สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ
Thailand Information Security Association (TISA)

IT & Information Security Professional Career Opportunities and Development

www.tisa.or.th

December 2009

สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ
Thailand Information Security Association (TISA)

"Career Opportunities and Development for Asia Information Security Professional with the IT Security Essential Body of Knowledge (EBK) "

Prepared by

Prinya Hom-anek,
CGEIT, CISSP, SSCP, CISA, CISM, SANS GCFW, IRCA: ISMS Lead Auditor
Thailand Information Security Association (TISA) Committee and Secretary

Chaiyakorn Apiwathanokul,
CISSP, IRCA: ISMS, SANS GCFA
Thailand Information Security Association (TISA) Committee

Nipon Nachin,
CSSLP, CISSP, SANS GCFA, CISA, CISM, SSCP
Thailand Information Security Association (TISA) Committee

Supachai Pamornchaisirikit,
CISSP, CISA, IRCA: ISMS Lead Auditor
Thailand Information Security Association (TISA) Sub-Committee

Tirayut Sripeamlap,
IRCA: ISMS, BCMS
Thailand Information Security Association (TISA) Sub-Committee

TISA: IT Security Essential Body of Knowledge Test (TISET)

Hot Topics 2010 by ACIS Professional Center

1. Virtualization and Cloud Computing Security
2. Web 2.0 and Social Networking Security
3. Mobile and Wireless Security ⇒ Mobile Forensic
4. Fraud, Internet Banking and E-Commerce Security
5. GRC (Governance, Risk Management & Compliance) Implementation
   - Enterprise Governance (Corporate Governance) ⇒ COSO
   - IT Governance (ITG) ⇒ CobiT and Val IT
   - Information Security Governance (ISG) ⇒ ISO/IEC 27001

Hot Topics 2010 by ACIS Professional Center

6. Business Process Improvement/Business Process Re-Engineering
   - IT Service Management (ITSM, ITIL & ISO/IEC 20000)
   - Information Security Management (ISO/IEC 27001)
   - Business Continuity Management (BCM)
   - Project Management using PMBOK from PMI
7. e-Discovery and Intelligence Information Gathering
8. Complex Social Engineering Techniques on Social Network (Human as a Target)
9. The Rising of Information Security Awareness Training within organization (for Everyone)
10. International Standards and Best Practices Real-World Implementation ➡ Alignment, Agility, Holistic and Risk-based Approach

Top 10 Cyber Security Threats 2010

by ACIS Professional Center

INTERNATIONAL INSTITUTES, CERTIFICATION AND CERTIFICATES

CompTIA. GIAC Global Information Assurance Certification (ISC)² International Standard for Information Security ISACA Serving IT Governance Professionals IRCA

Institutes

CompTIA
The Computing Technology Industry Association, Inc.

Global Information Assurance Certification
The SANS Institute

International Information Systems Security Certification Consortium, Inc.

Information Systems Audit and Control Association

International Register of Certificated Auditors
IRCA

ITIL Information Technology Infrastructure Library
Office Of Government Commerce (OGC)

Certificates

CompTIA Security+ Certified

- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Server+
- CompTIA Linux+
- CompTIA PDI+
- CompTIA RFID+
- CompTIA Convergence+
- CompTIA CTT+
- CompTIA CDIA+
- CEA-CompTIA DHTI+
- CompTIA Project+

GIAC Certified Firewall Analyst | GIAC Assessing Wireless Networks | GIAC Certified Forensics Analyst | GIAC Certified Intrusion Analyst

Certified Secure Software Lifecycle Professional | Certified Information Systems Security Professional | Systems Security Certified Practitioner | Certification and Accreditation Professional

CGEIT | CISM | CISA | CobiT Foundation

ISO/IEC 20000-1 (ITSMS) Lead Auditor | ISO/IEC 27001 (ISMS) Lead Auditor | BS25999 (BCMS) Lead Auditor

- Principal Auditor
- Lead Auditor
- Auditor
- Provisional Auditor

ITIL Service Manager (Master Certification) | ITIL Practitioner | ITIL Foundation

itSMF ISO/IEC 20000

itSMF International
The IT Service Management Forum

CompTIA Certifications

CompTIA Certifications

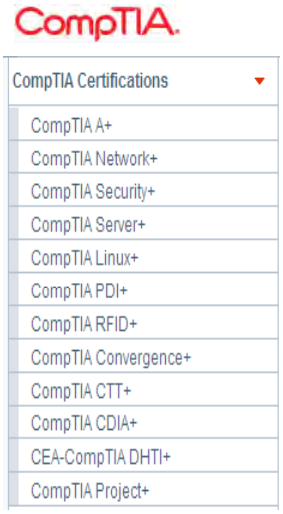
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Server+
- CompTIA Linux+
- CompTIA PDI+
- CompTIA RFID+
- CompTIA Convergence+
- CompTIA CTT+
- CompTIA CDIA+
- CEA-CompTIA DHTI+
- CompTIA Project+

CompTIA is the non-profit trade association advancing the global interests of information technology (IT) professionals and companies including manufacturers, distributors, resellers, and educational institutions

For individuals, attaining certifications means increased job security, additional career opportunities and increased credibility in the workplace. For businesses, hiring certified workers means higher customer satisfaction, increased productivity and lower employee turnover.

- **CompTIA A+**
  For entry-level IT technicians, the CompTIA A+ exam covers preventative maintenance, basic networking, installation, troubleshooting, communication and professionalism.
- **CompTIA Network+**
  For networking professionals, the CompTIA Network+ exam covers managing, maintaining, troubleshooting, operating and configuring basic network infrastructure.
- **CompTIA Security+**
  For experienced security professionals, the CompTIA Security+ exam covers system security, network infrastructure, cryptography, assessments and audits.
- **CompTIA Server+**
  For experienced IT professionals, the CompTIA Server+ exam covers areas such as RAID, SCSI, managing multiple CPUs and disaster recovery.
- **CompTIA Linux+**
  For experienced Linux professionals, the CompTIA Linux+ exam covers user administration, file permissions, software configurations and the fundamental management of Linux systems.
- **CompTIA PDI+**
  For entry-level printer and document-imaging technicians, the CompTIA PDI+ exam covers basic electromechanical components and tools, print engine and scan processes, color theory and networking.

CompTIA Certifications



CompTIA is the non-profit trade association advancing the global interests of information technology (IT) professionals and companies including manufacturers, distributors, resellers, and educational institutions

(cont.)

- **CompTIA RFID+**
  For RFID professionals, the CompTIA RFID+ exam covers installation, maintenance, repair and troubleshooting of RFID products.
- **CompTIA Convergence+**
  For experienced convergence professionals, the CompTIA Convergence+ exam covers designing, implementing and managing voice and data networks.
- **CompTIA CTT+**
  For technical instructors, the CompTIA CTT+ exam covers classroom preparation, presentation, communication, facilitation and evaluation in both traditional classroom and virtual classroom environments.
- **CompTIA CDIA+**
  For document imaging solutions sellers, the CompTIA CDIA+ exam covers planning, designing and specifying a document imaging management system.
- **CEA-CompTIA DHTI+**
  For experienced home technology professionals, the CEA-CompTIA DHTI+ certification covers configuring, integrating, maintaining and troubleshooting electronic and digital home systems.
- **CompTIA Project+**
  For project managers, the CompTIA Project+ certification covers the entire process of project management, including initiation, planning, execution, acceptance, support and closure.

Global Information Assurance Certification

Certifications

- GIAC Certified ISO-17799 Specialist (G7799)
- GIAC Assessing Wireless Networks (GAWN)
- GIAC Certified Enterprise Defender (GCED)
- GIAC Certified Forensics Analyst (GCFA)
- GIAC Certified Firewall Analyst (GCFW)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Incident Manager (GCIM)
- GIAC Certified Project Manager Certification (GCPM)
- GIAC Certified Security Consultant (GCSC)
- GIAC Certified UNIX Security Administrator (GCUX)
- GIAC Certified Windows Security Administrator (GCWN)
- GIAC Information Security Fundamentals (GISF)
- GIAC Information Security Officer (GISO)
- GIAC Information Security Professional (GISP)
- GIAC Legal Issues (GLEG)
- GIAC .Net (GNET)
- GIAC Operations Essentials Certification (GOEC)
- GIAC Certified Penetration Tester (GPEN)
- GIAC Reverse Engineering Malware (GREM)
- GIAC Security Audit Essentials (GSAE)
- GIAC Security Essentials Certification (GSEC)
- GIAC Secure Internet Presence (GSIP)
- GIAC Security Leadership Certification (GSLC)
- GIAC Systems and Network Auditor (GSNA)
- GIAC Securing Oracle Certification (GSOC)
- GIAC Secure Software Programmer - C (GSSP-C)
- GIAC Secure Software Programmer - Java (GSSP-JAVA)
- GIAC Secure Software Programmer - .NET (GSSP-NET)
- GIAC Web Application Penetration Tester (GWAPT)

Global Information Assurance Certification

Gold Certifications

- GIAC Certified ISO-17799 Specialist (G7799) - GOLD
- GIAC Assessing Wireless Networks (GAWN) - GOLD
- GIAC Certified Forensics Analyst (GCFA) - GOLD
- GIAC Certified Firewall Analyst (GCFW) - GOLD
- GIAC Certified Intrusion Analyst (GCIA) - GOLD
- GIAC Certified Incident Handler (GCIH) - GOLD
- GIAC Certified UNIX Security Administrator (GCUX) - GOLD
- GIAC Certified Windows Security Administrator (GCWN) - GOLD
- GIAC Information Security Fundamentals (GISF) - GOLD
- GIAC .Net (GNET) - GOLD
- GIAC Certified Penetration Tester (GPEN) - GOLD
- GIAC Reverse Engineering Malware (GREM) - GOLD
- GIAC Security Essentials Certification (GSEC) - GOLD
- GIAC Secure Internet Presence (GSIP) - GOLD
- GIAC Systems and Network Auditor (GSNA) - GOLD

Certificates:

- GIAC Auditing Wireless Networks - Certificate (GAWN-C)
- GIAC Business Law and Computer Security (GBLC)
- GIAC Contracting for Data Security (GCDS)
- GIAC Critical Infrastructure Protection (GCIP)
- GIAC E-warfare (GEWF)
- GIAC Fundamentals of Information Security Policy (GFSP)
- Securing Windows 2000 - The Gold Standard (GGSC-0100)
- Securing Solaris - The Gold Standard (GGSC-0200)
- Auditing Cisco Routers - The Gold Standard (GGSC-0400)
- GIAC HIPAA Security Implementation (GHSC)
- GIAC Cutting Edge Hacking Techniques (GHTQ)
- GIAC Intrusion Prevention (GIPS)
- GIAC Law of Fraud (GLFR)
- GIAC Legal Issues in Information Technologies (GLIT)

International Information Systems Security Certification Consortium, Inc.

