แนวทางการพัฒนา Information Security Professional ในประเทศไทย

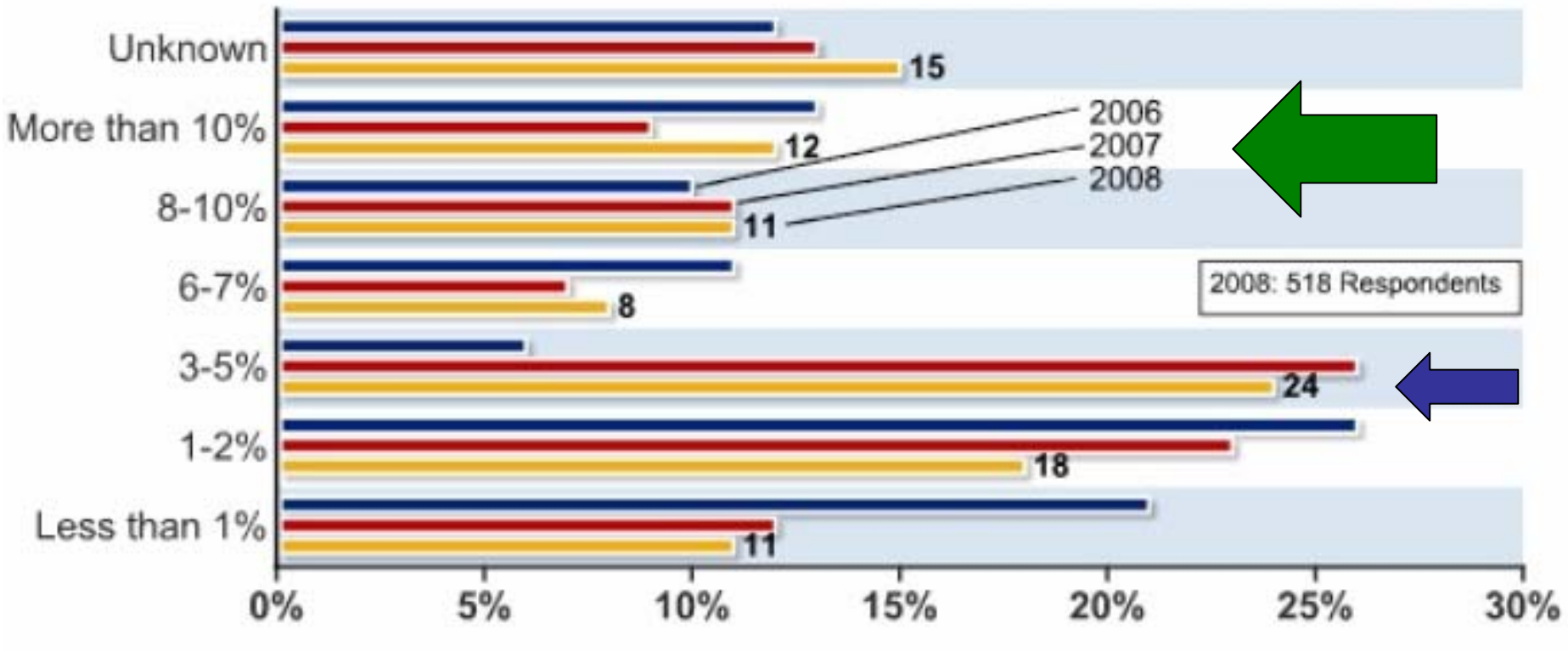
โดย

Thailand Information Security Association (TISA)

Agenda

1) Global Information Security Professional Situation
2) Current Thailand Information Security Professional Situation
3) Information Security Essential Body of Knowledge (EBK) from Department of Homeland Security (DHS)
4) TISA and Information Security Professional Development Program
5) EBK and Enterprise Information Security Capability : The Future Roadmap

Percentage of IT Budget for Security

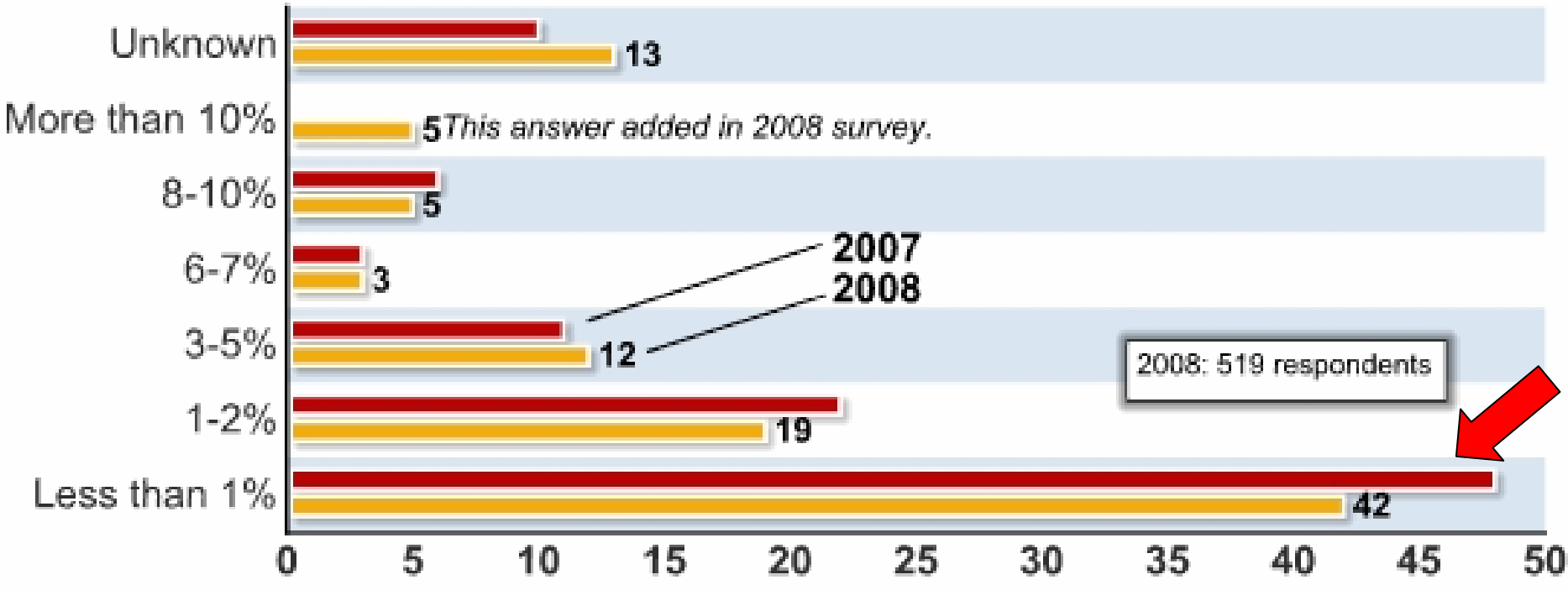


Most organizations put it around 3-5%

10%+ seem to be the norm

Source: 2008 CSI Computer Crime & Security Survey

Awareness Training as a Percentage of Security Budget



Organizations put too small effort on the weakest link – human. The misperception that IT security is only the responsibility of IT dept. negatively influence the implementation, Only if the perception is change, the figure will.

