AFRICAN ADVANCED LEVEL TELECOMMUNICATIONS INSTITUTE (AFRALTI)

TRAINING WORKSHOP OUTLINE

Title:	**CYBER SECURITY & RISK ANALYSIS**
Proposed Dates:	**11th – 15th August 2014.**
Duration:	**5 days**
Location:	**Blantyre, Malawi.**

Course Description:
Today, the Internet has become an integral part of modern societies with over 2.4 billion users connected in the world. This has in turn created a new realm for malicious users to perpetrate fraud, theft and forgery and transmit illegitimate content just as it happens in the traditional offline setup.

Government agencies, business organisations and individuals are nowadays depending on the Internet to fulfil their obligations and business objectives. With the sophistication cyber attacks, availability of user-friendly attack tools, loopholes in legal frameworks, organised online crimes, vulnerabilities in hardware and software systems, cyber security continues to be the greatest concern.

This intensive 5-day course discusses the safeguards that should be taken to ensure that government agencies, business organisations and end users benefit from the full advantages of Internet. The course also prepares participants for security related certifications like CISA, CISM, and CISSP among others.

Target Audience
This course will significantly benefit ICT professionals who design, build and manage enterprise information security, and anyone who is concerned about the integrity of the cyber world.

Expected Outcomes:
Upon completion of this course, participants will be able to:

- Demonstrate understanding of the concepts of information systems and cyber security.
- Demonstrate a good understanding cyber technology
- Explain the information security governance and risk management techniques
- Explain the use of cryptography in enhancing cyber security
- Design security architecture to provide CIA
- Explain the day to day operations that ensure integrity of business processes
- Discuss measures to ensure secure network communications
- Explain vulnerability assessment and audit techniques
- Discus the importance of business continuity and disaster recovery

- Explain the legal and regulatory and compliance requirements in information handling

Prerequisites:
Good knowledge of ICT and Internet skills

Methodology

The curriculum consists of instructor-led training covering both theory and practical lessons. Participants will be provided with security related resources and all tools needed to enhance safety in the cyber world.

Training Contents

Module 1: Fundamentals of Cyber Security
- Describe the goals of cyber security.
- Describe the evolution of cyber security.
- Describe the drivers for cyber security.
- Describe cyber attacks types (reconnaissance attacks; access attacks; DOS,DDOS).
- Discuss how cyber crimes are threat to government, public sector; private sector and citizens.
- Describe cyber attacks mitigation.

Module 2: Understanding Cyber Technology
- Describe the cyber world
- Understanding the TCP/IP
- Describing the internet architecture and design
- Describe communication channels
- Describe internetworking components
- Describe cyber applications

Module 3: Information Security Governance and Risk Management
- Identification of an organization's information assets
- development, documentation and implementation of policies, standards, procedures and guidelines
- Information classification/ownership
- Risk management concepts: Asset Identification, Exposures and Countermeasures
- Personnel security
- Security education, training and awareness

Module 4: Applied Cryptography
- Explain how cryptology consists of cryptography (encoding messages) and cryptanalysis (decoding messages) and how these concepts apply to modern day cryptography.
- Explain how securing communications by various cryptographic methods, including encryption, hashing and digital signatures, ensures confidentiality, integrity, authentication and non-repudiation.
- Describe the use and purpose of hashes and digital signatures in providing authentication and integrity.
- Explain how authentication is ensured.

- Explain how integrity is ensured.
- Explain how data confidentiality is ensured using symmetric encryption algorithms and pre-shared keys.
- Explain how data confidentiality is ensured using asymmetric algorithms in a public key infrastructure (PKI) to provide and guarantee digital certificates.

Module 5: Cyber Security Architecture and Design

- Fundamental concepts of security models
- Capabilities of information systems (e.g. memory protection, virtualization)
- Countermeasure principles - design, implement, monitor, and secure, operating systems, equipment, networks and applications
- Vulnerabilities and threats

Module 6: Operations Security

- Resource protection - the controls over hardware, media and the operators with access privileges to any of these resources.
- Incident response and handling
- Attack prevention and response
- Patch and vulnerability management
- Securing Administrative Access with Authentication, Authorization, Accounting (AAA)
- Multifactor authentication

Module 7: Securing Network Communications

- Describe firewalls
- virtual private network
- Intrusion detection systems and intrusion prevention systems

Module 8: Vulnerability assessment and Audit

- System scanning
- Vulnerability assessments tools vulnerability assessments
- Executing penetration tests
- Review log files and working with syslog servers

Module 9: Business Continuity and Disaster Recovery Planning

- Business impact analysis
- Recovery strategy
- Disaster recovery process
- Provide training

Module 10: Legal, Regulations, Investigations and Compliance

- Describe cyber crimes laws and regulations
- Describe methods of cyber crimes investigations – gathering evidence to determine whether a crime has been committed.
- Computer forensic procedures
- Admissible evidence - compliance requirements/procedures.

FACILITATOR PROFILES

MR DAVID NJOGA

David Njoga has over 15 years of experience in the ICT space, having grown his profession in Systems Administration, Network Management and Security Management making him a highly accomplished, talented and knowledgeable ICT professional with extensive knowledge of designing new ICT solutions, systems administration, network management, information security assurance and information systems audit to improve business productivity and efficiency.

David has worked in the Kenya Defence Forces in major IT functional roles between 2003 and 2010, and the national carrier, Kenya Airways Ltd between 2010 and 2012 as Business Continuity Analyst. He has a wide experience in the practice and research in Enterprise Risk Management specializing in IT Value Delivery, IT Performance Measurement, IT Resource Management, Strategic Alignment, Project Management, Process Integration and Business Continuity Management.

He holds a BSc Information Sciences from Moi University, and a holder of a MSc IT degree specializing in Information Systems Security and Audit & Networking Communications of Strathmore University.

In addition to being a Certified Information Systems Auditor (CISA) and holder of a Certificate of the Business Continuity Institute (CBCI), David is a member of the Information Systems Audit and Control Association (ISACA), the Business Continuity Institute (BCI) and the Institute of Risk Management (IRM).

MR STEVE GACHOGU

Mr. Stephen Gachogu holds an honours degree of Bachelor of Science in Computing and Information Systems from the University of Portsmouth, United Kingdom. He also holds a Diploma in Information Technology , a Diploma in Technical Education and has over 10 years experience in the ICT industry.

Mr. Gachogu has undergone extensive ICT training and undertaken a lot of research work on the design and implementation of enterprise IP networks. He holds certificates on Wireless LANs and Security, Network Security, WIMAX, VOIP, Backbone Routing, Internet Development Tools awarded by various institutions including USTTI-USA, IIT-Canada. He has attended other ICT courses in Kenya, South Africa, United Kingdom and the USA.

Mr. Gachogu holds active certifications in Cisco Certified Network Professional (CCNP), Cisco Certified Network Associate (CCNA), CCNA Security and is Cisco Certified Academy Instructor (CCAI) for CCNA and CCNP Courses.

His area of specialization is in the design and implementation of local and wide area enterprise IP networks utilizing multilayer switching and advanced routing technologies. He has expert knowledge of Ethernet technology, Wireless LANs standards and TCP/IP protocol suite. Mr. Gachogu also specializes in deployment of enterprise security, IPv6, MPLS and VOIP technologies.

For more information, please contact us on
Tel: +254 710 207 061, +254 733 444 421
info@afralti.org or training@afralti.org www.afralti.org