Systems Security Certified Practitioner (SSCP®)

Certification and Accreditation Professional (CAP®)

Certified Secure Software Lifecycle Professional (CSSLP[CM])

Certified Information Systems Security Professional (CISSP®) and related concentrations

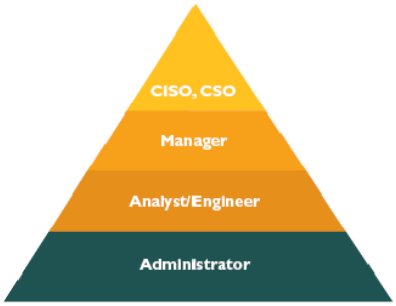
Information Systems Security Architecture Professional (CISSP-ISSAP®)

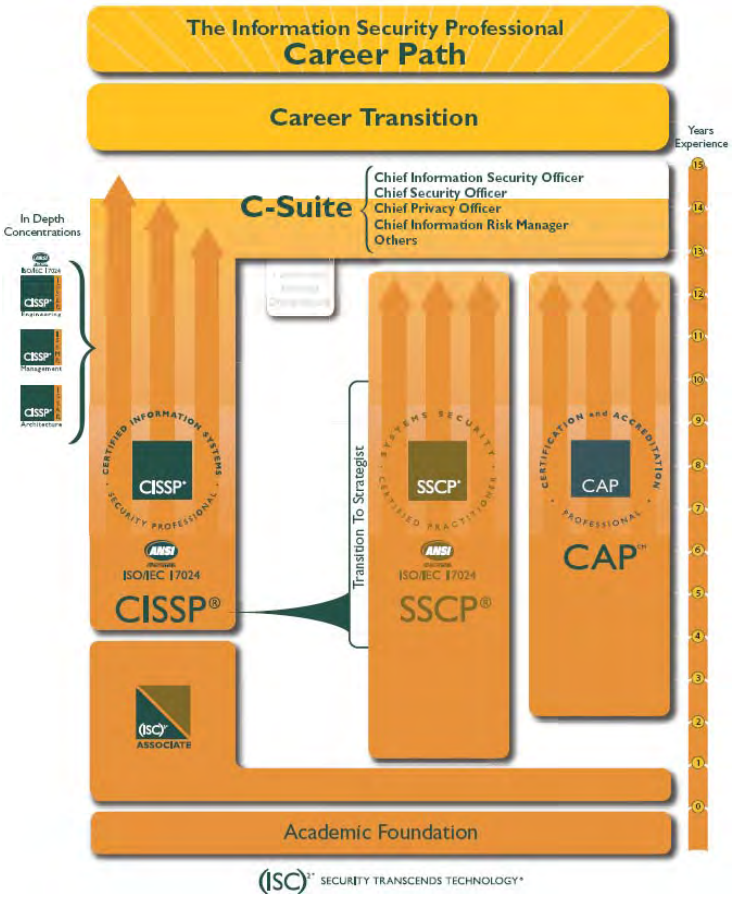
Information Systems Security Engineering Professional (CISSP-ISSEP®)

Information Systems Security Management Professional (CISSP-ISSMP®)

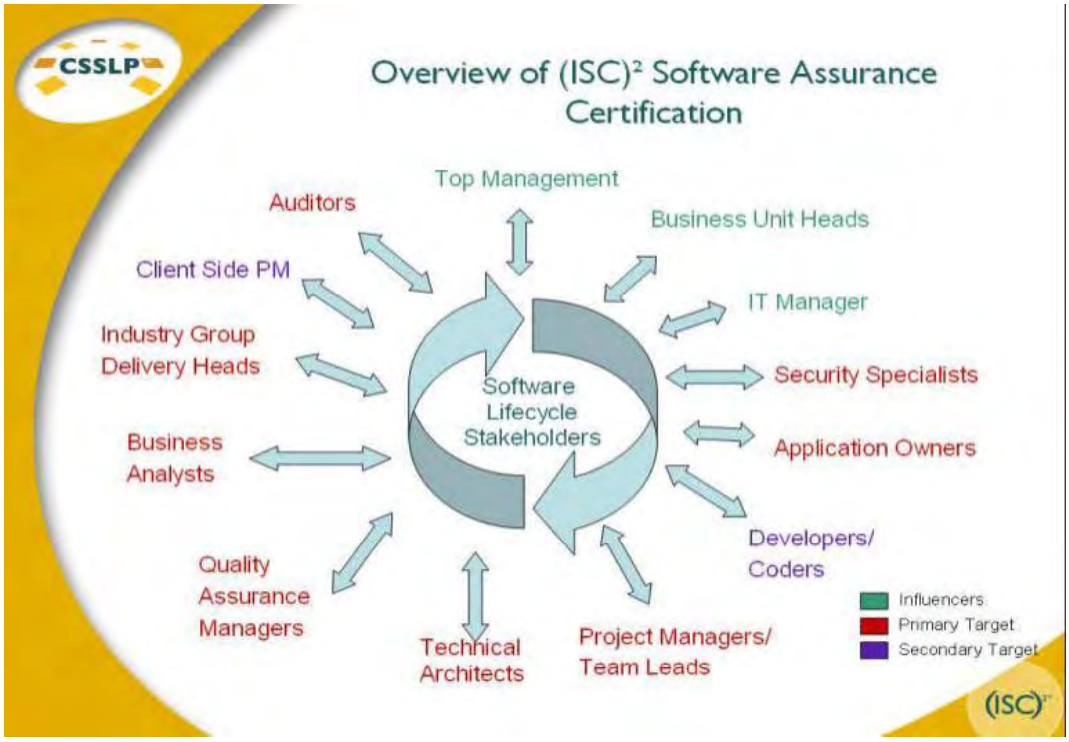
Typical Job Path:

- University graduate - Information security administrator, eligible for Associate of (ISC)2 program
- 1+ years work experience – Information security administrator, eligible for SSCP® certification
- 4+ years work experience – Information security analyst/engineer, eligible for CISSP® certification
- 7+ years work experience – Information security manager
- 9+ years work experience – Director of IT or information security, chief security officer (CSO) or chief information security officer (CISO)

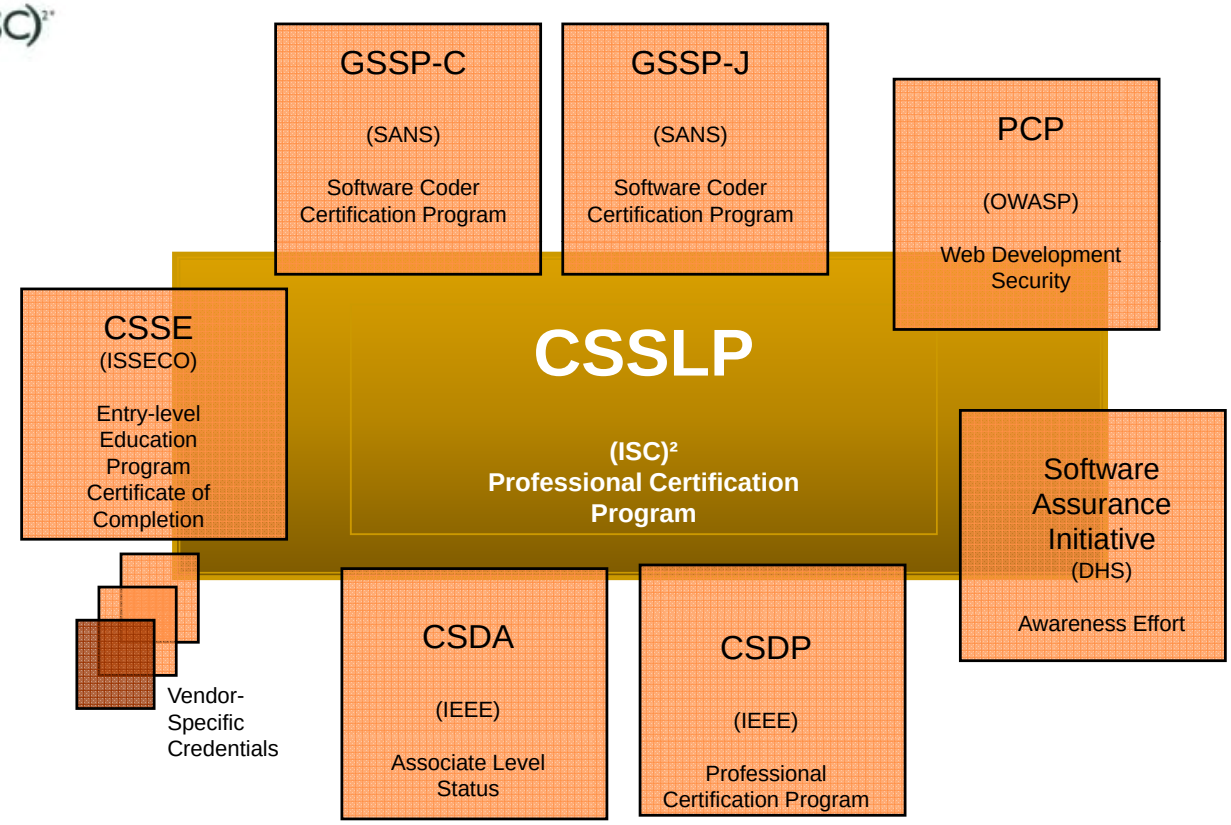




Certified Secure Software Lifecycle Professional (CSSLP®)



Key Players – Knowledge Area Overlap



Information Systems Audit and Control Association

The Certified in the Governance of Enterprise IT® (*CGEIT®*)