Source: 2008 CSI Computer Crime & Security Survey

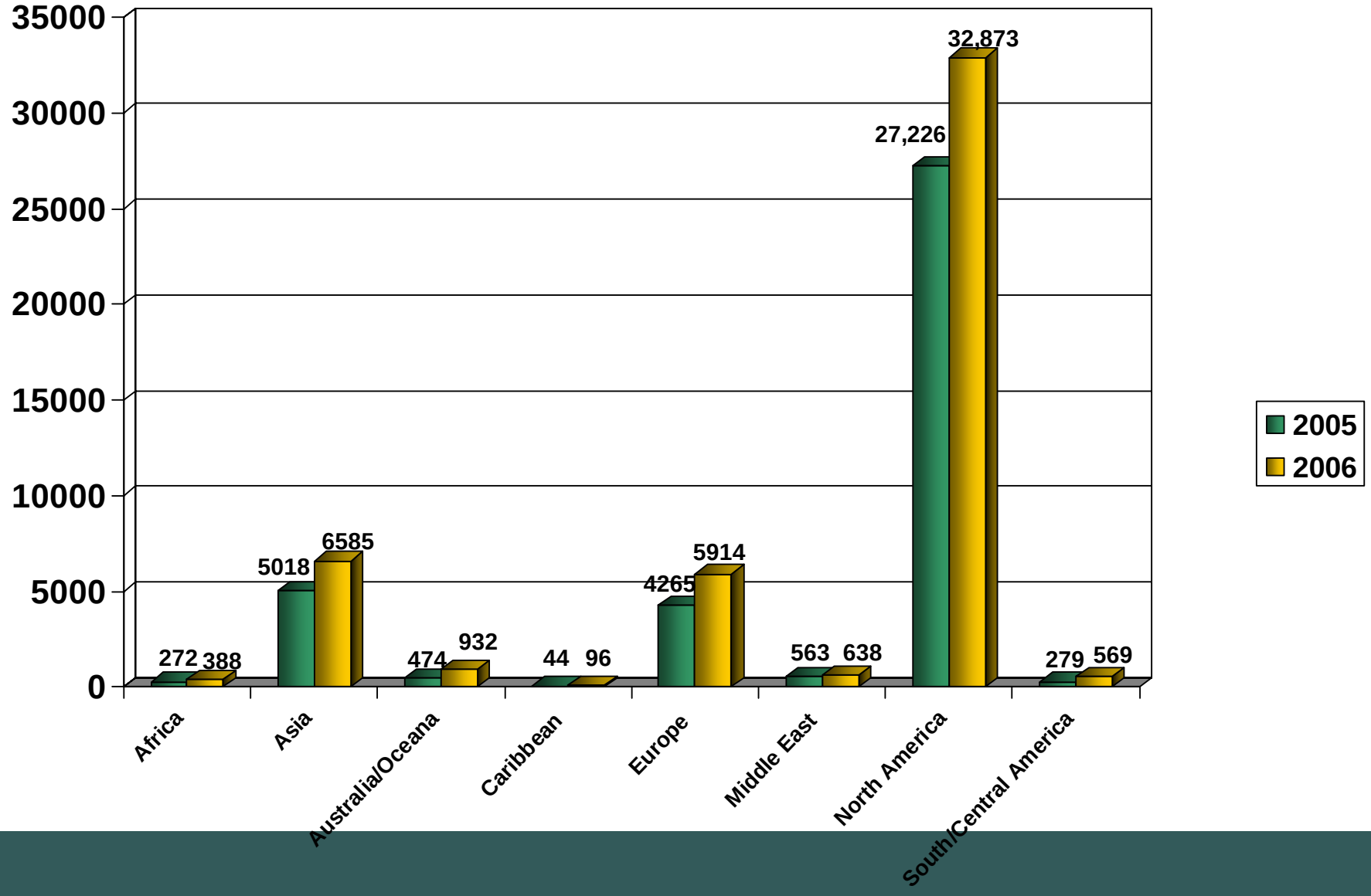
Leading IT and InfoSec Professional Certification Institutes

(ISC)² - Insight from the Workforce

- Established in 1989 - Non-profit consortium of industry leaders dedicated to educating and certifying information security professionals worldwide
- 57,000 members in 135 countries
- Consultation and Research:
- (ISC)2 CBK® – World's largest taxonomy of information security topics
- Board of Directors - top information security professionals worldwide.
- CISSP and SSCP are accredited ANSI/ISO/IEC Standard 17024 and were the first technology-related credentials to receive this accreditation.

