Information Technology (IT)

Security - Controls - Assessment

Presented By: George B. Tselentis, Adjunct Professor

Information Technology (IT)

Security - Controls - Assessment

The Focus

Security Project Assessment

Security Domains

IT Security *Domains*

The Ten Security Domains of CISSP

Certified Information Security Systems Professional

1. Access Control Systems & Methodology-requires that the candidate understands the concepts, systems and methodologies involved in granting and restricting access to resources.

2. Applications & Systems Development-requires that the candidate understand the security controls found in systems and application software, such as the affects of malicious code on distributed application environments and the security controls involved in data warehousing.

3. Business Continuity & Disaster Recovery Planning-involves the preparation, planning and updating of specific actions to protect mission critical services and data.

4. Cryptography-this domain addresses the concepts, means and methods of encrypting data to ensure authenticity, integrity, and confidentiality.

5. Law, Investigation & Ethics-this domain addresses computer crime laws, methods for gathering evidence, and related ethical issues.

IT Security *Domains*

The Ten Security Domains of CISSP

Certified Information Security Systems Professional

6. Operations Security (Computer)-this domain identifies the controls over hardware, media and the operators of these resources, and issues related to auditing and monitoring.

7. Physical Security-this domain involves the threats, vulnerabilities and countermeasures utilized to physically protect enterprises resources.

8. Security Architecture & Models-this domain involves the design, concepts, standards, and implementation security measures that ensure the availability, integrity and confidentiality of operating systems, applications and equipment.

9. Security Management Practices-involves the identification of a company's information assets, and the development, documentation and implementation of security policies.

10. Telecommunications & Network Security-this domain involves designing and planning voice and data infrastructure and communications with a security strategy that includes preventative, detective and corrective measures.

IT Security *Domains*

The Ten Security Domains of CISSP

Certified Information Security Systems Professional

- NOTE from George B. Tselentis:
- I am adding an additional DOMAIN that I feel is very important and often overlooked
- (11) Training: The training of the “general user”, the “technical user” and “senior management” should not be overlooked. The training of the aforementioned groups will give the users an understanding of why Security is important. Security is important because it affects every aspect of a company, it protects the company, it protects the customer, it protects the jobs of the employees working at that company. For proof of what I have just said, look at the aftermath of post 911 downtown Manhattan, jobs lost, vendors lost business and businesses went of business.

IT Security *Domains*

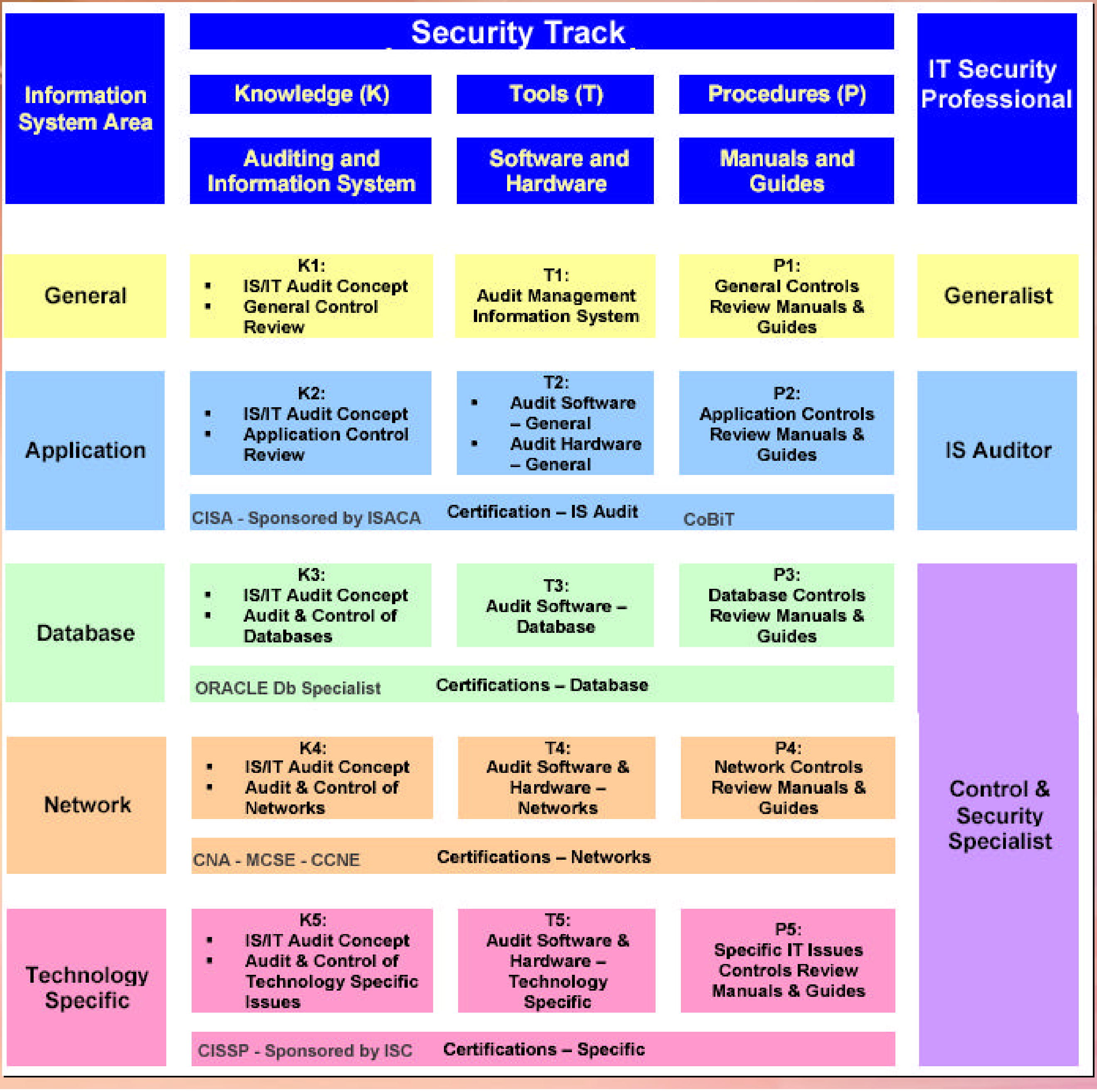
Security Project Planning: A robust governance model that addresses time and cost constraints but also monitors the compliance insures that govern the client company.