The Certified Information Security Manager® (*CISM®)*

The Certified Information Systems Auditor® *(CISA®)*

The Control Objectives for Information and related Technology *(COBIT)*

Well-known Certifications in Thailand

* Only those available in Thailand

- The Institute of Internal Auditors (IIA)
  - **CIA** - The Certified Internal Auditor
  - **CCSA** - Certification in Control Self-Assessment
  - **CFSA** - Certified Financial Service Auditor
- Association of Certified Fraud Examiners (ACFE)
  - **CFE** - Certified Fraud Examiners
- The Bank Administration Institute (BAI)
  - **CBA** - Certified Bank Auditor
- Information Systems Audit and Control Assoc. (ISACA)
  - **CISA** - Certified Information Systems Auditor
  - **CISM** - Certified Information Security Manager
- Intl Information Systems Security Certification Consortium (ISC)2
  - **CISSP** - The Certified Information Systems Security Professional

ABOUT THAILAND INFORMATION SECURITY ASSOCIATION (TISA)

Thailand Information Security Association (TISA)

- **Vision**
  - Thailand and Asia community have been recognized that we are safe and secure in information security from global point of view.
- **Mission**
  - To develop internationally accepted process and information security practitioners

TISA Committees

Thailand Information Security Association

http://www.tisa.or.th

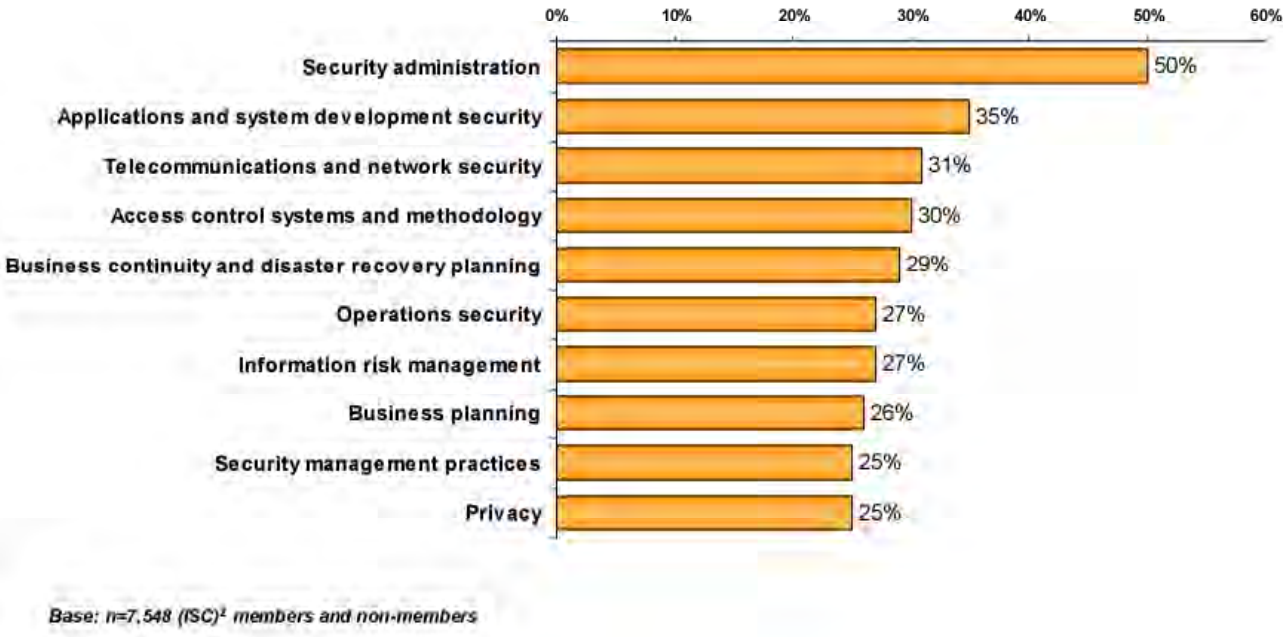
TISA Activities 2008-2009

- 1st TISA Seminar : Information Security Seminar on topic : "How The New Thailand ICT Law effect IT industry" over 400 Attendees attended at Sasin, Chulalongkorn Univeristy.
- In-Depth Study on "Information Security Rating for IT/Infosec Professional in Thailand"
  - NIST SP800-16, DHS - EBK 2008 (September, 2008)
  - DoD Directive 8570.01-M (May 15, 2008)
- In-Depth Study on Thailand Information Security Testing Programme for IT/Information Security Professional
- Develop Local Information Security Professional Certification (to be first step to get International Professional Certification)
  - TISA Management Level I
  - TISA Management Level II
  - TISA Management Level III
  - TISA Technical Level I
  - TISA Technical Level II
  - TISA Technical Level III

Current Challenges in Thailand

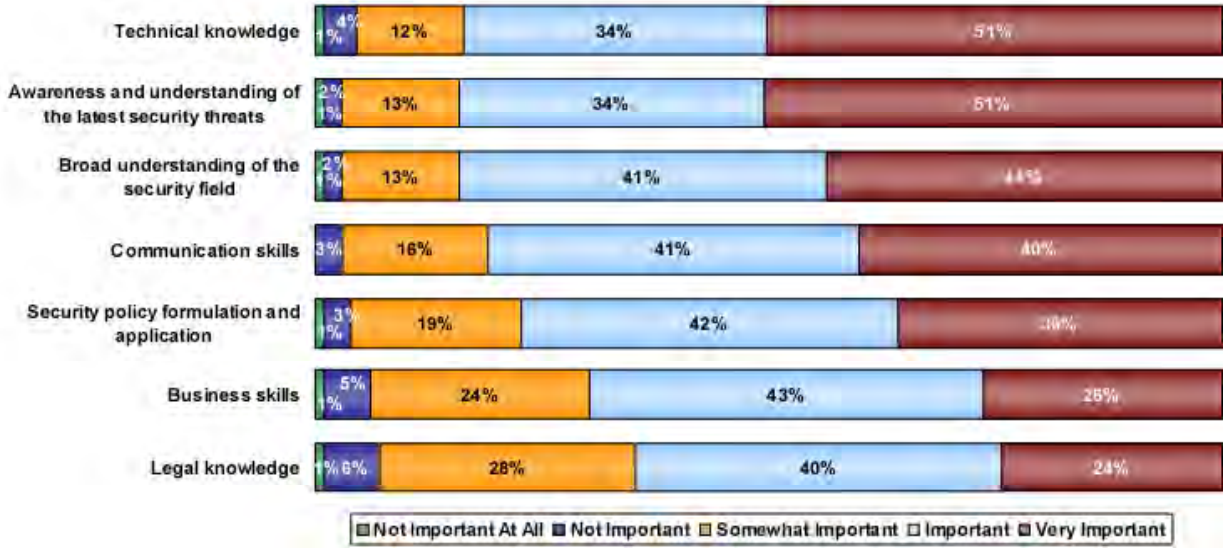
- Value recognition of Information Security practitioner
  HR thinks it's just another IT position, what make it so important???
- Unclear career path
  Only few organizations has CSO, CISO or dedicate division/department to handle Infosec in the organization
- Under pay
  Asia-pacific got about 10-20 times less than in US.
- Incentive is not yet attractive to motivate people to jump into this field
  why do they have to work harder with the same pay or only small raise?

Growing Need for Information Security Training

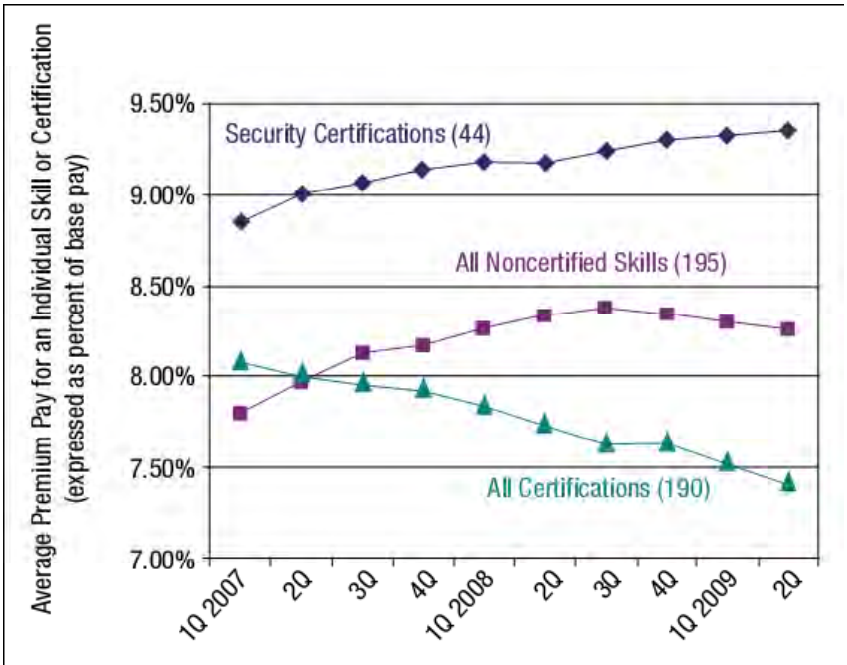


Base: n=7,548 (ISC)² members and non-members

Importance of Information Security Skills



2007-2009 IT Skills and Certifications Pay Performance



Source: Foote Partners, IT Skills and Certifications Pay Index™ (88,200 IT professionals), *www.footepartners.com*

BASELINE CERTIFICATIONS AND WORKFORCE DEVELOPMENT (DOD DIRECTIVE 8570.01-M)

DoD Directive

Information Assurance Workforce Improvement Program

As of December 2005

IAT Level I	IAT Level II	**IAT Level III**
A+ Network+ SSCP	**GSEC** **Security+** **SCNP** **SSCP**	CISA CISSP GSE SCNA
IAM Level I	**IAM Level II**	**IAM Level III**
GISF GSLC Security+	**GSLC** CISM CISSP	**GLSC** CISM CISSP