(ISC)² Around the World – Membership Distribution

(ISC)² has members in 133 countries across the globe



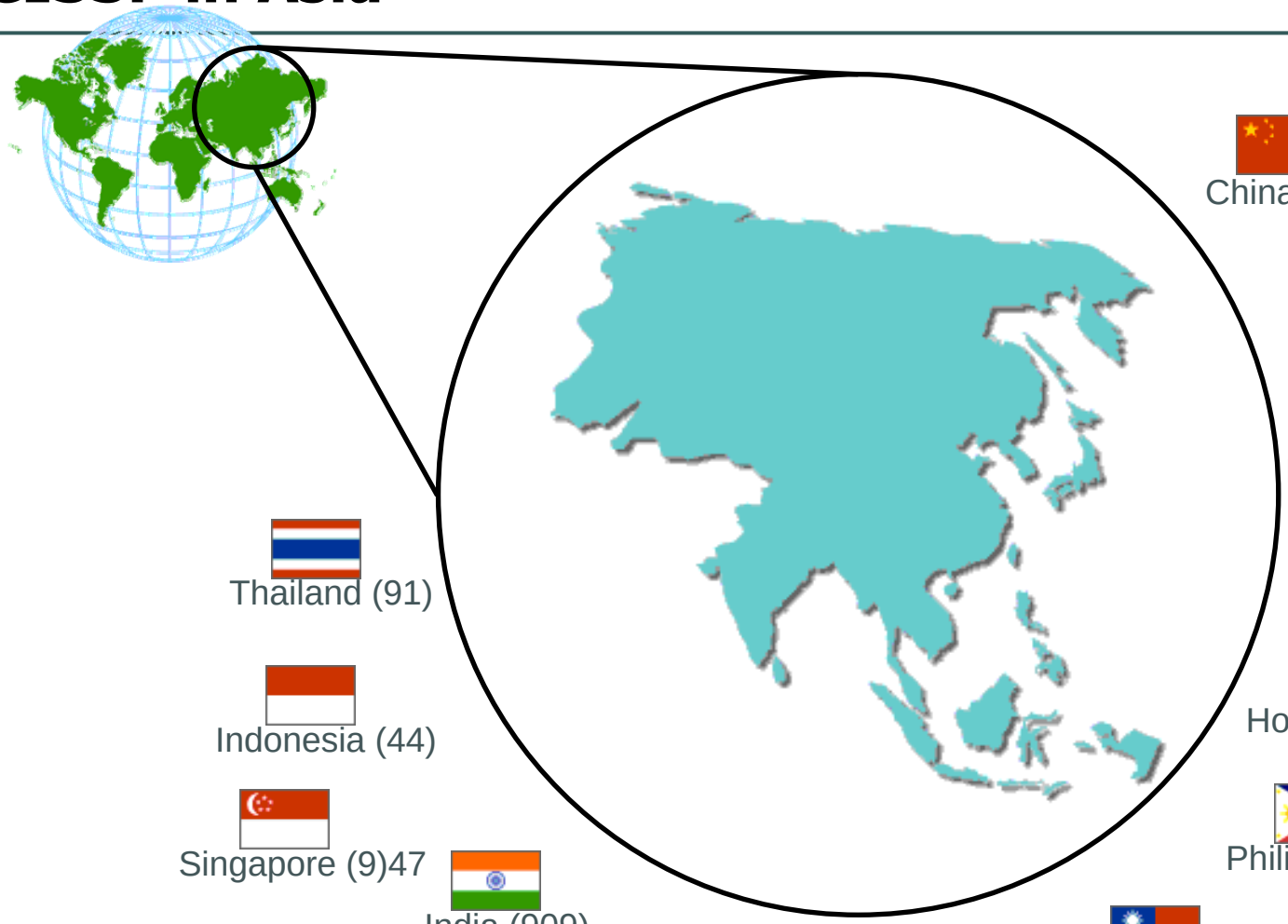
Membership Milestones in Asia-Pacific

8 economies have at least 200 members *(as of 30/09/07)*

- South Korea – 1,991
- Hong Kong – 1,315
- Singapore – 953
- India – 923
- Australia – 898
- Japan – 883
- China – 400
- Taiwan – 244

CISSPs in Asia- South Korea: Highest population of CISSP in Asia

As of: 30/SEPT/07



China (400)

Macao (8)

Korea, South (2,003)

Japan (883)

Hong Kong (1,311)

Philippines (112)

Taiwan (238)

Malaysia (177)

Sri Lanka (35)

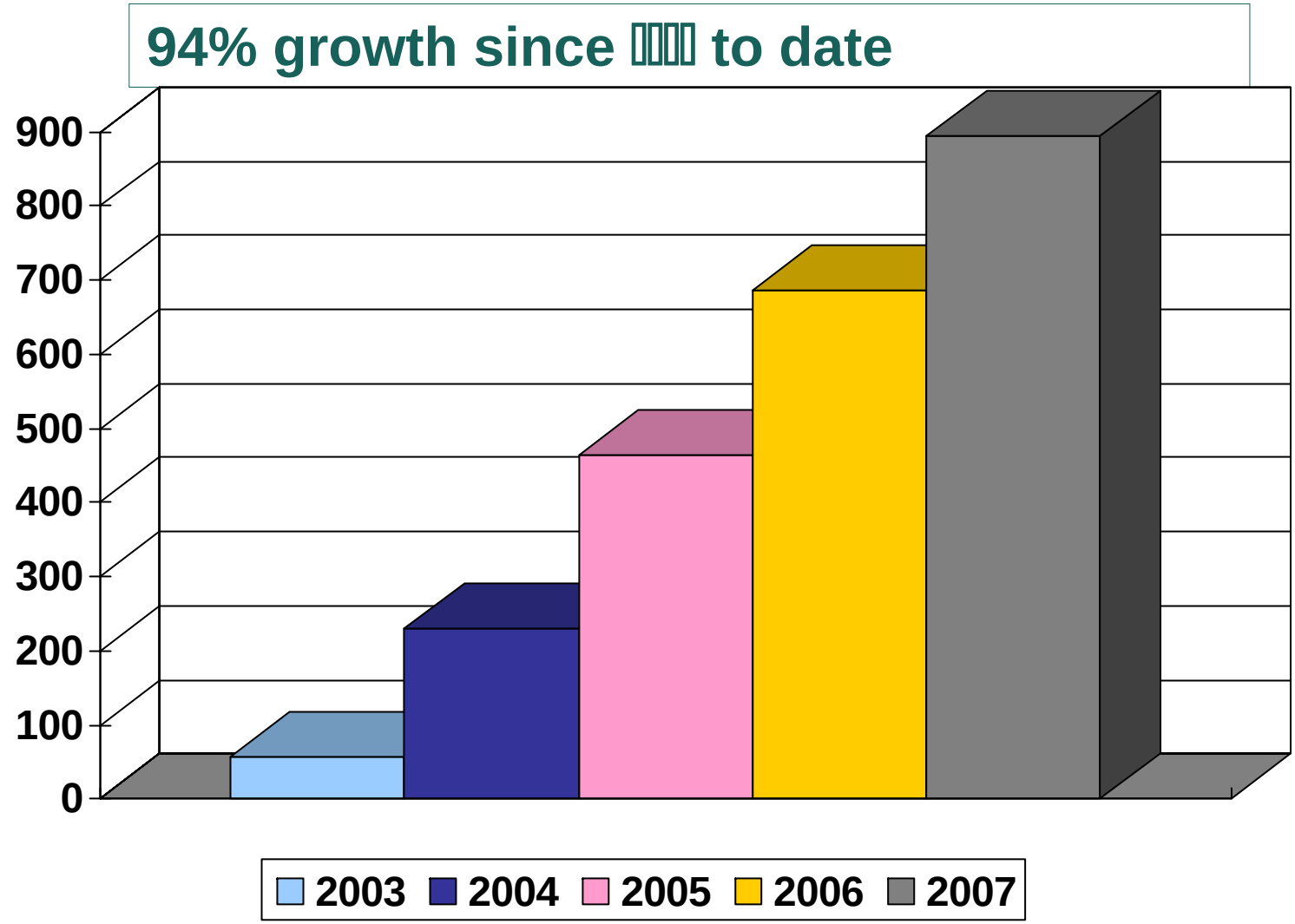
India (909)

Singapore (9)47

Indonesia (44)

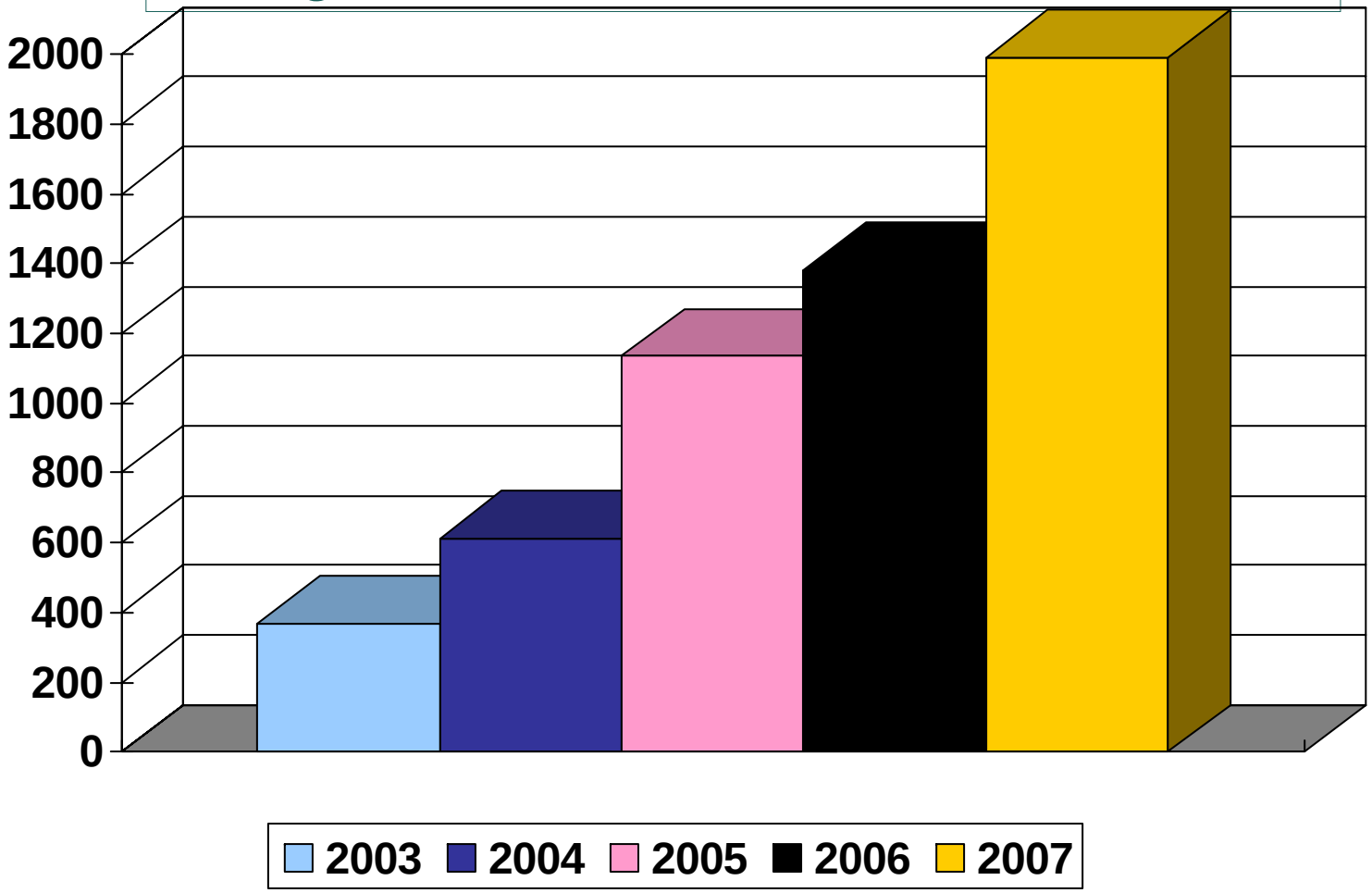
Thailand (91)

