UNIX Trainers & Consultants
Head Office: Wema Twins Annex, Plot No. 181,
Boko-Bagamoyo Road, P.O. Box 33826, Dar es salaam.
Mob: +255-715-361-880/+255-754-361-880
Email: info@unixtrainers.com; training@unixtrainers.com
Website: www.unixtrainers.com

Information Security Management in the Public Sector

Course Overview:

Information security management describes the set of policies and procedural controls that IT and business organizations implement to secure their informational assets against threats and vulnerabilities. Many organizations develop a formal, documented process for managing InfoSec. With an ever-changing climate of technology and threats (both technical and human), the need for trained security personnel to protect our information becomes an increasingly critical evolutionary task.

Information is at risk from many sources, legal, electronic, physical, internal, and external to mention a few. It is paramount that security and related management personnel have an understanding of the risks, controls, and countermeasures that are available to secure information and technology within an effective management framework. Furthermore, utilizing countermeasures, best practices and management techniques will mitigate electronic and physical risks and enhance the protection of an organization

Course Objectives:

At the end of this course, the participants will be able to:

- Gain knowledge of the concepts relating to information security management (confidentiality, integrity, availability, vulnerability, threats, risks, countermeasures, etc.)
- Understand the current legislation and regulations which impact information security management
- Be fully aware of current national and international standards such as ISO 27002, frameworks and organizations which facilitate the management of information security
- Understand the current business and common technical environments in which information security management has to operate
- Gain knowledge of the categorization, operation, and effectiveness of controls of different types and characteristics

Course Coverage:

Topic 1: Overview of Information Security:

- What is Information Security?
- Examples of Information Security Incidents
- What is Information Security Management?
- Human Aspect of Information Security
- Social Engineering

Topic 2: Information Security for Server Systems:

- Attacks on Personal Computers and Smartphones and countermeasures
- Information Security Risk Management
- What is the Risk Management process?
- Identifying Information Assets
- Identifying Security Risks and evaluation
- Risk Treatment

Topic 3: Security Risk Management as an Organization:

- Information Security Governance
- Information Security Management System (ISMS)
- Information Security Policy, Standards, and Procedures
- Information Security Evaluation
- Security Incident Response

Topic 4: Information Security and Cryptography:

- Requirements for Secure Communication
- What is Cryptography?
- Classic and Modern Cryptography
- Common Key Cryptography algorithms: DES, Triple DES, AES
- Problems of Key Distribution for Common Key Cryptography

Topic 5: Data Integrity and Digital Signature:

- Integrity of Data
- Hash Function
- Digital Signature
- Public Key Certificate and Public Key Infrastructure (PKI)
- Certificate Authority

Targeted Groups:

- Risk Management
- IT Security and IT Security Auditing
- Technical IT Management
- Those with involvement in systems integration and corporate IT development
- Financial controllers with a technical interest may also benefit from the seminar

---