Seven Project Rules:

1. Prove: Need to prove specific improvements are necessary.
2. Coach: By developing a performance matrix you can show long term and short term goals.
3. Influence: A systematic approach to continuous improvement by applying constant pressure
4. Partner: You need to have one member of Senior Management onboard, approach them with the question "What can I do?"
5. Pilot: Create a teaching case through a successful completed project.
6. Benchmark: Ask the question " If you had the highest market share and the highest customer satisfaction and can charge the highest prices how would that make you feel?
7. Align: Align the conversations with senior management in a way that speaks their language.

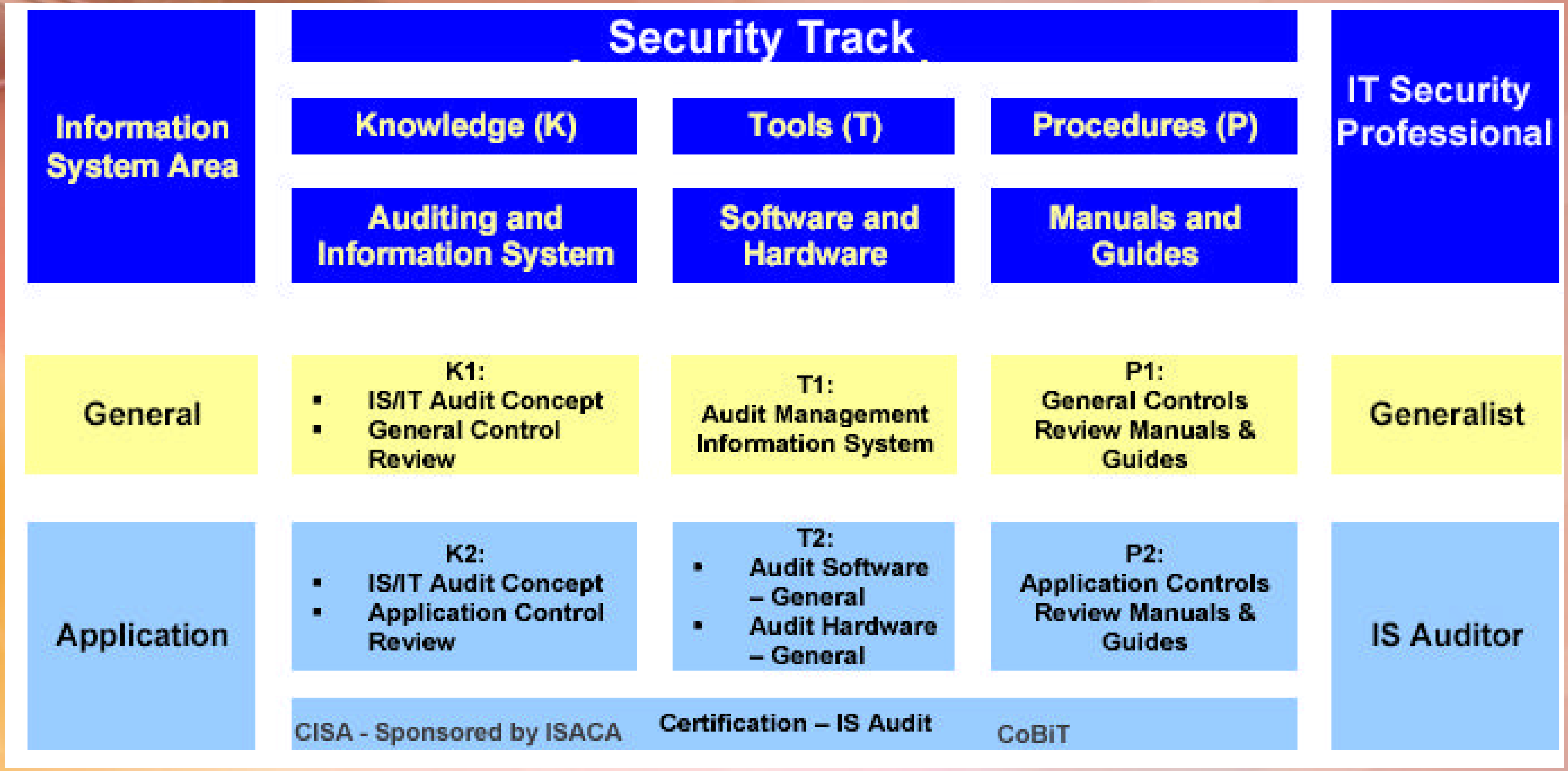
ROI - EPS - Growth Rate - ROA - EBITDA - Revenues - Share Price.

