INTERGRATED INTERNAL AUDITOR: SUITE OF COURSES

Auditing Cyber Security and Information Security using NIST and ISO 27002 (ACSIS)

DAY/S: 3 | CPD:24 | LEVEL: 1,2

INFORMATION SYSTEMS

COURSE OBJECTIVE

This course is designed for internal auditors involved in IT audits or those involved in audit activities that require an understanding of how to manage the impact of cybersecurity events on business risks. The objective is to provide auditors the ability to examine preventive, detective and corrective controls and how to apply the audit process to a cloud environment. Attendees will be exposed to the mobile environment and cyber standards, as well as learn how to audit common security solutions. The course will cover the following topics and concepts from an audit perspective:

- Hacking and Cyber warfare
- Internet Security
- Personal data security and encryption
- Wireless Security and mobile security
- Digital Certificates/Identities
- Digital forensic and investigations
- Computer Security Incident Response Teams (CSIRTs)
- Legal Framework (South Africa)
- Cyber Security Governance

COURSE OUTCOME

- Define cybersecurity from an audit perspective, including an understanding of its scope, limitations and how to measure effectiveness
- Understand how to assess an organization's cyber capabilities from an attacker perspective using threat modelling
- Identify the purpose of preventive, detective and corrective controls
- Understand cyber liability insurance and its impact on cybersecurity
- Understand cyber standards, state notification laws and how they affect an organization
- Assess cybersecurity risks and controls related to using cloud providers or third-party vendors

WHO SHOULD ATTEND?

Those who need to understand and wish to undertake security audits.