Membership Growth in Japan



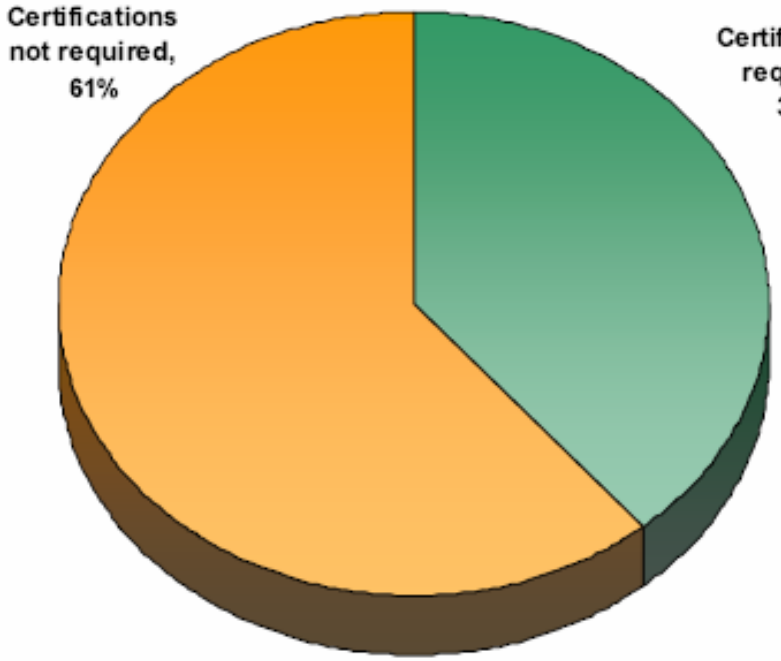
Membership Growth in Korea

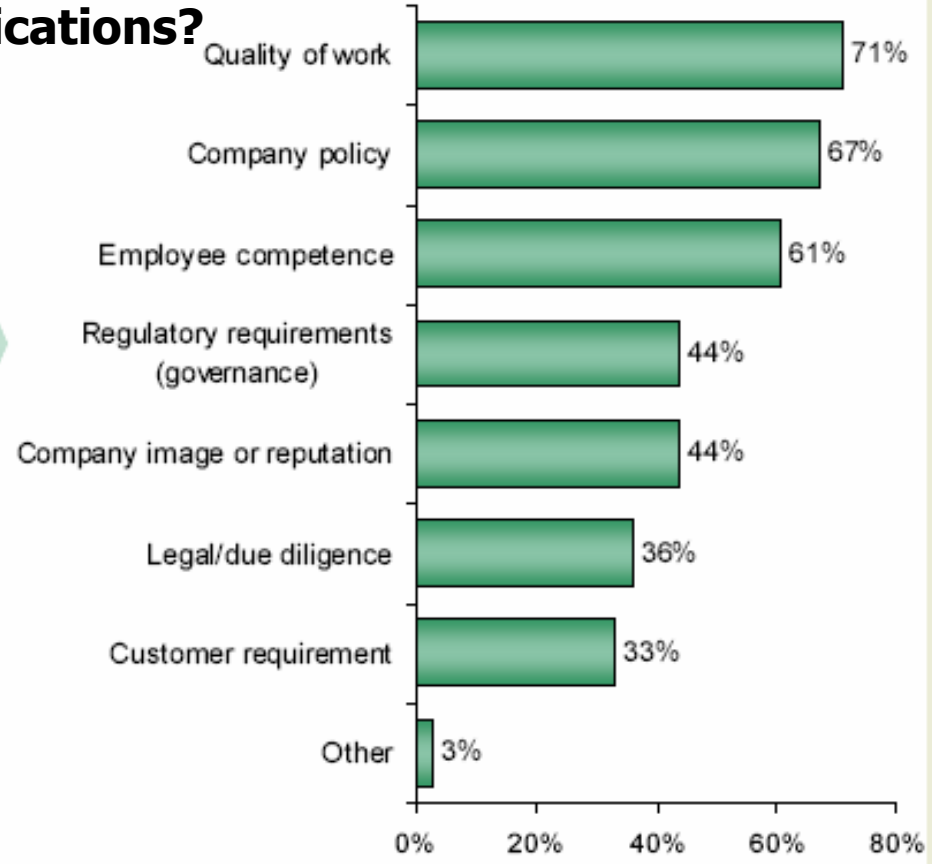
82% growth since 2003 to date



Does your organization require its staff to have information security certification?

IF YES - What are all the reasons your organization requires staff to have information security certifications?