IT Security *Matrix*



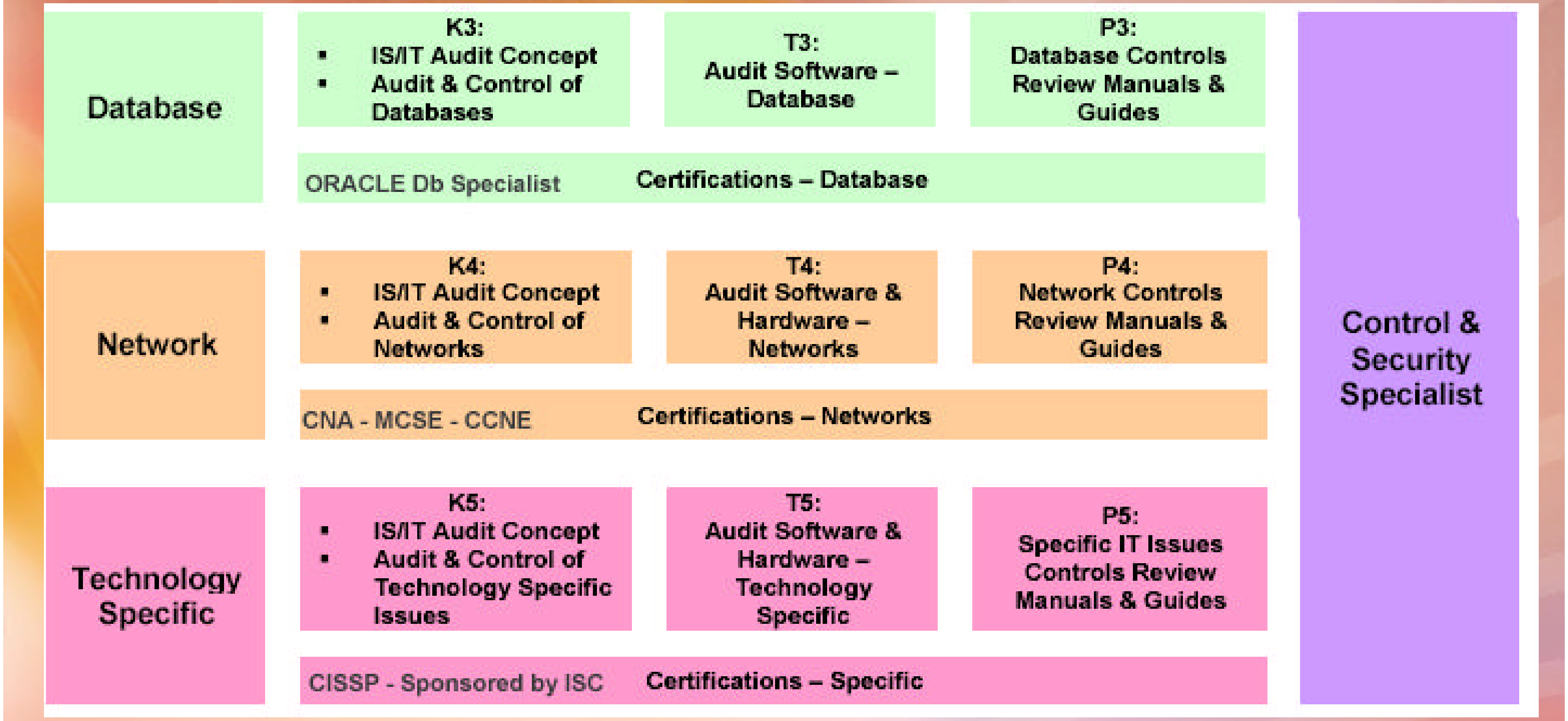
Information System Area	Security Track			IT Security Professional
	Knowledge (K)	Tools (T)	Procedures (P)	
	Auditing and Information System	Software and Hardware	Manuals and Guides	
General	K1: ▪ IS/IT Audit Concept ▪ General Control Review	T1: Audit Management Information System	P1: General Controls Review Manuals & Guides	Generalist
Application	K2: ▪ IS/IT Audit Concept ▪ Application Control Review	T2: ▪ Audit Software – General ▪ Audit Hardware – General	P2: Application Controls Review Manuals & Guides	IS Auditor
	CISA - Sponsored by ISACA	Certification – IS Audit	CoBiT	
Database	K3: ▪ IS/IT Audit Concept ▪ Audit & Control of Databases	T3: Audit Software – Database	P3: Database Controls Review Manuals & Guides	Control & Security Specialist
	ORACLE Db Specialist	Certifications – Database		
Network	K4: ▪ IS/IT Audit Concept ▪ Audit & Control of Networks	T4: Audit Software & Hardware – Networks	P4: Network Controls Review Manuals & Guides	
	CNA - MCSE - CCNE	Certifications – Networks		
Technology Specific	K5: ▪ IS/IT Audit Concept ▪ Audit & Control of Technology Specific Issues	T5: Audit Software & Hardware – Technology Specific	P5: Specific IT Issues Controls Review Manuals & Guides	
	CISSP - Sponsored by ISC	Certifications – Specific		

IT Security *Matrix*



Information System Area	Security Track			IT Security Professional
	Knowledge (K)	Tools (T)	Procedures (P)	
	Auditing and Information System	Software and Hardware	Manuals and Guides	