DoD 8570.01-M, Table AP3.T2. *DoD Approved Baseline Certifications*

DoD 8570.01-M

Information Assurance Workforce Improvement Program

As of May 2008

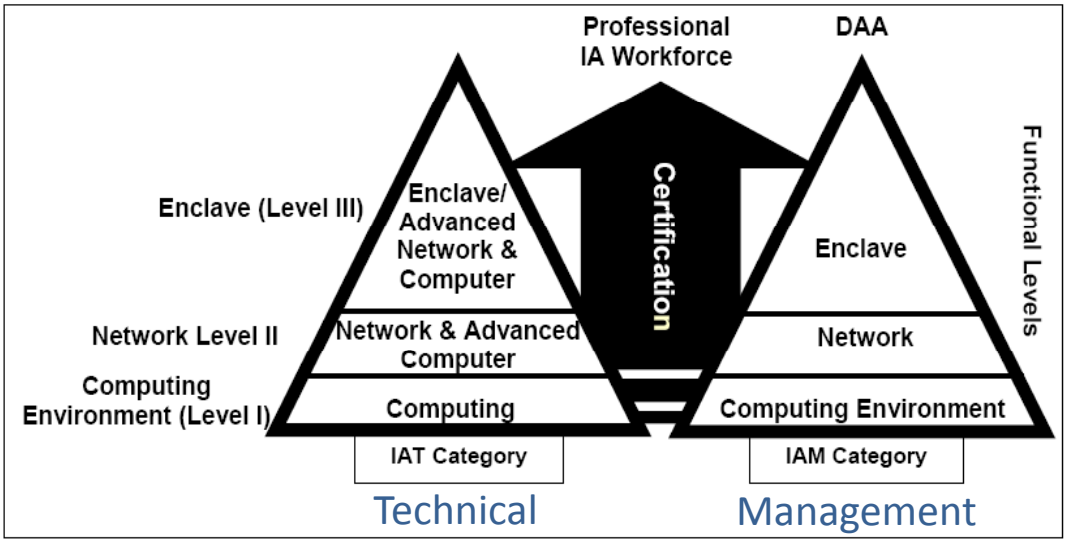
IAT Level I	IAT Level II	IAT Level III
A+ Network+ SSCP	GSEC Security+ SCNP SSCP	CISA CISSP *(or Associate)* GSE SCNA

IAM Level I	IAM Level II	IAM Level III
GISF GSLC Security+	GSLC CISM CISSP *(or Associate)*	GSLC CISM CISSP *(or Associate)*

CND Analyst	*CND Infrastructure Support*	*CND Incident Responder*	*CND Auditor*	*CND-SP Manager*
GCIA	*SSCP*	*GCIH* *CSIH*	*CISA* *GSNA*	*CISSP-ISSMP* *CISM*

IASAE I	*IASAE II*	*IASAE III*
CISSP (or Associate)	*CISSP (or Associate)*	*ISSEP* *ISSAP*

IA Workforce structure



INFORMATION TECHNOLOGY (IT) SECURITY

ESSENTIAL BODY OF KNOWLEDGE (EBK)

A Competency and Functional Framework for IT Security Workforce Development

United States Department of Homeland Security

Published: September 2008

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

Purpose of EBK (cont.)

- 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.

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

EBK Development Process

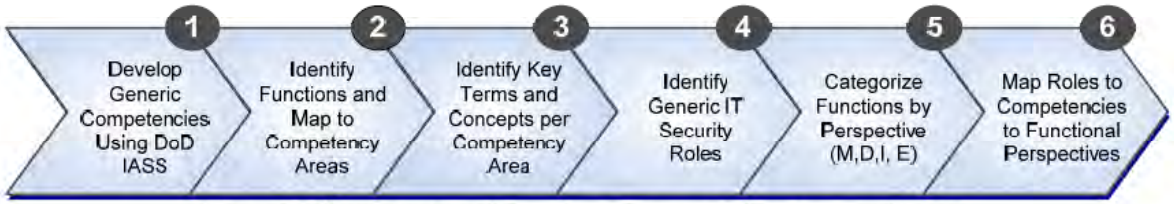


Figure 1-1: Competency and Functional Framework Development Process


Homeland Security

Information Technology (IT) Security Essential Body of Knowledge (EBK):

A Competency and Functional Framework for IT Security Workforce Development

Office of Cybersecurity and Communications
National Cyber Security Division

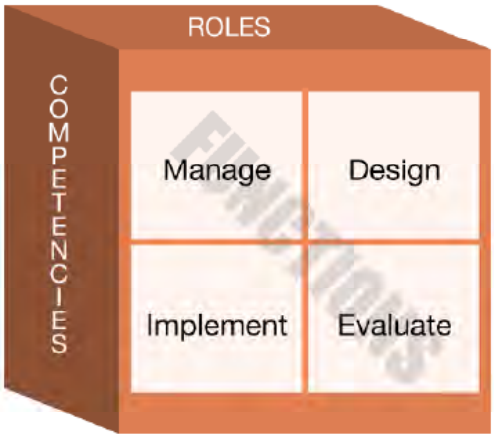
September 2008

United States Department of Homeland Security
Washington, D.C. 20528

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

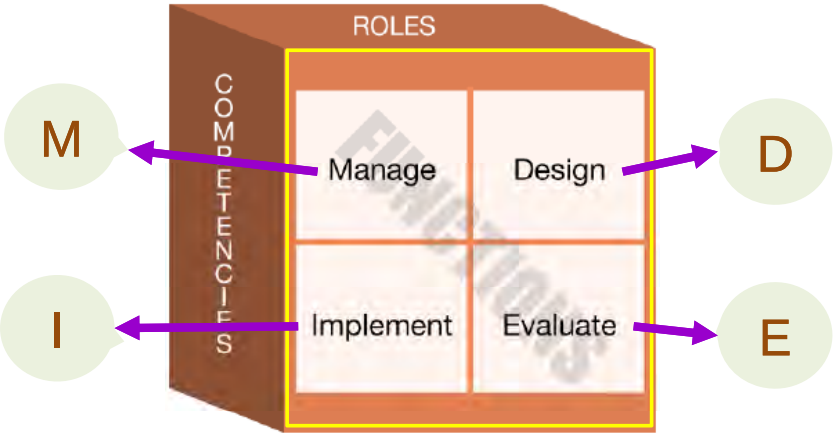
Key Dimensions

- 4 functional perspectives
- 14 competency areas
- 10 roles

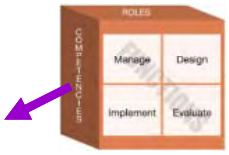


Functional Perspectives (MDIE)

- Manage
- Design
- Implement
- Evaluate



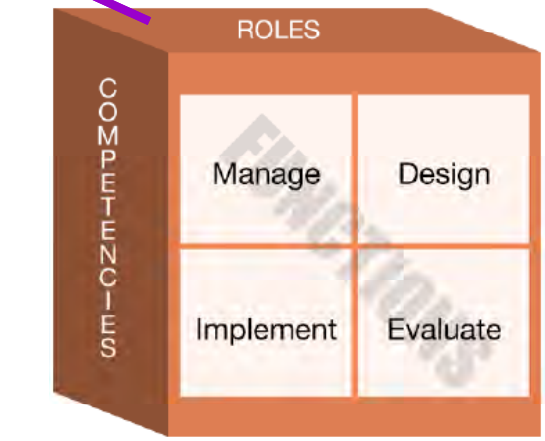
Competency Areas *(MDIE in each)*



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

Roles of Information Security

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



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

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

EBK Analysis

IT Security EBK:
A Competency and Functional Framework

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

	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
M	11	12	0	1	2	1	0	1	3	1
D	2	7	1	3	4	6	4	2	6	1
I	0	1	2	5	8	3	4	4	4	1
E	3	10	14	3	5	7	2	3	5	1
Total Competency Units	16	30	17	12	19	17	10	10	18	4

Managerial Level | Professional Level | Entry Level

สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ
Thailand Information Security Association (TISA)

TISA TISET Examination

TISET = TISA IT Security EBK Test

The First Local Information Security Knowledge Testing in Thailand

The Example of TISA TISET Exam

Information Security Competency Score Card

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

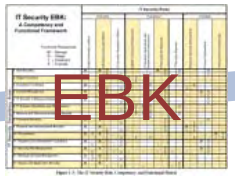
Enterprise Infosec Competency Profile

Enterprise/ Personnel 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

TISET Development

- Study and develop test item according to DHS-IT Security EBK 2008
- Matching test items with corresponding competency and functional perspective (MDIE).
- Refer to CISSP, SSCP, CISA, CISM, CIA and PMP knowledge

Initial Plan	Arp-09	May-09	Jun-09	Jul-09	Aug-09
Current Plan			Oct-09	Dec-09	Feb-10
1 Lot items (8/CU)	X				
Peer review		X			
rescrubbing		X			
Committee review			X		
1st pilot exam			X		
Finalize				x	
1st launch					x

TISA TISET Exam Item Development Restriction

1. **None of the item development committee has access to all developed items**
2. **Item development committee shall only see the item they developed and those when peer-reviewed.**
3. **TISA reserved the right not to disclose any or all of the developed items to those who does not involve with the item development process.**
4. **Item development committee must abide to the signed Non-disclosure Agreement (NDA).**
   - **Storage encryption technique was used (AES 128 bits)**
   - **2-Man dual control mechanism was practiced (one hold the key file and one hold the pass-phrase)**
   - **Secure Erase, ANTI-Forensic (US DoD 5220.22-M 3 Pass) was practiced**

Thailand Information Security Association

TISA ITS-EBK Test Model
TISET Pilot Exam Summary
17-Oct-2009

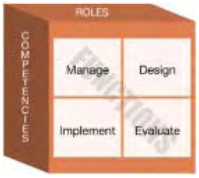
http://www.tisa.or.th

TISA TISET Pilot Exam Methodology

- All 500 items in databank were tested
- There were 4 sets of question papers (A-B-C-D)
- Each question set contains 125 questions
- Each question set contains all 14 competencies with 4 detail functional perspectives (14x4=56 CU's)
- 2.5 hours to finish
- 2B Carbon pencil answer sheet (like CISSP,CISA Exam)

TISET Pilot Exam Summary

- **Pilot Test Date:** 17 Oct. 2009
- **Pilot Test Group:** 4 Groups (125 Questions each group (set), 2:30 hrs.)
- **Knowledge-base:** IT Security Essential Body of Knowledge (EBK)