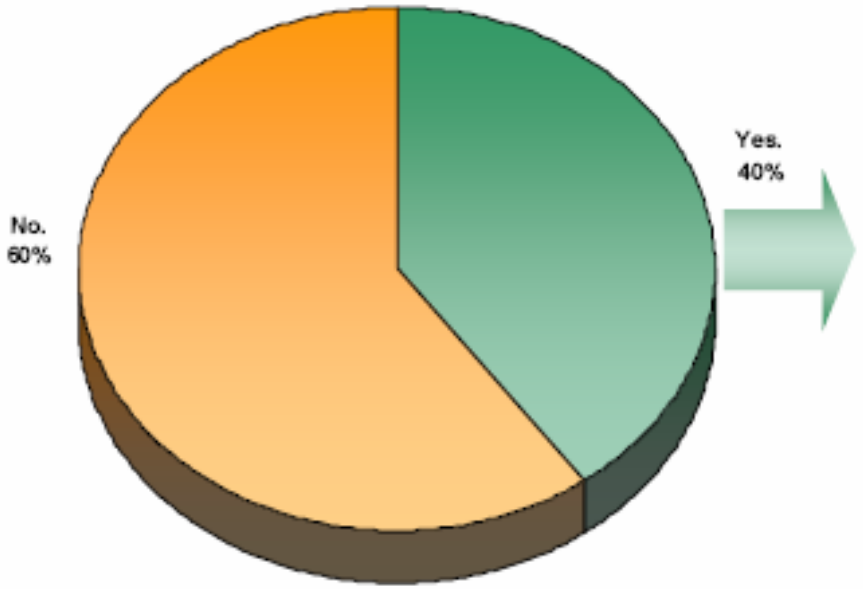


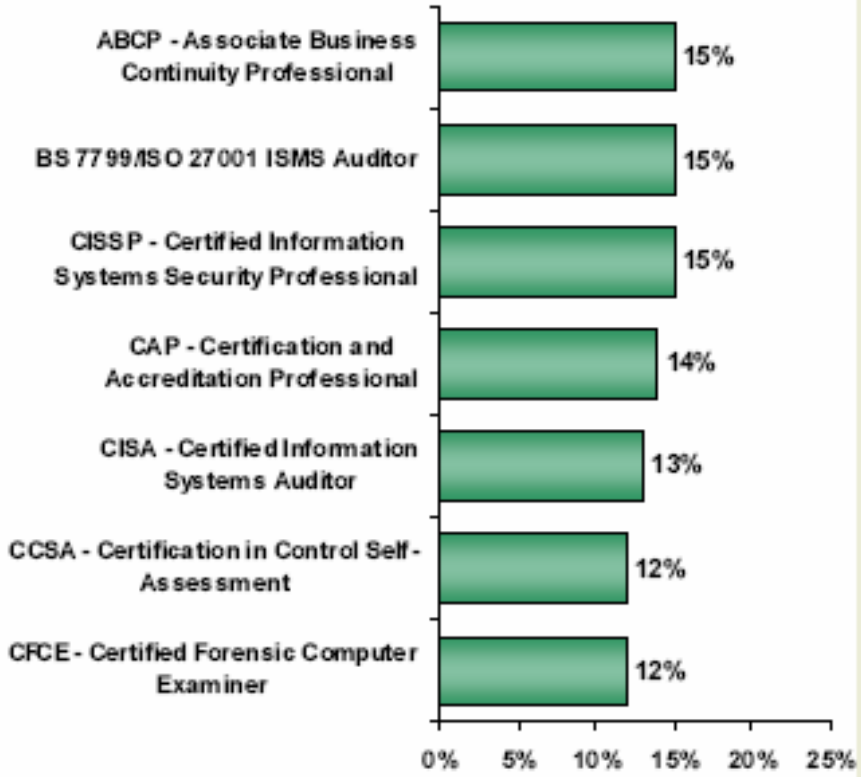
Base: n=7,548 (ISC)² members and non-members

Plans to Acquire Additional Certifications

Are you planning to acquire additional security certifications in the next 12 months?

IF YES - Which additional vendor neutral security certifications are you planning to acquire or renew in the next 12 months?





Base: n=7,548 (ISC)² members and non-members

(ISC)2 Global Membership (as of June,08)

(ISC)² Members Worldwide:	
CISSP	**58,080**
ISSAP	**770**
ISSEP	**355**
ISSMP	**675**
CAP	**380**
SSCP	**666**
Associate of (ISC)²	**831**
(ISC)2 Members in Thailand:	
CISSP	**98**

ISACA Global Membership (as of June,08)

CISA Members Worldwide:

CISA	45,000
CISM	8,000
CGEIT	364

CISA Members in Thailand:

CISA	135
CISM	24
CGEIT	2

Difference among IA, IT Audit, Infosec Audit and System Security Audit

	Internal Audit	IT Audit	InfoSec Audit	System Security Audit
Audit scope	Enterprise	IT	IS Security	System specific
Audit Framework	COSO	CobiT	ISO27001	NIST(SPP800-53A,SP800-115), NSA:IAM, OSSTMM
Audit objective	CG	ITG, IT/Biz Alignment	Security Governance	System security, hardening
Professional Cert.	CIA	CISA	CISSP, IRCA:ISMS	NSA:IAM,OPST, OPSA, CEH, SSCP, CSSLP
etc.				

Information Technology (IT) Security

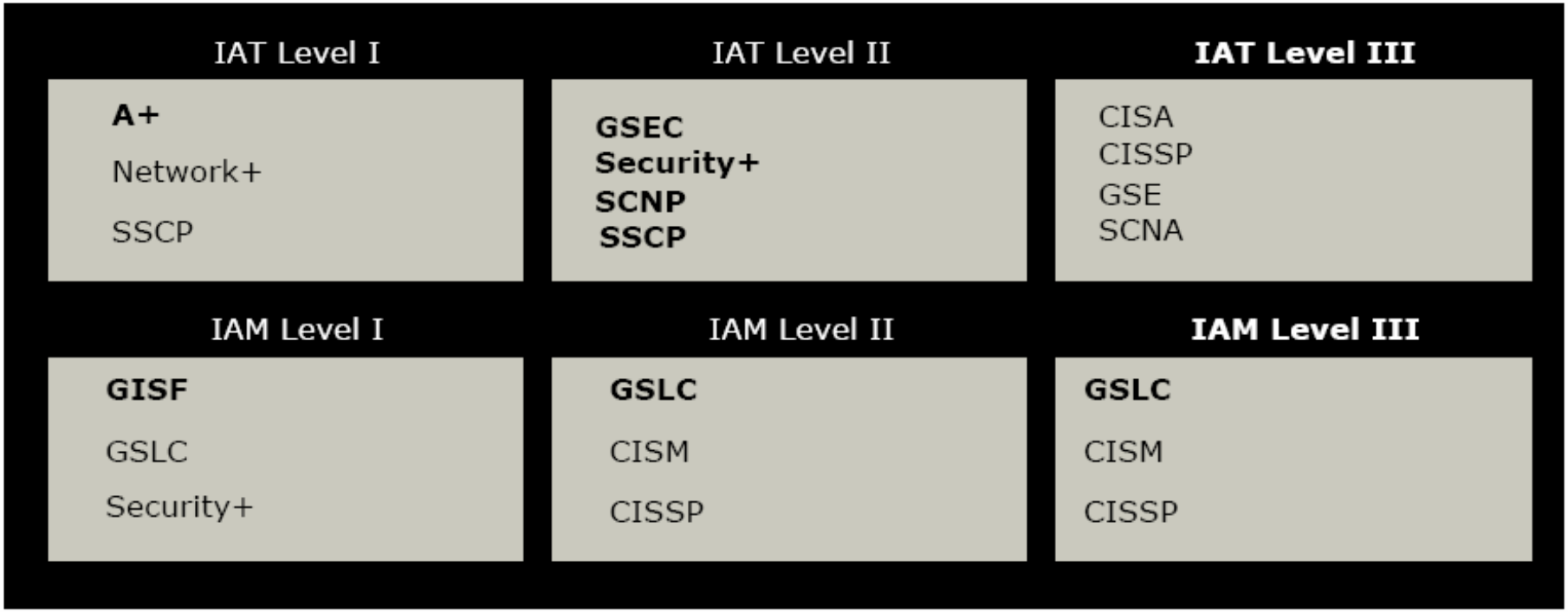
Essential Body of Knowledge (EBK)

