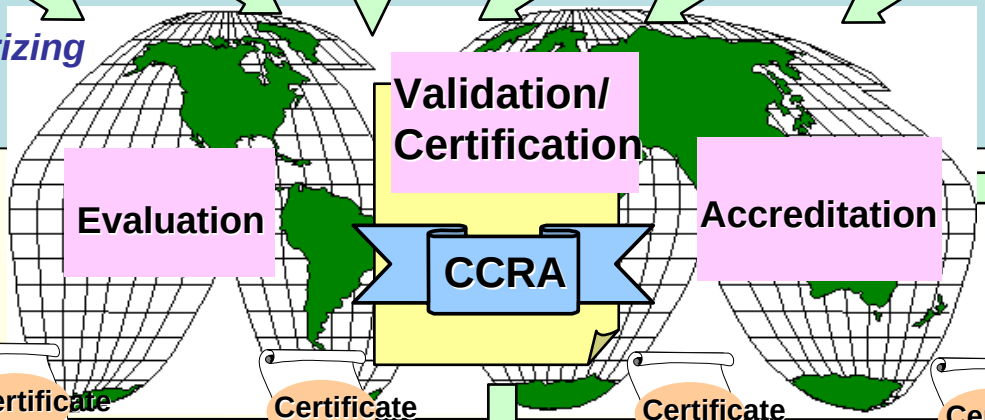
To ensure that the information and communication devices meet the security quality control, information and communication security requirements to reduce the potential threat

- There are currently 26 members
- To certify information and communication equipment is a voluntary decision
- In most countries, the information and communication security competent authority requires that the government agencies should follow the " Information and Communication Equipment Validated List " announced by the authority concerned for purchasing information and communication security equipment

CCRA: Arrangement on the Recognition of Common Criteria Certificates in the filed of Information Technology Security

CCRA Members





Finland
Greece
Italy
Israel
Austria
Hungary
Turkey
Czech Republic
Singapore
India
Denmark
Malaysia
Pakistan

CAP (13) + CCP (13) = 26

(Certificate Consuming Participant, CCP)

CCRA Certificates Issued

	USA	UK	Canada	France	German	Australia	Japan	Netherland	Norway	Korea	Spain	小計
1997	0	0	1	0	0	0	0					1
1998	1	6	0	0	1	0	0					8
1999	1	5	2	4	1	0	0					13
2000	2	7	2	11	0	1	0					23
2001	4	4	2	16	1	1	0					28
2002	26	7	2	12	8	2	2					59
2003	18	13	7	5	13	5	5					66
2004	31	6	6	22	49	3	17		1			135
2005	62	6	7	23	46	2	23		1			170
2006	39	4	4	21	44	1	43	1	0	53	4	214
2007	45	10	18	22	32	5	43	0	1	13	4	193
2008	43	7	15	29	56	4	71	0	0	2	9	236
2009	10	1	5	0	12	1	3	0	1	0	0	33
合計	282	76	71	165	263	25	207	1	4	68	17	1,179

Until 03/23/2009

- **Countries issued 1~6 certificates in the first year and year-on-year growth**
- **In terms of the number of certificates issued, the top three countries are USA, Germany and Japan**
  - 1st USA:282 (in 12years)→23 per year in average
  - 2ndGermany:263 (in 12years) → 21 per year in average
  - 3rdJapna:207 (in 8years) → 25 per year in average

4. Strategies(1/5)

1. Introduce the Mechanism of ISMS

- telecom industry shall ensure the security of data, system, equipment and network for consumer's interest by implementing ISMS
- telecom industry shall maintain and improve their security by management and auditing
- telecom industry shall perform internal audit in advance
- telecom industry shall be certified through an appointed third party

4. Strategies(2/5)

2. Improve the Protection Ability of Information and Communication Security of telecom industry

- Deploy honeynet for telecom industry client to detect and collect the attacks activities and malwares in network
- Build anti-hacker detection and information security incidents reporting system to alert, report and respond to those incidents