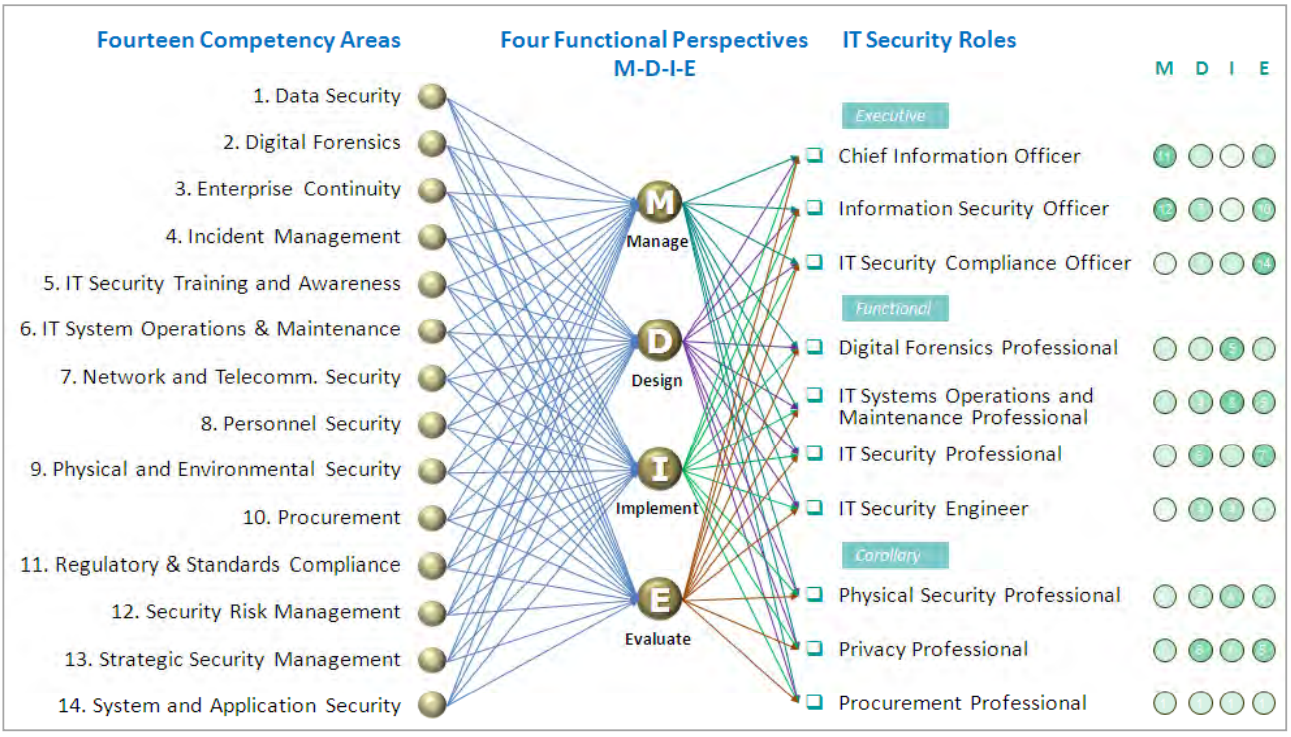
IT Security EBK: A Competency and Functional Framework

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

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

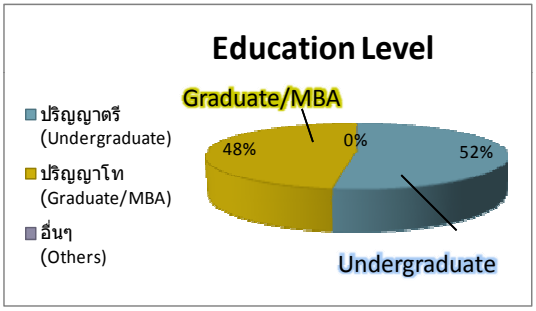
Figure 1-3: The IT Security Role, Competency, and Functional Matrix

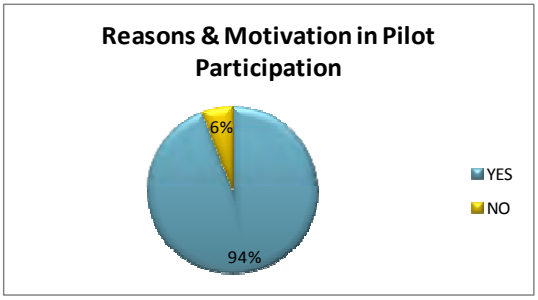
TISET Pilot Exam Summary



TISET Pilot Exam Summary

Total Candidates: 90 persons





Pre-test & Post-test Questionnaires

Any Experiences related to information security:

- **Yes = 77%**
- **No = 23%**

The NO Answers are those haven't experiences related to information security in their jobs. They are:

- **R&D/QA Engineer,**
- **Programmer, SA,**
- **IT Staff/Operations, IT Support,**
- **Researcher, IT instructors / students,**
- **and those hadn't specified.**

TISET Pilot Exam Summary

Total Candidates: 90 persons

IT Association Membership:

- Yes = 20 persons
- No = 70 persons

Those 20 of 90 persons are IT association members of:

- TISA = 3 persons
- $(ISC)^2$ = 2 persons
- ISACA = 5 persons
- IIA = 3 persons
- ITSMF = 5 persons
- Others = 2 persons

Pre-test & Post-test Questionnaires

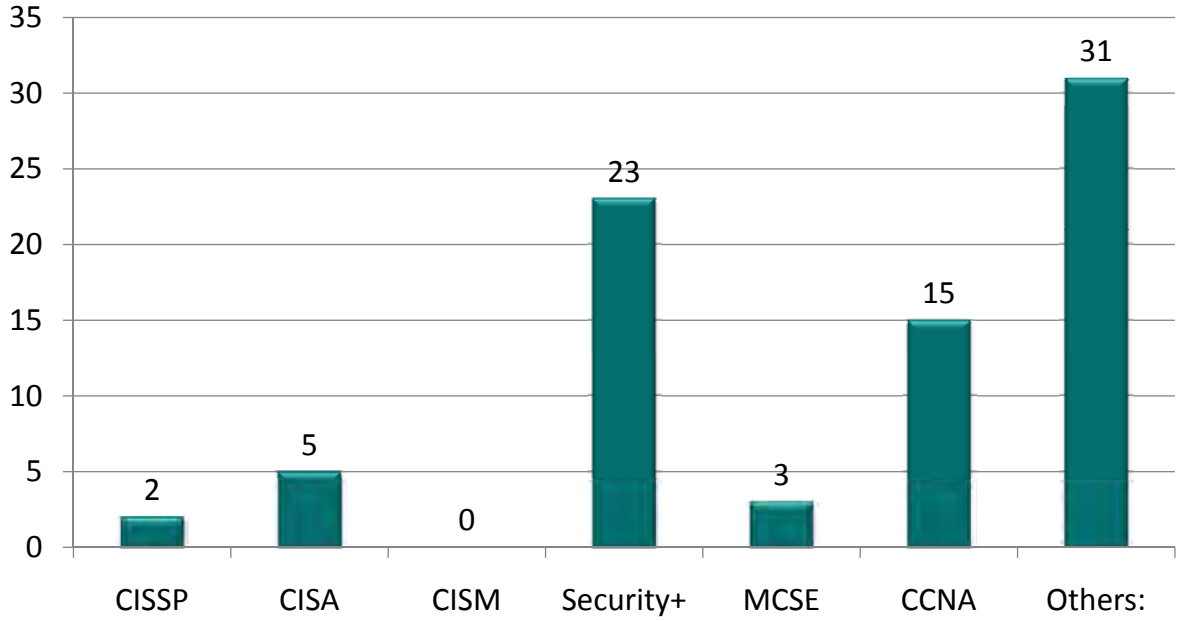
IT Professional Certificates:

- Yes 40% = 36 persons
- No 60% = 54 persons

Those 36 persons have hold 78 professional certificates:

- CISSP = 2 persons
- CISA = 5 persons
- CISM = 0 persons
- Security+ = 23 persons
- MCSE = 5 persons
- CCNA = 2 persons
- CEH = 4 persons
- ITIL = 4 persons
- PMP = 1 persons
- Others = 26 persons

Candidate Profile : IT and Information Security Professional Certificates



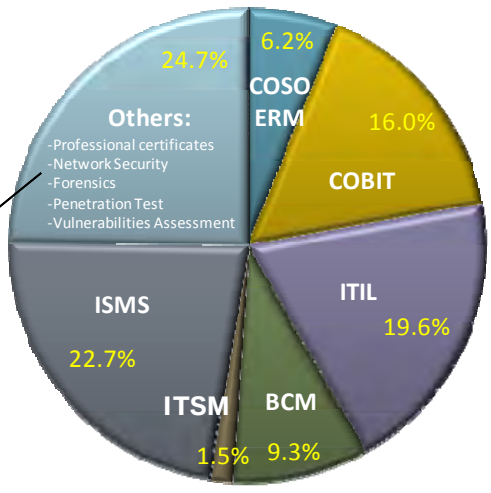
TISET Pilot Exam Summary

The Standards, Best Practices and IT Topics that the candidates currently are interested to the most:

- ISMS = 22.7%
- ITIL = 19.6%
- COBIT = 16.0%
- COSO ERM = 6.2%
- BCM = 9.3%
- ITSM = 1.5%
- Others = 24.7%

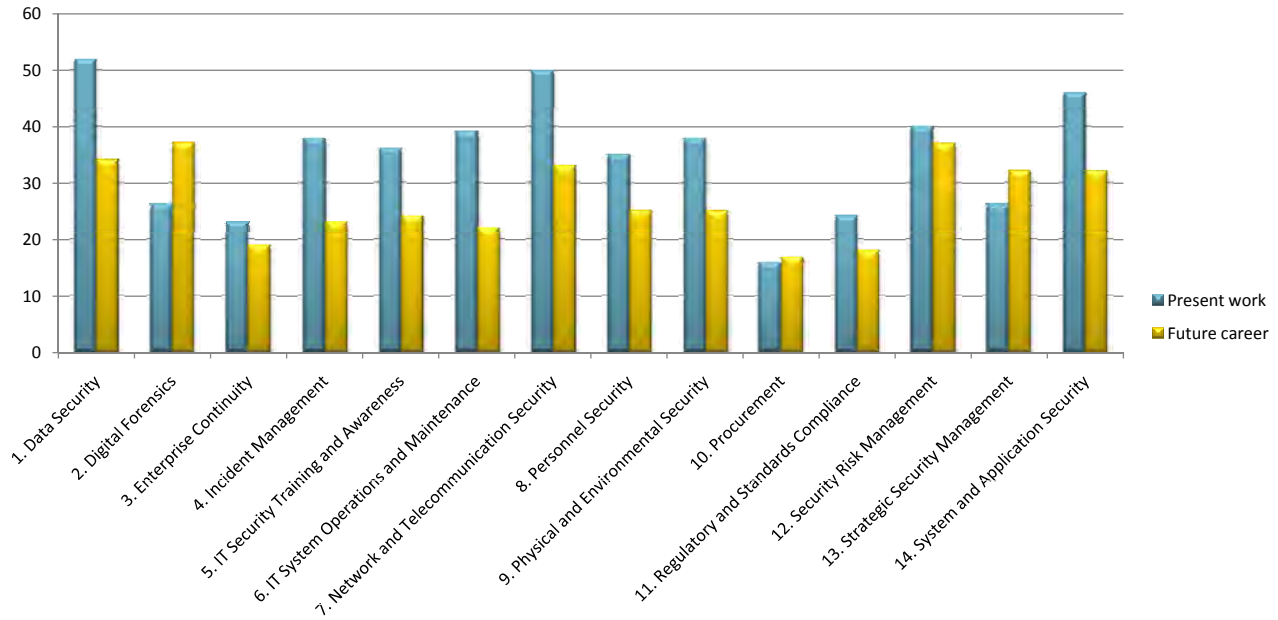
Others topics include:

