The Institute of Internal Auditors Tanzania

Practical Workshop On:

Intermediate IT Auditing & Essentials for AI Auditing

23 - 27 February 2026 Cate Hotel Morogoro

40 CPE

In today's rapidly evolving business landscape, the integration of artificial intelligence (AI) technologies is becoming increasingly prevalent. Organizations of all types are becoming more vulnerable to cyber threats due to their increasing reliance on computers, networks, programs and applications, social media, and data. A data breach can be disastrous, precipitating complex legal obligations, costly remediation, and long-lasting reputational damage.

Internal auditors play a pivotal role in ensuring effectiveness, safety, privacy, security and ability to recover should an event occur within organizations.

This course examines the connection between cybersecurity and network security, the pros and cons of technology, knowledge and skills necessary to navigate the complexities of AI, contribute effectively to their organization's and demonstrates how to apply the audit process to key areas.

Learning Objectives

- Define cybersecurity from an internal audit perspective.
- Understand the fundamentals of AI, including most commonly used artificial intelligence (AI) model types, tools and applications
- Identify risks associated with building AI systems responsibly, including safety, data integrity, privacy, security, and the 'black box' nature of AI algorithms
- Express how to assess an organization's cyber capabilities from an attacker perspective using threat modeling.
- Analyze applicable controls and considerations associated with social media and digital presence.
- Understand the risks and controls associated with identity access management, zero trust, and micro-segmentation.
- Examine the common practices for providing comprehensive assurance over operational and technological resilience programs.
- Consider regulatory compliance and standards associated with the use of AI
- Identify controls to mitigate AI risks, including Generative AI (Gen AI)

AGENDA AT A GLANCE

DAY 1

- Network and Cybersecurity Overview.
  Exploring connections between network and cybersecurity.
  Understanding the breach, including.

  Assessing a breach:
  - Attack view.
  - Detective view.
  - Corrective view.

- Applying Risk Management Techniques to Assess Technology.
  Applying risk management techniques.
  Mitigation through insurance.
  Cybersecurity and breach notification laws.

- Insider Threats.
  Recognizing the characteristics and warning signs related to insider threats.
  Describing common risks related to insider threats.
  Describing common controls to protect against insider threats.
  Identifying how to provide assurance of an insider threat program to the board of directors.

DAY 2

- Auditing Operational Resiliency in Technology.
  Operational Resiliency Overview.
  Governance and Ownership.
  Operational and Technological Resiliency for Business Services.

- Vulnerability and Patch Management.
  Auditing the Vulnerability Management Program.
  Patch Management.

- Incident Management.
  Incident Management.
  Red Team, Blue Team, Purple Team Testing.

- Auditing Identity Access Management, Zero Trust, and Micro-Segmentation.
  Overview of Identity Access Management, Zero Trust, and Micro-Segmentation.
  Related Risk and Control Groups.
  Risk Assessment Concerns for Internal Audit.
  Frameworks and Controls for Assurance.

DAY 3

- Understanding the Cloud Environment.
  Cloud Overview.
  Examining Cloud-Based Risks and Controls.
  Assessing the Cloud Environment.

- Auditing Mobile Computing and Connected Devices.
  Mobile Computing and Connected Device Essentials.
  Mobile Computing and Connected Device Risks and Controls.
  Assessing Mobile Computing and Connected Device Related Controls.

- Auditing Social Media and Digital Presence.
  Social Media and Digital Presence Overview.
  Social Media and Digital Presence Risks and Controls.
  Assessing Social Media and Digital Presence.

- Automation Center of Excellence
  How to audit the Automation Center of Excellence (CoE) and Cognitive Technologies.
  Automated Auditing Processes and Benefits.
  Automation CoE Risks.

DAY 4 & 5

- AI Overview - Understanding the fundamentals of AI and its evolution.
  Establish a solid foundation in AI technology.

- Risk Management in AI.
  Risk Identification and Management - Identifying and managing AI model risks
  ,and model use risks, such as safety, integrity, privacy, security.
  Understanding the unique risks posed by the ‘black box’ nature of AI systems.

- Internal Audit's Role in AI Strategy.
  AI Strategic Management - Exploring how organizations plan and execute AI strategies, and oversight required.
  Governance in AI - Understanding structures and processes for AI governance.
  Role of internal audit - Discussing the role of internal audit in AI governance.
  and the Three Lines Model, while leveraging internal controls in managing AI risks.
  Integrating AI risk assessment with existing annual/quarterly risk assessments.

DAY 5

- Regulatory Compliance and Standards.
  Understanding organization's policies, processes, and structures for complying with existing and upcoming regulations.
  International standards for AI auditing.

- AI Auditing Framework.
  Overview of the AI Auditing Framework - Understanding the framework and associated domains and risk categories.
  Applying the AI Auditing Framework through real-world scenarios.
  Identify potential AI-related risks, assess their significance, and develop audit plans that address these risks effectively.

- Controls for Mitigating AI Risks.
  Exploring controls to manage AI model and model usage risks, such as bias, safety, data, privacy, and security.
  Understanding controls for managing unique risks from the Gen AI models.

Who Should Attend?

Internal Auditors, Chief Audit Executives, Audit Managers, Senior Auditors, Directors of Internal Audit, External Auditors, Risk Managers, Information System Auditors and other interested parties.

Registration

Visit
www.iiatanzania.or.tz, events.iiatanzania.or.tz

or email to: info@iiatanzania.or.tz;

and for enquiry Call or WhatsApp: +255 684460777

Fees

Fees Category	Payment Before 16.02.2026	Payment After 16.02.2026
Member	**TZS 900,000**	**TZS 1,000,000**
Non-Member	**TZS 1,000,000**	**TZS 1,100,000**

Note that all participation fees are VAT 18% inclusive. Discount: All Workshop fees have been favourably discounted.

Course Fee Payment

All cheques should be payable to the
"The Institute of Internal Auditors Tanzania".

Scan to Register and Pay

Cancellation Policy:

Cancellation charge of 20% will be charged if written notification for cancellation is received by 16th February 2026. No refund shall be remitted for cancellation after 16th February 2026.

THE INSTITUTE OF INTERNAL AUDITORS TANZANIA

MASAKI PENINSULA - RUFIJI STREET, BLOCK No. 2

P.O BOX 80517, DAR ES SALAAM

TELEPHONE: +255 2137498 / FAX: +255 2126383 / CELL: +255 684 460777

EMAIL: info@iiatanzania.or.tz / WEBSITE: www.iiatanzania.or.tz

Institute of Internal Auditors Tanzania | The Institute of Internal Auditors Tanzania | IIATanzania | iiatanzania