TRAINING COURSE ON CYBERSECURITY

TITLE: INFORMATION SECURITY MANAGER COURSE (ADVANCED)

Duration: 5 days

Dates: 23rd to 27th April 2018

Venue: Arusha, Tanzania

Course Outline:

Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations Identify and manage information security risks to achieve business, organizational or national objectives. Create a program to implement the information security strategy. Implement an information security program. Oversee and direct information security activities to execute the information security program.

Learning Objectives

1. Information security governance (23 percent) — Establish and maintain a framework to provide assurance that information security strategies are aligned with the business objectives and consistent with applicable laws and regulations.
2. Information risk management (22 percent) — Identify and manage information security risks to achieve business objectives.
3. Information security program development (17 percent) —Create and maintain a program to implement the information security strategy.
4. Information security program management (24 percent) —Oversee and direct information security activities to execute the information security program.
5. Incident management and response (14 percent) —Plan, develop and manage a capability to detect, respond to and recover from information security incidents.
6. Emerging Trends: EU General Data Protection Regulations (GDPR) and its implications.

Target Audience

The course is based on the Certified Information Security Manager, CISM® examination and provides participants with the knowledge and understanding that they require to direct and manage Information Security entities. Target groups include but not limited to:

- Information Security Directors /Managers/Officers/Professionals
- Directors/Managers in charge of CERTS
- Telco professionals overseeing network security
- Auditors involved in Information Security

FACILITATOR – **John Walubengo, MSc, BSc, CISA**

Mr. Walubengo holds an MSc in Strategic Business IT (University of Portsmouth) and a BSc in Mathematics (Kenyatta University). He holds several industry certifications including the CCNA (Certified Cisco Network Associate) and the CISA (Certified Information Systems Auditor) certification. His area of specialisation is in ICT Governance, Security, Policy & Strategy.

He has over 20 years experience in the ICT Training and Consulting. His work experience included working for the Strathmore University as the IT Course Director and as the founding Dean, Faculty of Computing at the Multimedia University. He is currently a PhD candidate at the University of Nairobi and continues to provide Consultancy services to Government and other organisations. He writes a weekly column on topical ICT issues in one of the largest dailies in East and Central Africa.

Course Delivery (5Days)

DAY1

Domain 1 – Information Security Governance

- Explain the need for and the desired outcomes of an effective information security strategy
- Create an information security strategy aligned with organizational goals and objectives
- Gain stakeholder support using business cases
- Identify key roles and responsibilities needed to execute an action plan
- Establish metrics to measure and monitor the performance of security governance

-Exercises/Practice Qtns.

==========

DAY2

Domain 2 – Information Risk Management

- Explain the importance of risk management as a tool to meet business needs and develop a security management program to support these needs
- Identify, rank, and respond to a risk in a way that is appropriate as defined by organizational directives
- Assess the appropriateness and effectiveness of information security controls
- Report information security risk effectively

-Exercises/Practice Qtns

==========

DAY3

Domain 3- Information Security Program Development and Management

- Align information security program requirements with those of other business functions
- Manage the information security program resources
- Design and implement information security controls
- Incorporate information security requirements into contracts, agreements and third-party management processes

-Exercises/Practice Qtns

==========

DAY4

Domain 4 – Information Security Incident Management

- Understand the concepts and practices of Incident Management

Identify the components of an Incident Response Plan and evaluate its effectiveness

- Understand the key concepts of Business Continuity Planning, or BCP and Disaster Recovery Planning, or DRP
- Be familiar with techniques commonly used to test incident response capabilities

Exercise Practice /Qtn

==========

DAY 5

General Data Protection Regulation (GDPR)

- Overview, Issues, Implications.
- Privacy Principles
- Privacy Impact Assessments
- GDPR Overview & Key Terms
- Data Protection Impact Assessment (DPIA) Overview & Specifics
- Data Protection Impact Assessment Tool
- Relationship of Privacy Principles to GDPR DPIA Requirements
- Key Points for DPIAs

Closing Session

====ENDS==

For more details please contact:

EACO

Mr. Hermenegilde Ntahomvukiye
Email: hra@eaco.int

Multimedia University of Kenya

Mrs. Virginia Onyara
Email: vonyara@mmu.ac.ke


EACO
East African
Communications
Organisation


MMU