- *CISSP = 6.2%*
- *CEH = 2.1%*
- *CISA = 2.1%*
- *Network security = 2.0%*
- *VA, Penetration Test = 2.0%*
- *Forensics = 1.5%*
- *Others (each < 1%) = 8.8%*



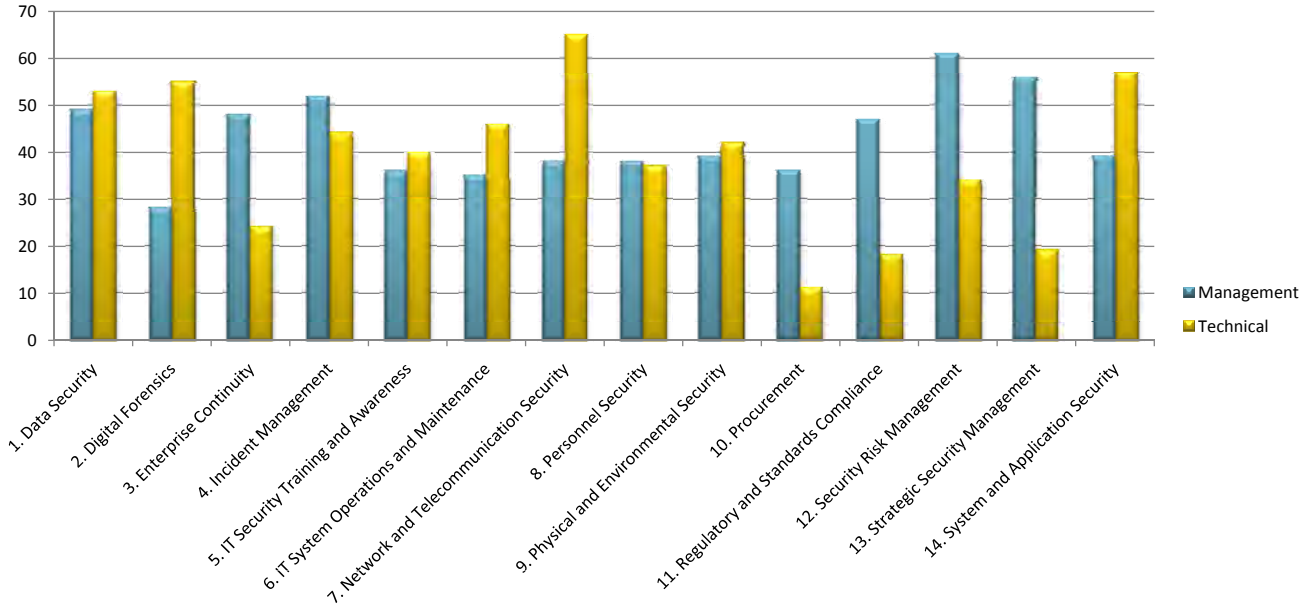
TISET Pilot Exam Summary

Involvement in Present Work & Future Career



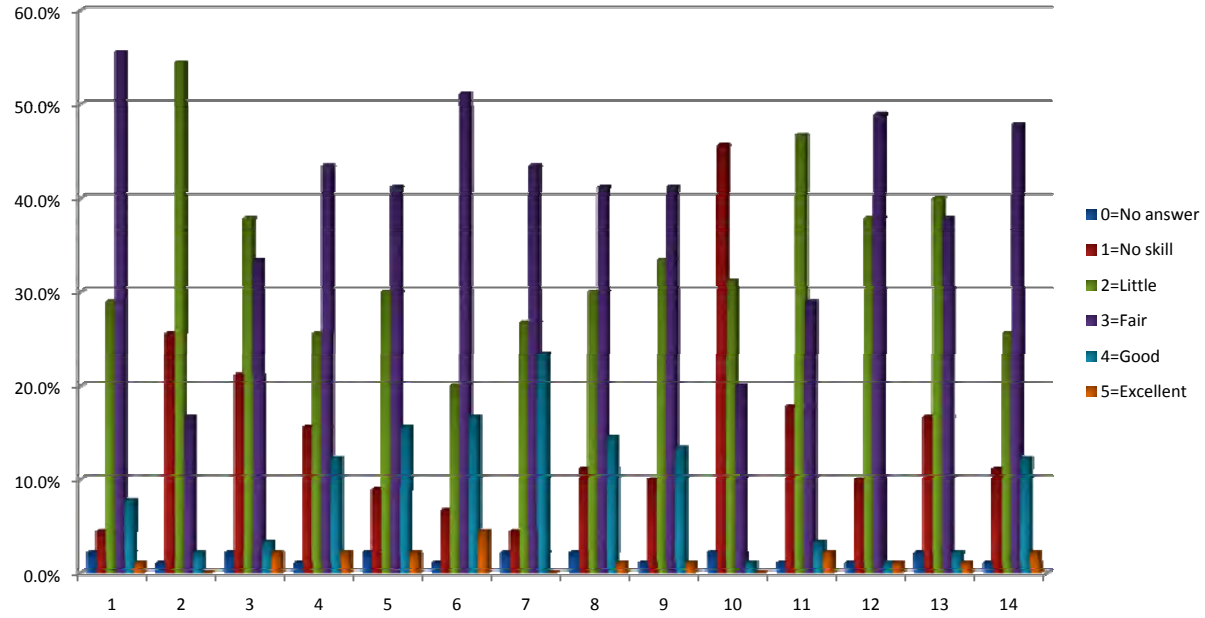
TISET Pilot Exam Summary

Interesting Topics (EBK Domains) by Management vs. Technical Perspectives



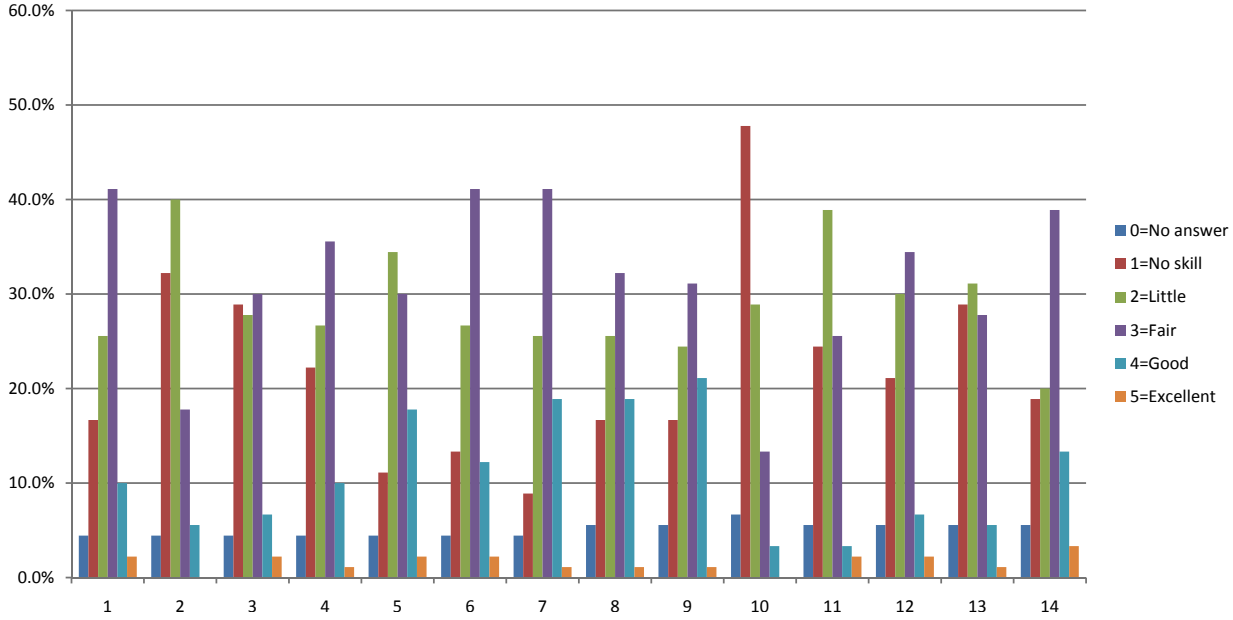
TISET Pilot Exam Summary

Pre-test Skill Assessment by EBK



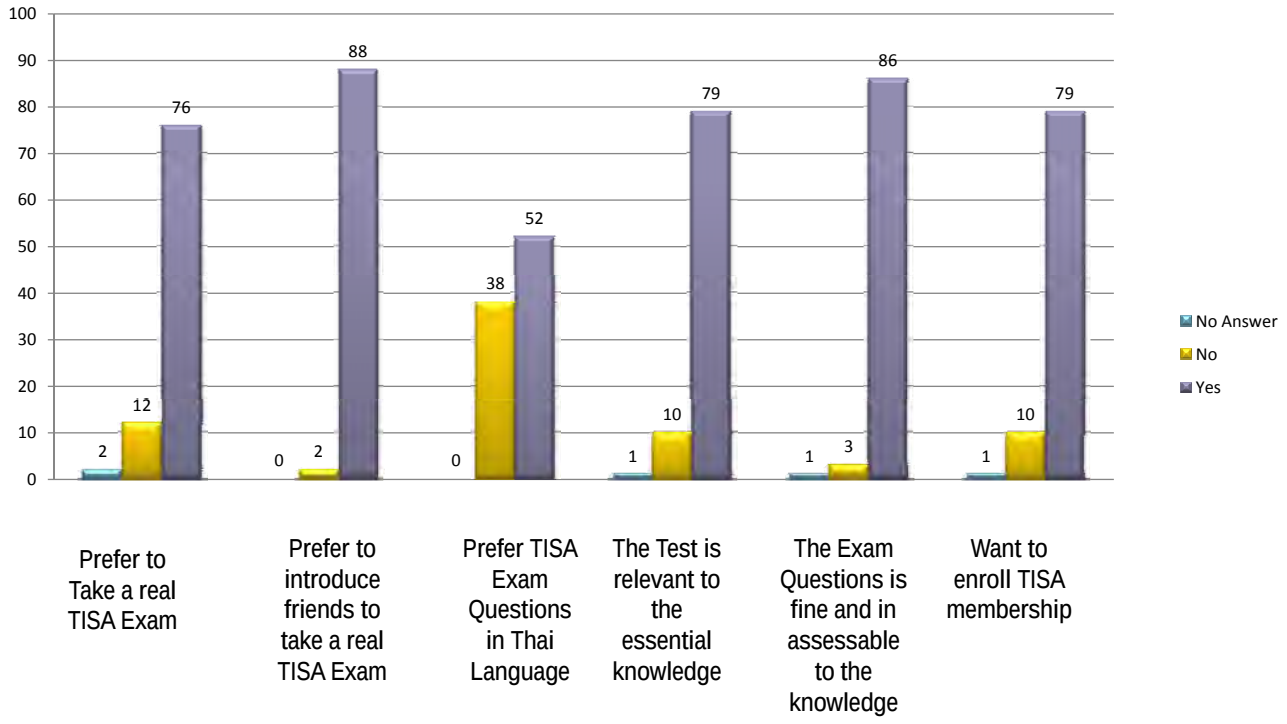
TISET Pilot Exam Summary

Post-test Skill Assessment by EBK



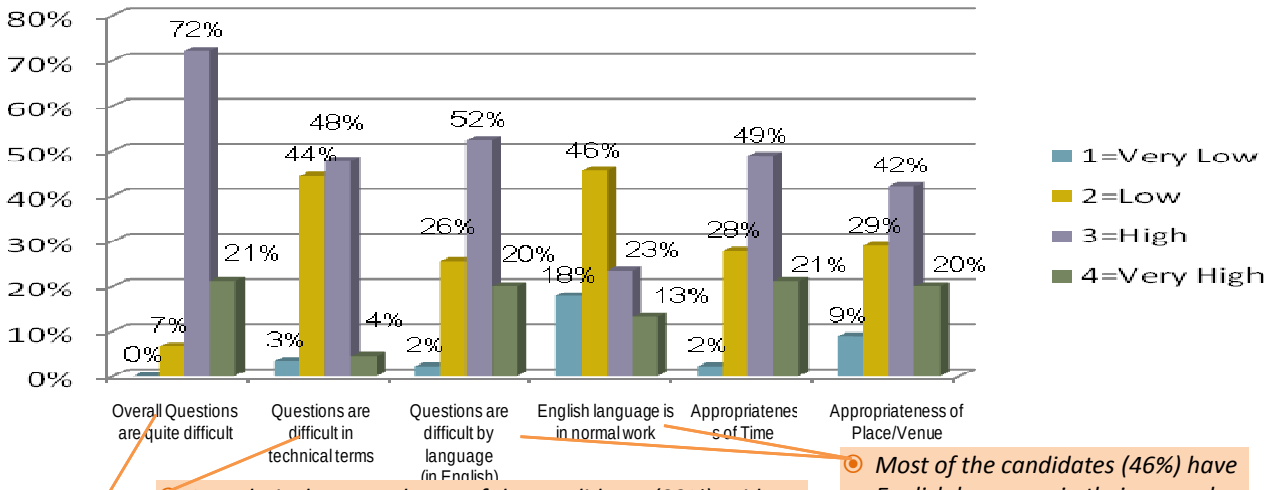
TISET Pilot Exam Summary

Candidates' Comments



TISET Pilot Exam Summary

Comments on Level of Difficulties/Hard of Questions and Appropriateness of Time & Venue



- *In technical terms, almost of the candidates (92%) said questions are hard (44%) and very hard (48%) respectively.*
- *By overall, about three-fourth of the candidates (72%) said the questions are hard, and almost one-fifth (21%) said the questions are very hard/difficult.*
- *Most of the candidates (46%) have English language in their normal work, but they (52%) still said the questions in English are quite hard / difficult.*

TISET Pilot Exam Summary

- ***The barrier of LANGUAGE is significant.***