4. Strategies(3/5)

3. Promote Certification Mechanisms of Information and Communication Equipment

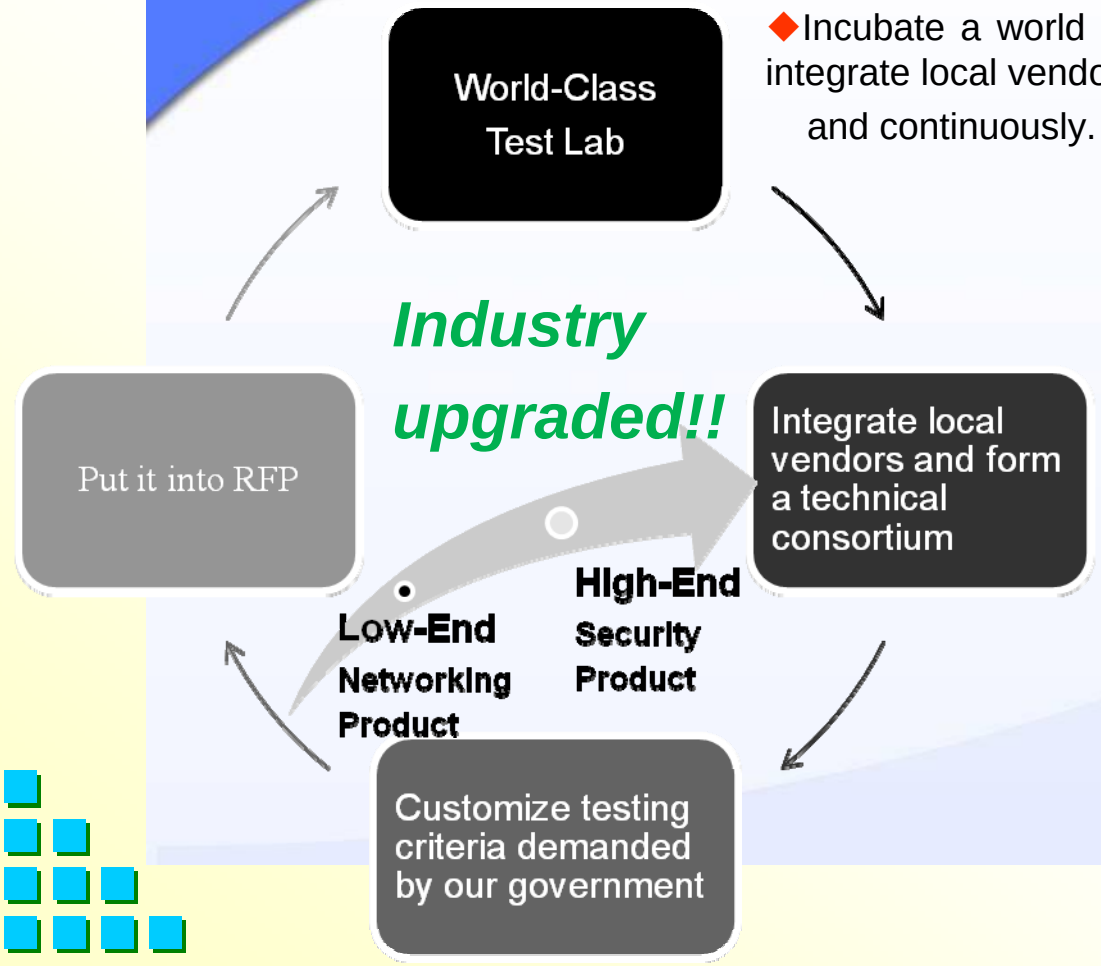
- Continue to provide the international Common Criteria (CC) certification services Domestic information and communication equipment vendors, if they are willing to apply for international CC certification, they can make full use of established domestic CC certification capacity to assist to promote the domestic information and communication security equipment globally
- Improve the information and communication security testing laboratory to meetthe needs of industry
- Plan domestic certification standard of information and communication security equipment Simplify certification items; Reduce evaluation costs and shorten the time to certify; Introduce government procurement standard of certified equipment as soon as possible
- Encourage government agencies to purchase certified information security products under the GPA of WTO
- Develop the complementary measure of encouraging domestic manufacturers to invest in security equipment R&D.

