THE REPUBLIC UNITED OF TANZANIA

INSTITUTE OF ACCOUNTANCY ARUSHA

IAA/BP/4

RE: INVITATION TO THE TRANING ON CYBER SECURITY COURSE.

INTRODUCTION

The Institute of Accountancy Arusha is pleased to invite you to attend a "**Cyber security course**".

Cyber security refers to a set of techniques used to protect systems, network and data from cyber-attacks. It aims at ensuring a system's integrity and confidentiality of information.

There are many kinds of cyber-attacks such as malware, phishing, unpatched software, hijacking files, hacking and identity theft, to name a few.

Cybersecurity is critical to business and involves the protection of IT systems and data from cyber threats such as computer-assisted fraud, espionage, sabotage or vandalism

Cyber security covers not only safeguarding confidentiality and privacy, but also the availability and integrity of data, both of which are vital for the quality and safety of computing assets and information systems. Security breaches can occur when we use paper records, send information using fax machines and even verbally. However, the consequences of security breaches with digital information are potentially far more severe, as information can be distributed more easily and to a far wider audience. Cyber-breaches are costly – in terms of expense, recovery time and through damage to reputation.

In governments cyber breaches Survey in 2018, 46% of businesses reported a cyber-breach or attack. That is why cyber security is a high priority for business and why all staff must be aware of how to implement protective measures.

Some few benefits of managing cybersecurity?

- Protect networks and data from unauthorized access
- Improved information security and business continuity management
- Improved stakeholder confidence in your information security arrangements
- Improved company credentials with the correct security controls in place
- Faster recovery times in the event of a breach

This cyber security course will make you well versed with the processes and practices followed for protecting networks and data from unauthorized attacks. This course enables you to detect vulnerabilities of a system, ward off attacks and manage emergency situations.

Course Objectives

Upon completion of Cyber Security Course, you will demonstrate competence in cyber security after learning the following:

Cybersecurity Introduction & Overview

- ✓ Introduction to Cybersecurity
  - The evolution of Cybersecurity
  - Cybersecurity & situational awareness
  - The Cybersecurity skills gap
- ✓ Difference between Information Security & Cybersecurity
  - Protecting digital assets
- ✓ Cybersecurity objectives
  - Confidentiality, integrity, & availability
  - Nonrepudiation
- ✓ Cybersecurity roles
  - Governance, risk management, & compliance
  - What does a Cybersecurity professional do?
  - Information Security roles
  - Board of Directors
  - Executive management
  - Senior Information security management
  - Cybersecurity practitioners
- ✓ Cybersecurity domains
  - Cybersecurity concepts
  - Security architecture principles
  - Security of networks, systems, applications, & data
  - Incident response
  - Security implications & adoption of evolving technology

Cybersecurity Concepts

- ✓ Risk
  - Approaches to Cybersecurity

- Key terms & definitions
- Likelihood & impact
- Approaches to risk
- Third-party risk
- Risk management

✓ Common attack types & vectors

- Threat agents
- Attack attributes
- Generalized attack process
- Nonadversarial threat events
- Malware & attack types

✓ Policies & procedures

- Policy life cycle
- Guidelines
- Policy frameworks
- Types of Information Security policies
- Access control policy
- Personnel Information Security policy
- Security incident response policy

✓ Cybersecurity controls

- Identity management
- Provisioning & de-provisioning
- Authorization
- Access control lists
- Privileged user management
- Change management
- Configuration management
- Patch management

Security Architecture Principles

✓ Overview of security architecture

- The security perimeter
- Interdependencies

- Security architectures & frameworks
  SABSA & the Zachman framework
- The open group architecture framework (TOGAF)

✓ The OSI model

- TCP/IP

✓ Defense in Depth

✓ Firewalls

- Firewall general features
- Network firewall types
- Packet filtering firewalls
- Stateful inspection firewalls
- Stateless vs. stateful
- Examples of firewall implementations
- Firewall issues
- Firewall platforms

✓ Isolation & segmentation

- VLANs
- Security zones & DMZs

✓ Monitoring, detection, and logging

- Ingress, egress, & data loss prevention (DLP)
- Antivirus & anti-malware
- Intrusion detection systems
- IDS limitations
- IDS policy
- Intrusion prevention systems

✓ Cryptography Fundamentals

- Key elements of cryptographic systsms
- Key systems

✓ Encryption techniques

- Symmetric (private) key encryption
- Asymmetric (private) key encryption
- Elliptical curve cryptography
- Quantum cryptography

- Advanced encryption standard
- Digital signature
- Virtual private network
- Wireless network protections
- Stored data
- Public key infrastructure