  Since all of questions are in English, 72% of candidates pointed that the exam questions were quite hard although 69% admitted that English language is in their normal work. (By Language, 52% said it's hard, and 20% said it's very hard respectively)

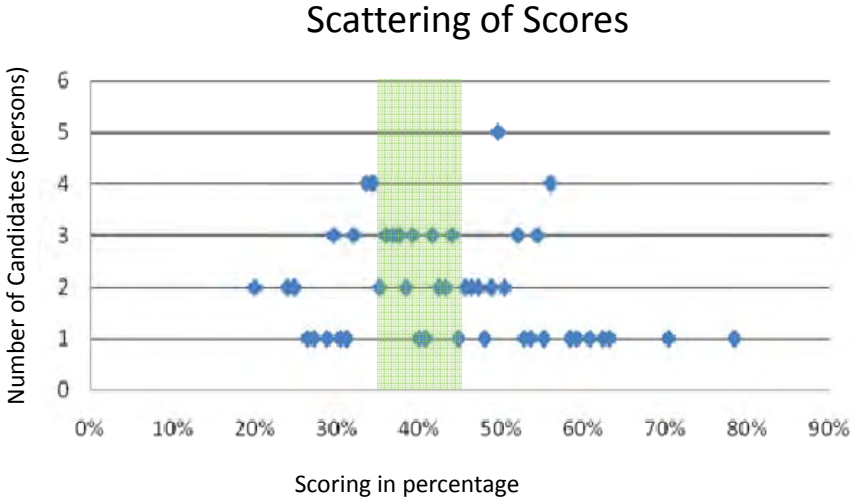
- ***The exam questions in OVERALL seemed quite hard/difficult***

  Most candidates (93%) said the questions were quite hard;
  - Three-fourth (72%) said it's hard; One-fifth (21%) said it's very hard

- ***In TECHNICAL terms, the exam questions are rated hard/difficult***

  Most candidates (92%) said questions appeared quite hard;
  - About 44% said it's hard, and about 48% said it's very hard

TISET Pilot Exam Summary
Result Report



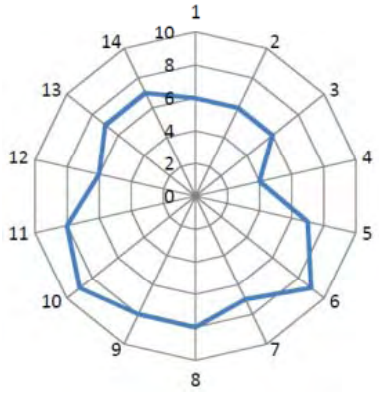
Scoring Profile

	Score	Percentage
Full Score	125	100%
Max	98	78%
Min	25	20%
Avg	53	42%

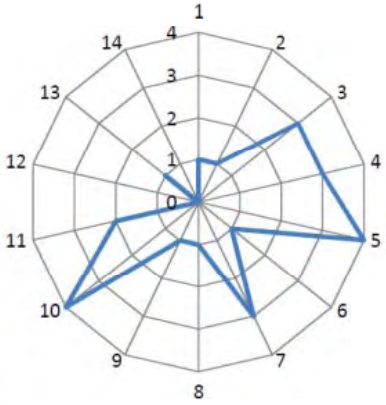
Score	# of candidate	% of candidate
>20%	12	13%
>30%	30	33%
>40%	26	29%
>50%	17	19%
>60%	3	3%
>70%	2	2%
>80%	0	0%
Total	90	100%

TISET Report: Competency Profile

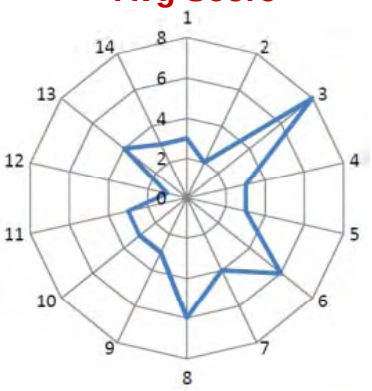
Max Score



Min Score



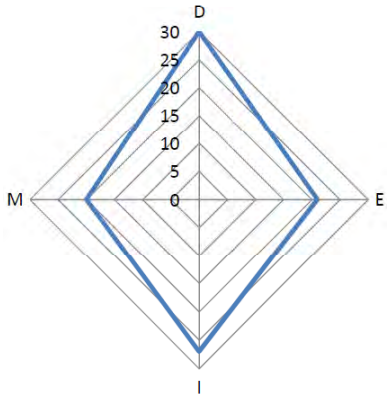
Avg Score



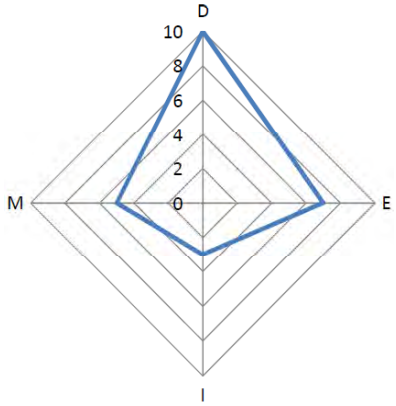
1. Data Security
2. Digital Forensics
3. Enterprise Continuity
4. Incident Management
5. IT Security Training and Awareness
6. IT System Operations and Maintenance
7. Network and Telecommunication Security
8. Personnel Security
9. Physical and Environmental Security
10. Procurement
11. Regulatory and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