A Competency and Functional Framework for IT Security Workforce Development

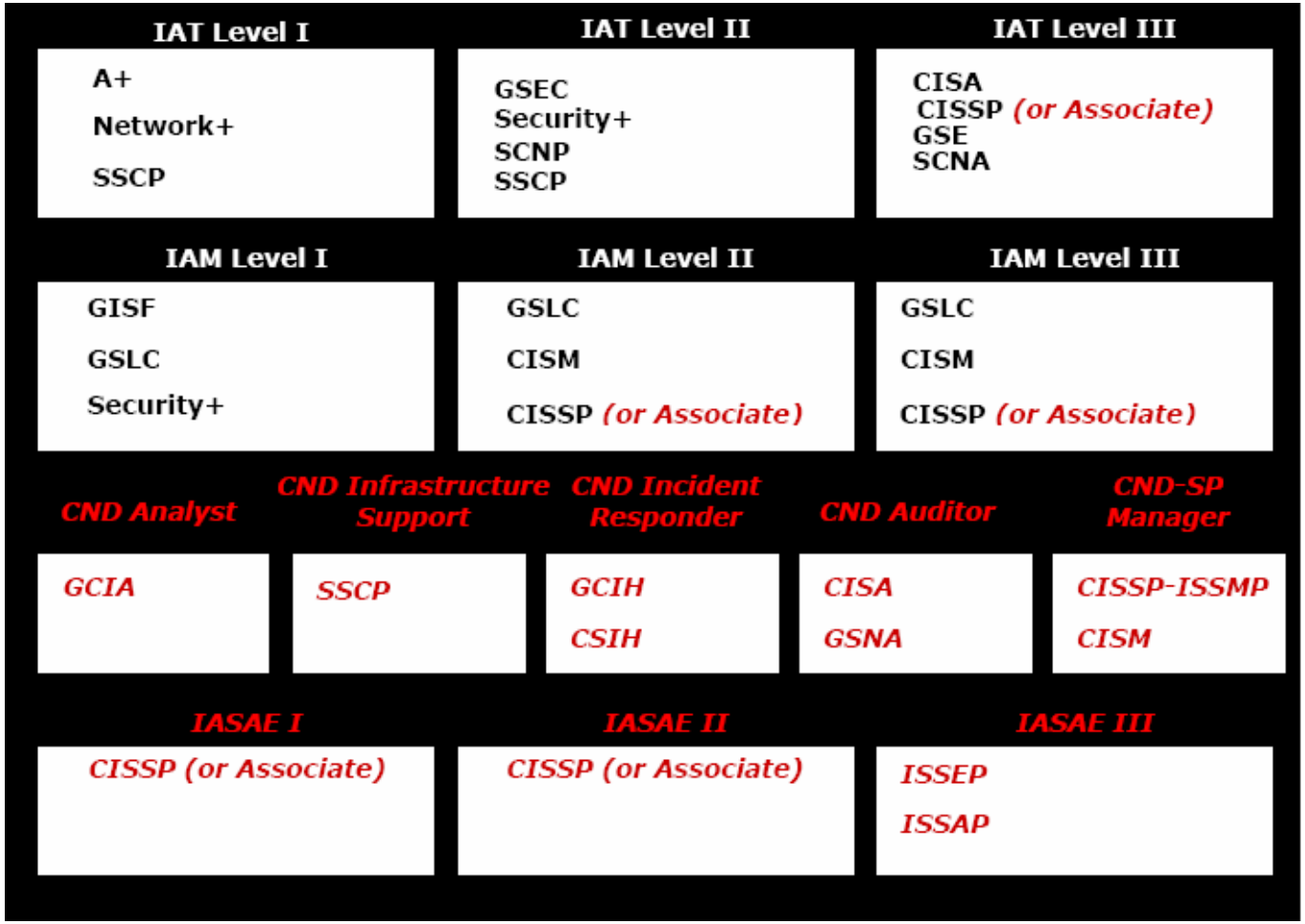
September 2008

United States Department of Homeland Security

DoD 8570.01-M
Information Assurance Workforce Improvement Program
December 19, 2005



DoD 8570.01-M
Information Assurance Workforce Improvement Program
May 15, 2008



Why was the EBK established?

- Rapid evolution of technology
- Various aspects and expertise are increasingly required
- Standard or common guideline in recruiting, training and retaining of workforce
- Knowledge and skill baseline
- Linkage between competencies and job functions
- For public and private sectors

Purpose of EBK

- Articulates functions that professionals within the IT security workforce perform in a common format and language.
- Provides a reference for comparing the content of IT security certifications, which have been developed independently according to varying criteria
- Promotes uniform competencies to increase the overall efficiency of IT security education, training, and professional development
- Offers a way to further substantiate the wide acceptance of existing certifications so that they can be leveraged appropriately as credentials
- Provides content that can be used to facilitate cost-effective professional development of the IT security workforce, including skills training, academic curricula, and other affiliated human resource activities.

How was this built?

- The President's Critical Infrastructure Protection Board (PCIPB) was established in October 2001
- PCIPB created the IT Security Certification Working Group (ITSC-WG)
- 2003, the President released the *National Strategy to Secure Cyberspace*
- 2003, DHS-NCSD was established to act as a national focal point for cyber security
- Lead by the Department of Homeland Security, National Cyber Security Division (DHS-NCSD) together with academia, government, and private sector
- DHS-NCSD introduced this **first draft** to a broader audience of SMEs in **January 2007**
- It will be re-evaluated approximately every two years

EBK Development Process

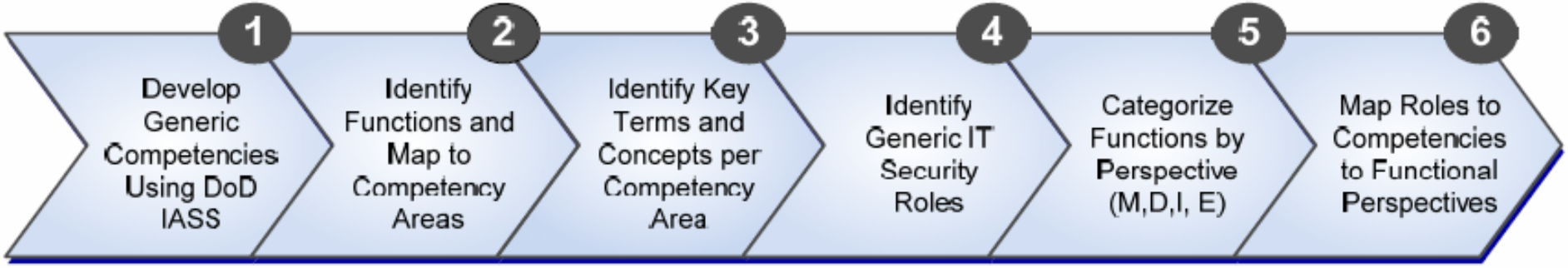
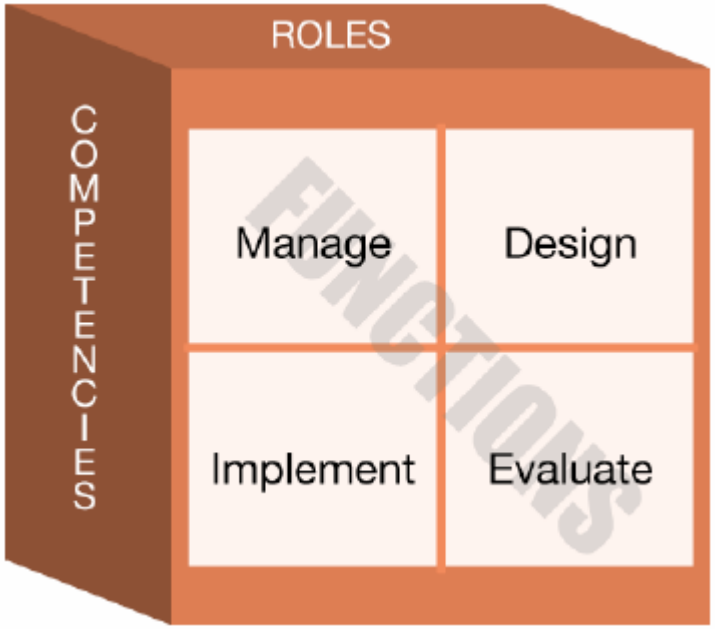