4. Strategies(4/5)

3. Promote Certification Mechanisms of Information and Communication Equipment -2

Complementary Strategy to Upgrade the Industry

◆Incubate a world class test lab The test lab can be used to integrate local vendors to enhance the technologies substantially and continuously.



◆Many networking products from Taiwan have outstanding results in the world, ex. SOHO router has more than 50% of market share worldwide.

◆However, security products still have room for improvement, ex. only shares 1% of the local market and 3% of the worldwide market.

4. Strategies(5/5)

4. To Promote Information and Communication Security Awareness and Publish the Information of Certificated Equipment

- Establishment of information and communication promoting website
  - To provide update information and communication infrastructure related security information and knowledge, enhance the user's awareness, and prevent potential threats of information and communication security
  - Publish the information and communication equipment certified list to provide government agencies with choices of the certificated information and communication equipment

5. Action Plan(1/5)

1. Establish ISMS of the telecom industry

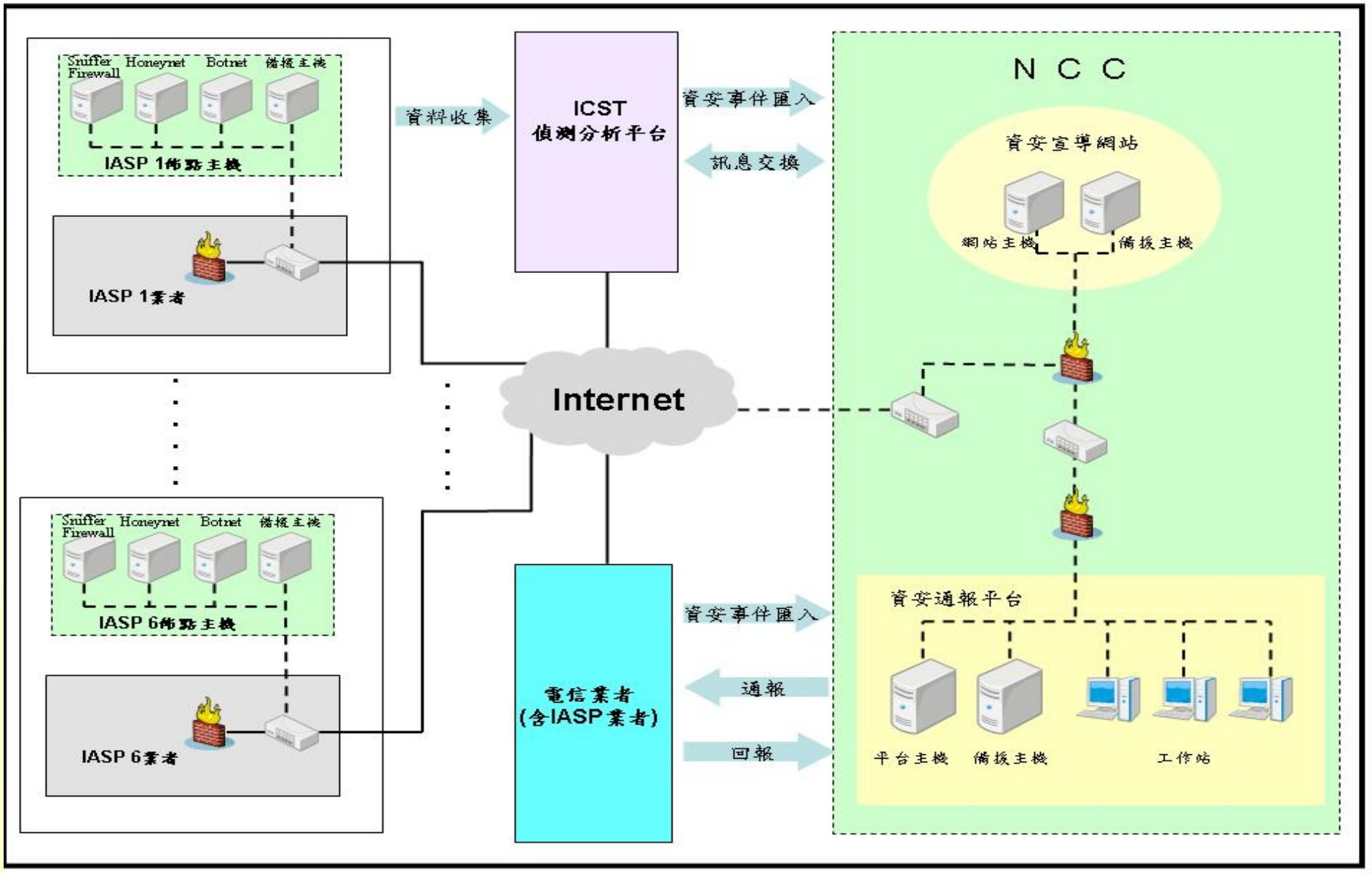
- The 16th action plan of national Information and communication security development program: ” Authorized in accordance with laws and regulations to promote the use of third-party evaluation utilities ”
- Implementation points
  - Promoting the institutions to establishment internal audit system and to implement
  - Promoting information and communication security as one of the internal control cycle of business
  - Guiding the institutions to have a third party vendor to conduct an external audit of information and communication security
  - NCC will establish the information security system management mechanism of telecommunications business
- We will revise the relevant provisions of the Telecommunications Act to regulate the telecom industry to implement the information and communication security management and information security internal audit; and appointed by an trusted third party to conduct an information and communication security external audit and implement the security measures to detect security events for timely notification and response.