TISET Report: IT Security Role Match

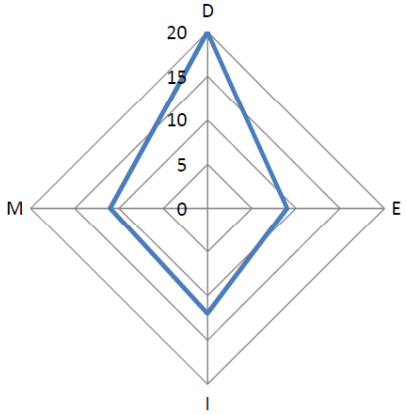
Max Score



Min Score



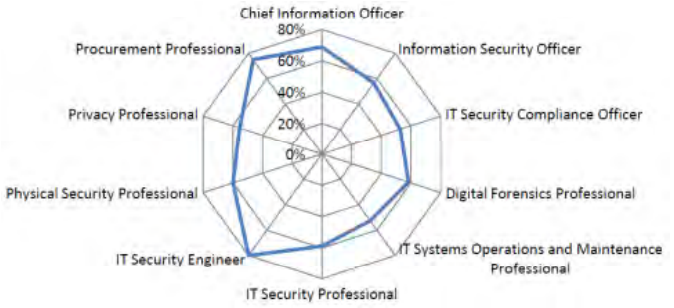
Avg Score



M – Manage
D – Design
I – Implement
E - Evaluate

TISET Report: IT Security Role Match

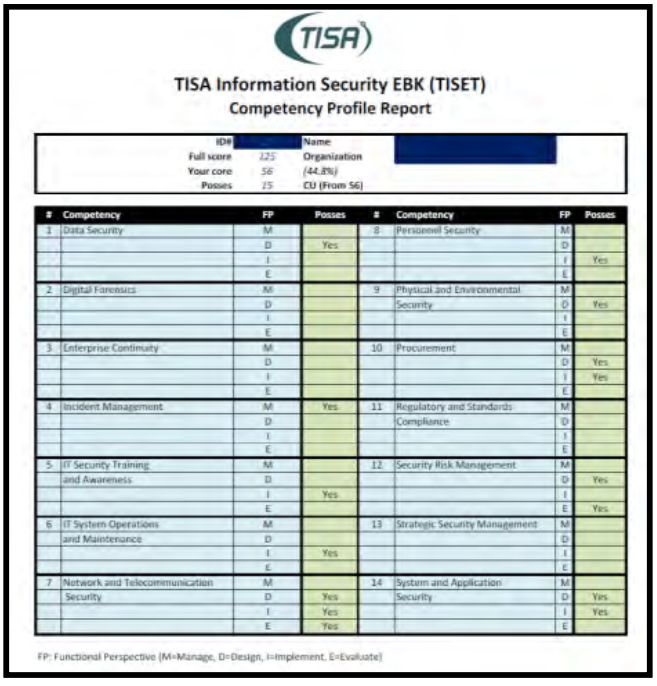
Max Score



Min Score

Avg Score

Example of TISA TISET Report

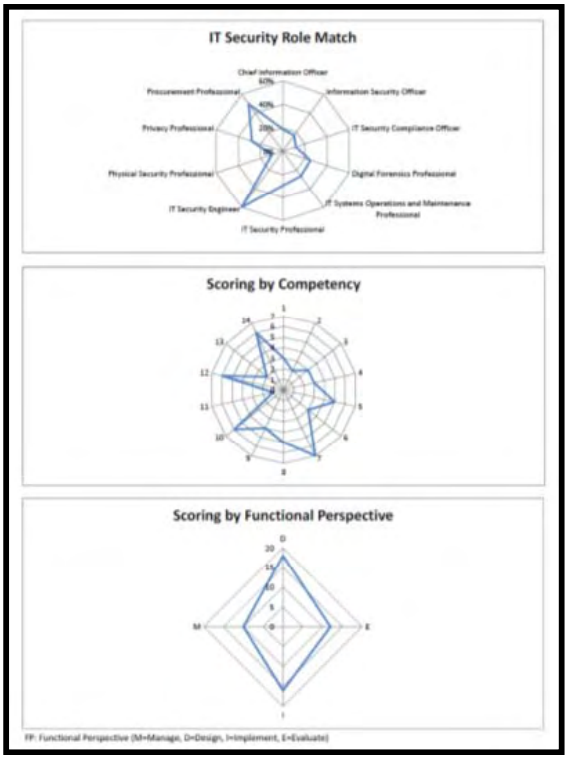


TISA Information Security EBK (TISET)
Competency Profile Report

ID#		Name:	
Full score	125	Organization	
Your core	56	(44.8%)	
Posses	15	CU (From 56)	

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

FP: Functional Perspective (M=Manage, D=Design, I=Implement, E=Evaluate)



TISET Pilot Exam Summary

☑ *The Top Performer, scoring 78%*

- *The IT Auditor, with a background of IT System Engineer, having 7 professional certificates (CISSP, CISA, Security+, CCNA, CEH, MCITP, PMP)*

☑ *The Top Ten performers, scoring range 55%-78%*

- *The Top Five scores 60%-80%*
- *Those only 1 PMPs listed at the Top ranking*
- *Those only 2 CISSPs listed in the Top Ten Ranking*
- *Those only 5 CISAs listed in the Top Ten Ranking*
- *The Two of Top performers didn't specify having any certificate*
- *Five of Top Ten performers are InfoSec Consultants,*

IT Professional Certificates:

- Yes 40% = 36 persons
- No 60% = 54 persons

Those 36 persons have hold 78 professional certificates:

- CISSP = 2 persons
- CISA = 5 persons
- CISM = 0 persons
- Security+ = 23 persons
- MCSE = 5 persons
- CCNA = 2 persons
- CEH = 4 persons
- ITIL = 4 persons
- PMP = 1 persons
- Others = 26 persons

TISET Pilot Exam Summary: Next Target

❖ First Launch of a real TISA ITS-EBK Exam

- In the first quarter of 2010 (about February 2010)

❖ Accrue a Databank of TISA Exam questions

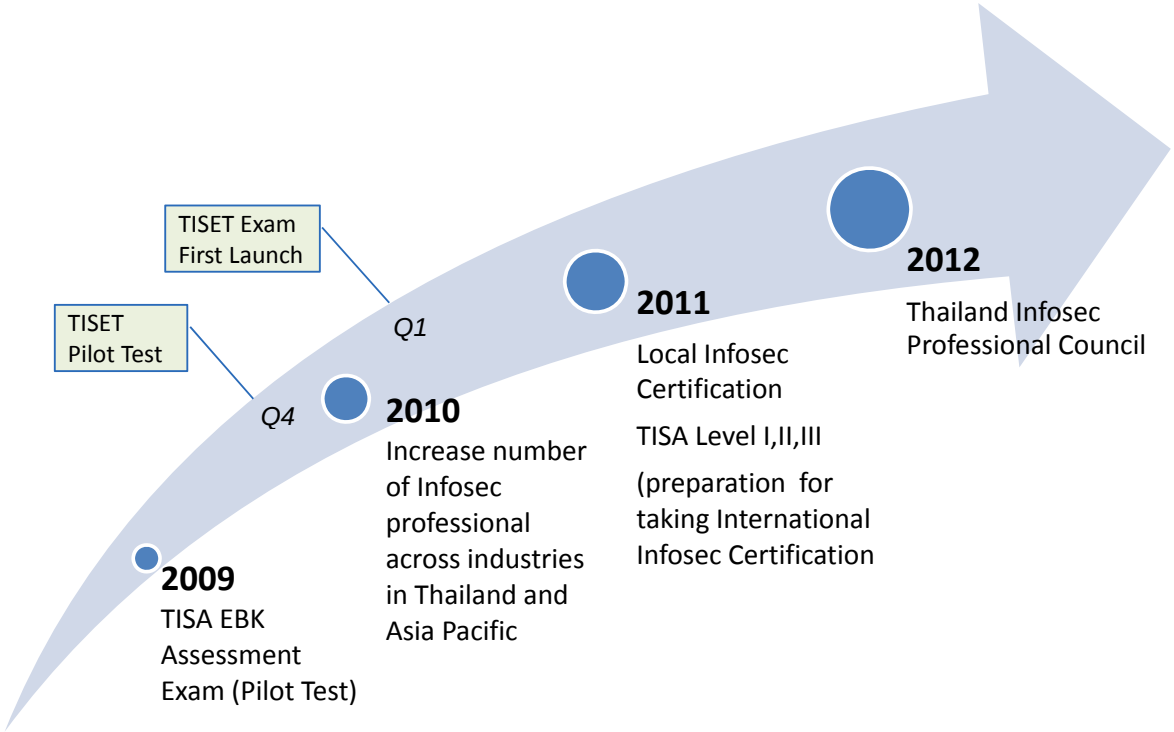
- Volunteers of qualified professional in developing more exam questions
- Qualify the exam questions
- Localize the exam questions in Thai language
- Promote Information Security practitioners to sit for an examination

❖ Accredit to the TISA TISET Examination

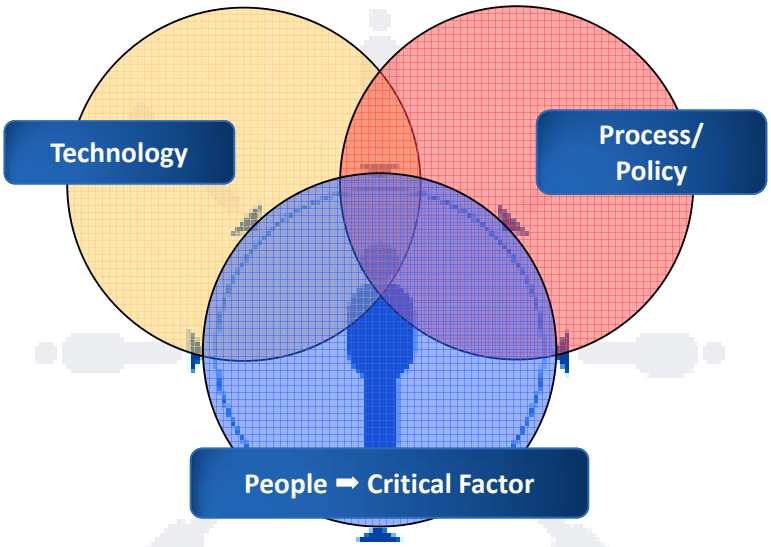
- Supported and Accredited by Government Agents
- Endorsed by TISA and Thailand Information Security Professional Council

TISET: Certification Roadmap

TISA: TISET Exam
Mission and The Next Target



Back to the Basic : PPT Concept



People is "KEY" ⇒ Information Security Professional Development Programme

สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ
Thailand Information Security Association (TISA)

http://www.TISA.or.th

Thailand Information Security Association