Arab ICT Organization

Training workshop

"Setting up an Electronic Certification Authority"

Date : November 28 - December 1st 2016 **[4 days]**

Venue : Tunis

Training workshop :
"Setting up an Electronic Certification Authority"

Date : November 28 - December 1st 2016 **[4 days]**

Venue : Tunis -Tunisia

Framework :

- "AICTO" Action plan [2016] - Pillar III "**Capacity Building**" : Building Arab skills capacity in the field of ICT.

Main objectives :

The goal of the training is to develop the capacity of the attendees to protect critical assets, infrastructure, and information by strengthening your organization's defensive posture through continuous, automated protection and monitoring of your sensitive information technology infrastructure to reduce compromises, minimize the need for recovery efforts, and lower associated costs. The main objectives are listed in the following:

- To provide an overview of the techniques allowing the identification of the critical assets and their core elements.
- To formally establish a governance framework to ensure that the security risks affecting critical assets are managed consistently and appropriately on an ongoing basis.
- To identify key third parties and effectively manage the associated risks that may have an impact on the security of an organisation's critical assets
- To increase critical systems' security awareness throughout the Arab industrial ecosystem and to ensure that all personnel have the appropriate knowledge and skills required to fulfill their role

Target Audience :

Arab ministries of Interior, **Arab ministries of Defence,** Public sector (ICT Ministries and public institutions), Cybersecurity agencies, ICT regulators, ICT companies, ICT research organizations, Service providers, Telecom. Operators, Academia & All interested parties.

Agenda :

Day 1	**Terminology, taxonomy and fundamental concepts.**
	▪ Security challenges and cryptography risks ▪ Digital signature/ciphering implementations ▪ Trust in the cyberspace ▪ PKI protocols: SSL/TLS, IPSec, S/MIME
Day 2	**Strategy/policy issues**
	▪ PKI roles and responsibilities ▪ Certification authority architectures ▪ Agreements and relying parties ▪ Strategic documents (CP, CPS) ▪ Key management policies
Day 3	**Operational issues**
	▪ Creating and managing a certification authority ▪ Identifying the core functionalities of the PKI ▪ Managing the issuance and revocation of digital certificates ▪ Integrating digital certificates into applications and services
Day 4	**Governance and economic issues**
	▪ PKI compliance ▪ Evaluation criteria ▪ Gap assessment ▪ Accreditation and certification ▪ Economic models for PKI