✓ Encryption applications

- Applications of cryptographic systems

Security of Networks, Systems, Applications, & Data

✓ Process controls - risk assessments

- Attributes of risk
- Risk response workflow
- Risk analysis
- Evaluating security controls
- Risk assessment success criteria
- Managing risk
- Using the results of the risk assessment

✓ Process controls - vulnerability management

- Vulnerability management
- Vulnerability scans
- Vulnerability assessment
- Remediation
- Reporting & metrics

✓ Process controls - penetration testing

- Penetration testers
- Penetration testing phases

✓ Network security

- Network management
- LAN/WAN security
- Network risks
- Wireless local area networks
- Wired equivalent privacy & Wi-Fi protected access (WPA/WPA2)
- Ports & protocols

- Port numbers
- Protocol numbers & assignment services
- Virtual private networks
- Remote access

✓ Operating system security

- System/platform hardening
- Modes of operations
- File system permissions
- Credentials & privileges
- Command line knowledge
- Logging & system monitoring
- Virtualization
- Specialized systems

✓ Application security

- System development life cycle (SDLC)
- Security within SDLC
- Design requirements
- Testing
- Review process
- Separation of development, testing, & production environments
- OWASP top ten
- Wireless application protocol (WAP)

✓ Data security

- Data classification
- Data owners
- Data classification requirements
- Database security

Incident Response

✓ Event vs. incident

- Events vs. incident
- Types of incidents

✓ Security incident response

- What is incident response?

- Why do we need incident response?
- Elements of an incident response plan
- Security event management

✓ Investigations, legal holds, & preservation

- Investigations
- Evidence preservation
- Legal requirements

✓ Forensics

- Data protection
- Data acquisition
- Imaging
- Extraction
- Interrogation
- Ingestion/normalization
- Reporting
- Network traffic analysis
- Log file analysis
- Time lines
- Anti-forensics

✓ Disaster recovery & business continuity plans

- What is a disaster?
- Business continuity & disaster recovery
- Business impact analysis
- Recovery time objectives (RTO)
- Recover point objective (RPO)
- IS business continuity planning o Recovery concepts
- Backup procedures

Security Implications & Adoption of Evolving Technology

✓ Current threat landscape/environment

✓ Advanced persistent threats (APTs)

- Evolution of the threat landscape o Defining APTs
- APT characteristics
- APT targets

- Stages of an APT attack

✓ Mobile technology - vulnerabilities, threats, & risk

- Physical risk
- Organizational risk
- Technical risk
- Activity monitoring & data retrieval
- Unauthorized network connectivity
- Web view/user interface (UI) impersonation
- Sensitive data leakage
- Unsafe sensitive data storage
- Unsafe sensitive data transmission
- Drive-by vulnerabilities

✓ Consumerization of IT & mobile devices

- Consumerization of IT
- BYOD

✓ Cloud & digital collaboration

- Risk of cloud computing
- Web application risk
- Benefits of cloud computing

TARGET PARTICIPANTS

ICT Security Managers/Officers, ICT managers, Systems administrators, system analysts, chief information officers, systems engineers, Network engineers, database administrators and Information Technology Officers, ICT Project managers, ICT engineers, Any other Person interested in **Cyber security.**

The fee for the Course is **TZS 1,500,000/=** (One million five hundred thousand only) to cover for course materials, tea/coffee, and lunch. It does not include accommodation and transport cost. Payment may be in cash, cheque or TISS paid directly to our Bank Account No. 014103007130 in the name of Institute of Accountancy Arusha, NBC, Arusha Branch.

DATES & VENUE

Monday, 21st October, 2019 – 25th, 2019 in **Arusha** at the **Institute of Accountancy Arusha** – **Arusha Main Campus.**

CONTACT

Course Director: Mr. Sifael Sabaya (Senior System Analyst and Lecturer) ssabaya@iaa.ac.tz /Sifaeli.sabaya@gmail .com; 0754 417359

Head of Department –Consultancy & Executive Development

Pamela Chogo E-mails: pchogo@iaa.ac.tz and pamsekela@gmail.com

Cell phone: +255 655 611 512 and +255 759 334 659

Course Administrator/Secretary Ms. Caroline Lucumay

E-Mail: clucumay@iaa.ac.tz and lucumayc@gmail.com

Cell phone: +255 782 993 077 and +255 652 379 888

APPLY TO: The Rector Institute of Accountancy Arusha

P.O. BOX 2798

Arusha.

Yours Faithfully,

THE INSTITUTE OF ACCOUNTANCY ARUSHA

Sifael Sabaya

FOR RECTOR