



## **AFRICAN ADVANCED LEVEL TELECOMMUNICATIONS INSTITUTE**

### **TRAINING WORKSHOP OUTLINE**

**Title:** Risk Management and Information Systems Control  
**Dates:** 4<sup>th</sup> – 10<sup>th</sup> January 2018  
**Venue:** AFRALTI, Nairobi, Kenya

---

#### **COURSE DESCRIPTION:**

In today's business environment, enterprises need to innovate in order to survive and flourish. Innovation, however, almost always involves risk. To maintain or attain their competitiveness, future-thinking enterprise leaders are increasingly recognizing the need for professionals who understand technology, and specifically how to implement and align effective risk management and control frameworks with their enterprise's business goals.

This course has been developed to help meet the rising demand for professionals with this critical blend of technical and business understanding and fully understand risk management.

When a student leaves this 5-day intensive class they will have deep understanding and experience in all facets of risk management.

#### **TARGET AUDIENCE AND PRE-REQUISITES:**

IT professionals interested in understanding risk and information systems controls. This course is for IT professionals, risk professionals, business analysts, project manager and/or compliance professionals, seeking to learn how to work towards evaluation and mitigation of enterprise risks. These include:

- IT professionals
- Risk professionals
- Control professionals
- Business analysts
- Project managers
- Compliance professionals

#### **TRAINING METHODOLOGY**

The course is delivered using a blended learning model of lectures, discussions, case studies, assessment and practical exercises using a highly-structured, learner-centered teaching methodology that ensures maximum learning. Helpful learning resources will be provided.

## **COURSE OBJECTIVES:**

The course covers the following four security domain:

### **Domain 1—Risk Identification**

Identify the universe of IT risk to contribute to the execution of the IT risk management strategy in support of business objectives and in alignment with the enterprise risk management (ERM) strategy.

### **Domain 2—IT Risk Assessment**

Analyze and evaluate IT risk to determine the likelihood and impact on business objectives to enable risk-based decision making.

### **Domain 3—Risk Response and Mitigation**

Determine risk response options and evaluate their efficiency and effectiveness to manage risk in alignment with business objectives.

### **Domain 4—Risk and Control Monitoring and Reporting**

Continuously monitor and report on IT risk and controls to relevant stakeholders to ensure the continued efficiency and effectiveness of the IT risk management strategy and its alignment to business objectives.

## **DETAILED COURSE OUTLINE**

### **Day 1 – Risk Management and Information Systems Control**

- Differentiate between risk management and risk governance
- Identify the roles and responsibilities for risk management
- Identify relevant standards, frameworks and practices
- Explain the meaning of key risk management concepts, including risk appetite and risk tolerance
- Differentiate between threats and vulnerabilities
- Apply risk identification, classification, quantitative / qualitative assessment and evaluation techniques
- Describe the key elements of the risk register
- Describe risk scenario development tools and techniques
- Help develop and support risk awareness training tools and techniques
- Relate risk concepts to risk assessment

### **Day 2 – Risk Response**

- List various parameters for risk response selection
- List the different risk response options
- Describe risk responses may be most suitable for a high-level risk scenario
- Describe how exception management relates to risk management
- Monitor existing risk.
- Report noncompliance and other changes in information risk
- Describe how residual risk relates to inherent risk and risk appetite
- Describe the need for performing a cost-benefit analysis when determining a risk response

- Describe the attributes of a business case to support project management
- Identify standards, frameworks and leading practices related to risk response

### **Day 3 – Risk Monitoring**

- As a result of completing this chapter, the CRISC candidate should be able to:
- Explain the principles of risk ownership.
- List common risk and compliance reporting requirements, tools and techniques.
- Describe various risk assessment methodologies.
- Differentiate between key performance indicators and Key Risk Indicators.
- Describe, at a high level, data extraction; aggregation; and, analysis tools and techniques.
- Differentiate between various types of processes to review organization's risk monitoring process.
- List various standards, frameworks, and practices related to risk monitoring.

### **Day 4 – Information Systems Control Design and Implementation**

- List different control categories and their effects
- Judge control strength.
- Explain the importance of balancing control cost and benefit.
- Leverage understanding of the SDLC process to implement IS controls efficiently and effectively.
- Differentiate between the four high-level stages of the SDLC.
- Relate each SDLC phase to specific tasks and objectives.
- Apply core project management tools and techniques to the implementation of IS controls.

### **Day 5 – Information Systems Control Maintenance and Monitoring**

- Describe the purpose and levels of a maturity model as it applies to the risk management process.
- Compare different monitoring tools and techniques.
- Describe various testing and assessment tools and techniques.
- Explain how monitoring of IS controls relates to applicable laws and regulations
- Understand the need for control maintenance.

**For more information, please contact us on**  
**Tel: +254 710 207 061, +254 733 444 421**  
**[training@afraiti.org](mailto:training@afraiti.org) or [info@afraiti.org](mailto:info@afraiti.org)**  
**[www.afraiti.org](http://www.afraiti.org)**