General	K1: ▪ IS/IT Audit Concept ▪ General Control Review	T1: Audit Management Information System	P1: General Controls Review Manuals & Guides	Generalist
Application	K2: ▪ IS/IT Audit Concept ▪ Application Control Review	T2: ▪ Audit Software – General ▪ Audit Hardware – General	P2: Application Controls Review Manuals & Guides	IS Auditor
	CISA - Sponsored by ISACA	Certification – IS Audit	CoBiT	

IT Security *Matrix*



Database	K3: ▪ IS/IT Audit Concept ▪ Audit & Control of Databases	T3: Audit Software – Database	P3: Database Controls Review Manuals & Guides	Control & Security Specialist
	ORACLE Db Specialist	Certifications – Database		
Network	K4: ▪ IS/IT Audit Concept ▪ Audit & Control of Networks	T4: Audit Software & Hardware – Networks	P4: Network Controls Review Manuals & Guides	
	CNA - MCSE - CCNE	Certifications – Networks		
Technology Specific	K5: ▪ IS/IT Audit Concept ▪ Audit & Control of Technology Specific Issues	T5: Audit Software & Hardware – Technology Specific	P5: Specific IT Issues Controls Review Manuals & Guides	
	CISSP - Sponsored by ISC	Certifications – Specific		

Decision Point

- Do we have to do it?
- Can we wait?
- How much will it cost either way?
- Can we do it “In-House”?

Penalties

- Red Cross fined 5 Million
- Federal Government beginning to crack down

- Building a security program
- Project management principles
- Repeatable process
- Following guidelines

Dangers

- Web Threats
- Disgruntled employee walking away with the business
- Fines
- Forced shutdown