5. Action Plan(2/5)

2. Build Internet Anti-hacker Detection and Information Security Reporting System

- The 14th action plan of national information and communication security development program: ” The development of critical information infrastructure protection strategies ”
- Implementation points
  - Establishing the critical infrastructure of information security prevention and early warning, detection, response, crisis management capability
  - Planning and designing IASP (Internet Access Service Provider) Union and the reporting mechanism
  - Building “information security communications reporting and responding platform” of telecommunications network, including information sharing platform, information sharing and portal interface
- The Internet anti-hacker detection and information security reporting system by NCC will be completed by 2010, which can detect and analyze the available Internet hacker attacks to effectively responding, alerting and reporting information security events
  - With CERT, SOC and ISAC multi-functional platform

Internet anti-hacker detection and information security reporting system



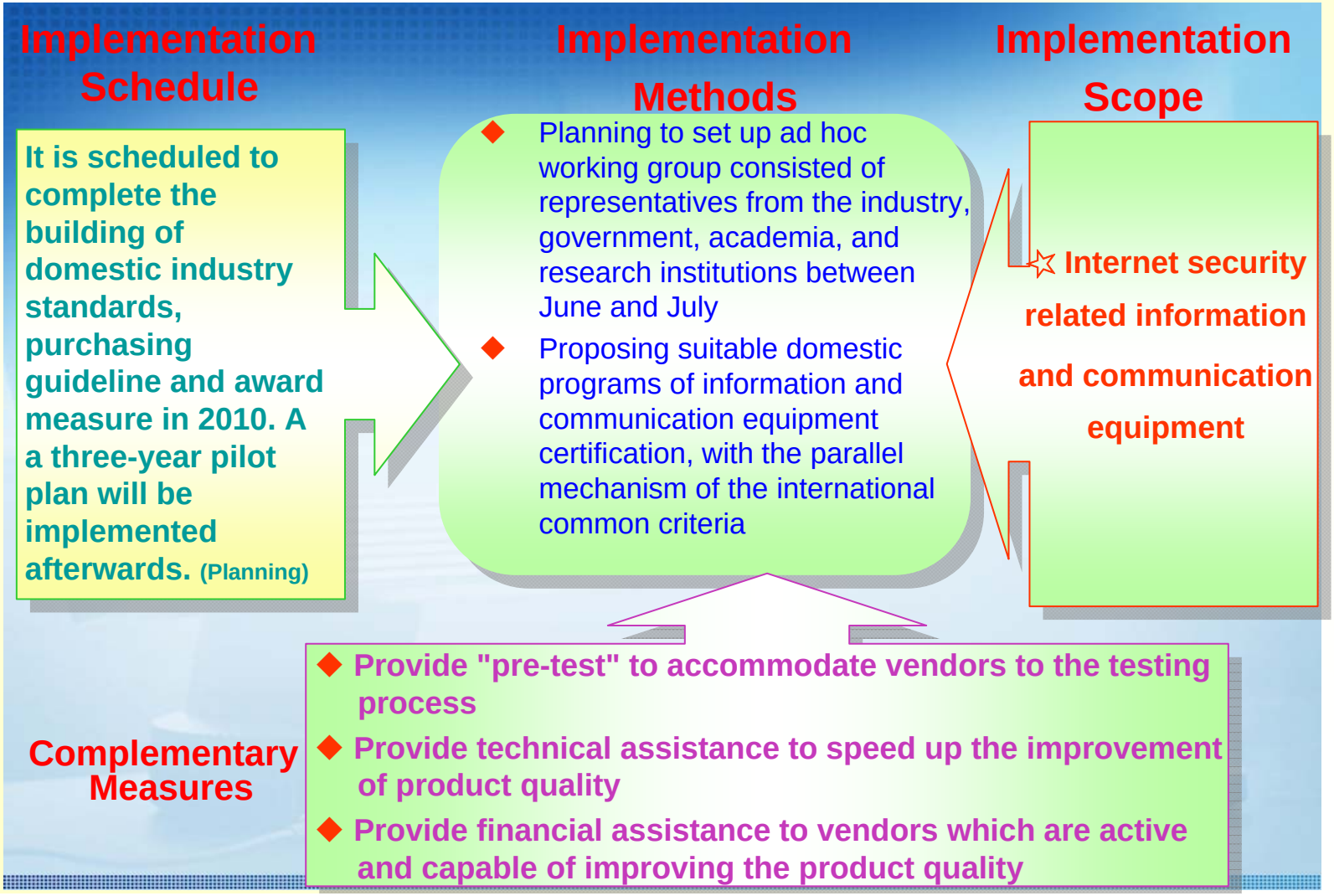
5. Action Plan(3/5)

3. Promote the Government Agencies to Purchase the Certificated Information and Communication Equipment-1

- The 9th action plan of national information and communication security development program: “Promoting the government agencies to purchase certificated information and communication equipment”
- Implementation points
  - Establish confidential and sensitive equipment items of information and communication security
  - Conduct certification training of information and communication security
- Encouraging government agencies to purchase certificated information and communication equipment; Developing standards for domestic industry, and then promote the pilot plan

5. Action Plan(4/5)

3. Promote the Government Agencies to Purchase the Certificated Information and Communication Equipment-2



5. Action Plan(5/5)

4. Establishment of Information and Communication Promoting Website

- Information and communication promoting website will be built in “Internet Anti-hacker Detection and Information Security Reporting System”, which will be set up in 2010
  - Provide relevant information and security information for information sharing and education purpose.
  - Publish “Information and Communication Equipment Certified List” to provide government agencies the latest information of certified information and communication equipment

6. Discussions

1. How to implement applicable ISMS for the domestic telecom industry?
2. How to improve the Internet's prevention ability of information and communication security?
3. How to develop a world-class testing lab in the field of information and security?
4. How to promote the applicable certification mechanism of information and communication security for the domestic environment?

Thanks for your attention!