Figure 1-1: Competency and Functional Framework Development Process

Refer to 53 Critical Work Function (CWF) from DoD IASS

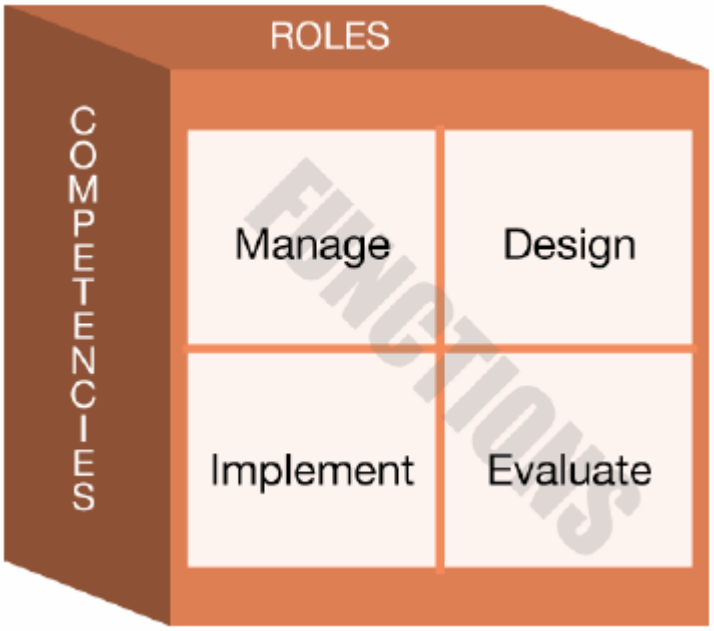
Key Divisions

- 4 functional perspectives
- 14 competency areas
- 10 roles



Functional Perspectives

1. Manage
2. Design
3. Implement
4. Evaluate



IT Security Roles

1. Chief Information Officer
2. Digital Forensics Professional
3. Information Security Officer
4. IT Security Compliance Officer
5. IT Security Engineer
6. IT Security Professional
7. IT Systems Operations and Maintenance Professional
8. Physical Security Professional
9. Privacy Professional
10. Procurement Professional

Competency Areas (MDIE in each)

1. Data Security
2. Digital Forensics
3. Enterprise Continuity
4. Incident Management
5. IT Security Training and Awareness
6. IT System Operations and Maintenance
7. Network and Telecommunication Security
8. Personnel Security
9. Physical and Environmental Security
10. Procurement
11. Regulatory and Standards Compliance
12. Security Risk Management
13. Strategic Security Management
14. System and Application Security

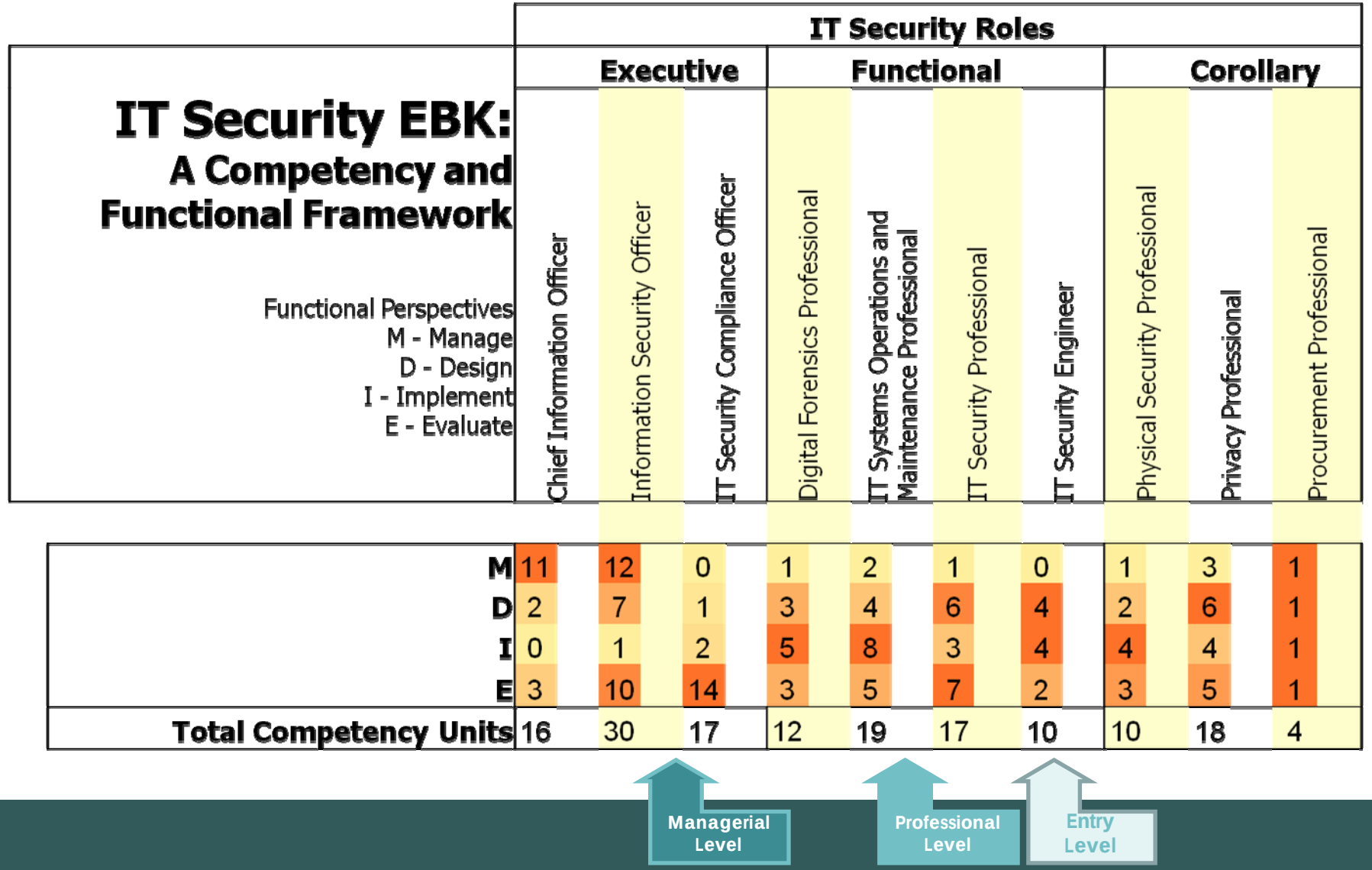
IT Security EBK:
A Competency and Functional Framework

Functional Perspectives
M - Manage
D - Design
I - Implement
E - Evaluate

IT Security Competency Areas	IT Security Roles																							
	Executive						*Functional*										*Corollary*							
	Chief Information Officer		Information Security Officer		IT Security Compliance Officer		Digital Forensics Professional		IT Systems Operations and Maintenance Professional		IT Security Professional		IT Security Engineer		Physical Security Professional		Privacy Professional		Procurement Professional	
1 Data Security	M		M	D							M	D		D				D		
				E		E			I	E		E		E				E		
2 Digital Forensics			M	D			M	D												
						E	I	E	I											
3 Enterprise Continuity	M		M							D						D				
				E		E			I			E			I					
4 Incident Management	M		M	D						D		D					M	D		
				E		E	I		I	E		E			I		I	E		
5 IT Security Training and Awareness	M		M									D						D		
				E		E					I	E						E		
6 IT Systems Operations and Maintenance								D	M	D				D						
						E	I	E	I	E			I							
7 Network and Telecommunications Security								D	M	D				D						
						E	I		I	E			I							
8 Personnel Security	M		M									D						D		
						E						E				E	I			
9 Physical and Environmental Security	M		M									D			M	D				
				E		E						E			I	E				
10 Procurement	M	D	M	D															M	D
				E		E		E		E						E			I	E
11 Regulatory and Standards Compliance	M		M	D		D											M	D		
		E		E	I	E					I						I	E		
12 Security Risk Management	M		M	D								D					M	D		
		E		E	I	E	I		I		I	E	I		I		I	E		
13 Strategic Security Management	M	D	M	D																
		E	I	E		E														
14 System and Application Security	M		M											D						
				E		E			I				I	E						

Figure 1-3: The IT Security Role, Competency, and Functional Matrix

TISA EBK Analysis



Your Competency Scorecard

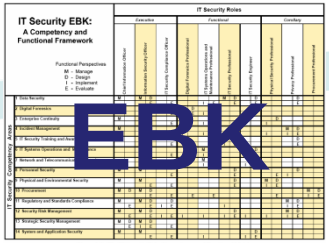
Competency Score Card

	IT Security Roles																					
	Executive						Functional										Corollary					
	Chief Information Officer		Information Security Officer		IT Security Compliance Officer		Digital Forensics Professional		IT Systems Operations and Maintenance Professional		IT Security Professional		IT Security Engineer		Physical Security Professional		Privacy Professional		Procurement Professional	
Competency matchs with job role	81%		73%		65%		42%		47%		47%		50%		20%		50%		25%	
No. of required CU		16		30		17		12		19		17		10		10		18		4
No. of possessed CU		13		22		11		5		9		8		5		2		9		1
No. of missing CU		3		8		6		7		10		9		5		8		9		3

Enterprise Infosec Competency Profile

Enterprise Capability

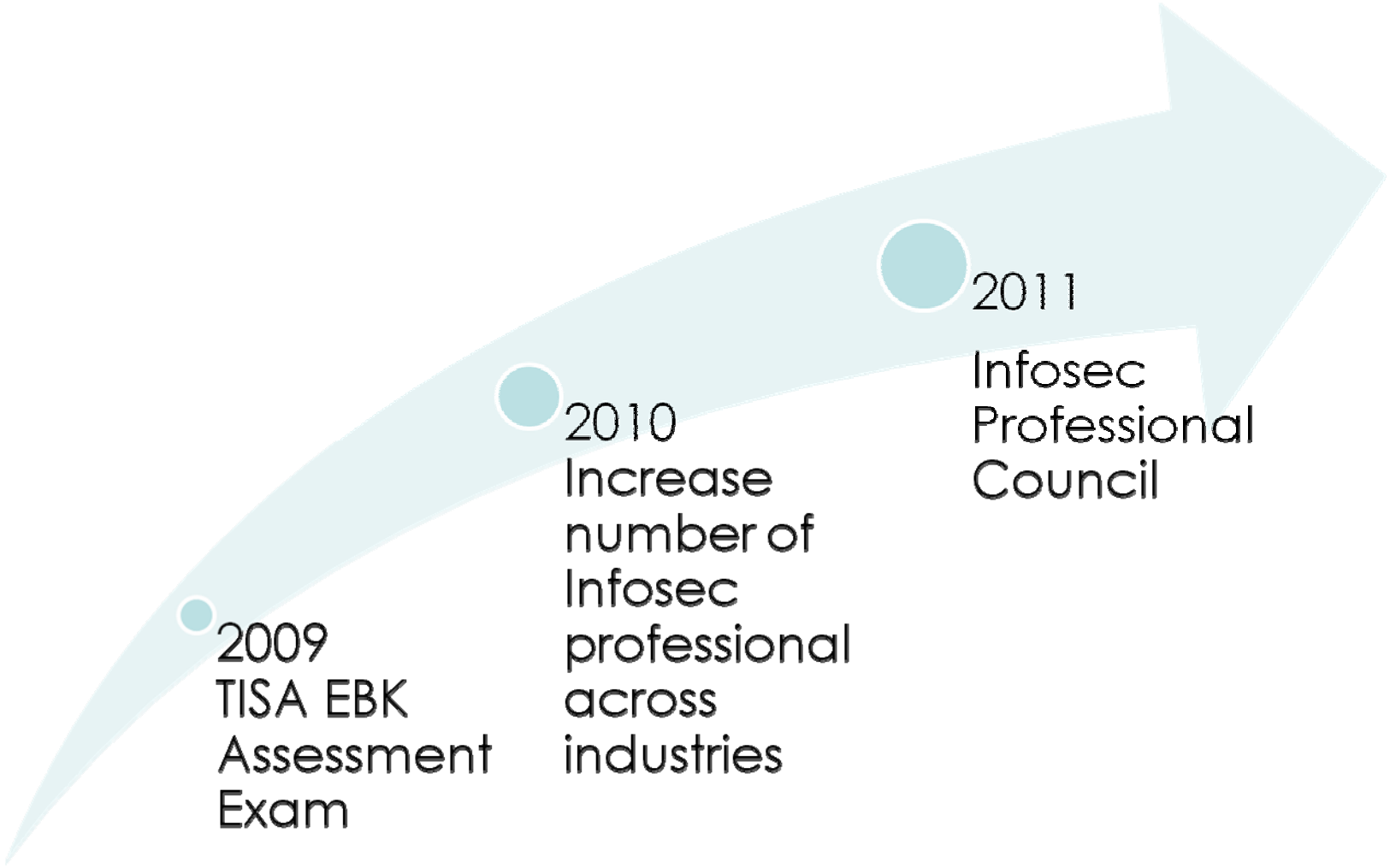
* Organization assess Infosec **competency requirement** against EBK
* **Assess current competency** within the enterprise
* Identify **competency gap** → training requirement, recruitment



Infosec training provider maps training courses to EBK

Training Provider

TISA : The Future Roadmap 2009-2011



http://www.TISA.or.th

Please contact : varapong@acisonline.net