# Cybersecurity Assurance & Incident Response

*From Requirements to Readiness, From Incidents to Resilience*

***Date:*** *3 & 4 March 2026 (two days)*
***Time****: 09:00 – 17:00*
***Location*** *– Xheko Imperial*
***Course director:*** *Komitas STEPANYAN*

## Introduction

In today's rapidly evolving threat landscape, cybersecurity is no longer just an IT concern, it is a critical governance, risk and assurance priority. Boards, regulators and stakeholders increasingly expect organizations to demonstrate robust cyber resilience, effective oversight and measurable preparedness against emerging threats.

This intensive two-day training program is designed specifically for internal auditors, risk professionals and cybersecurity officers/professionals who play a vital role in understanding the main risks and provide assurance over cybersecurity risk management. Participants will gain practical knowledge, hands on tools and the confidence to assess cybersecurity frameworks and evaluate incident response readiness in alignment with leading standards and regulatory expectations.

Through focused discussions, real world scenarios and actionable methodologies, this program bridges the gap between technical cybersecurity concepts and effective audit and risk oversight, enabling participants to deliver meaningful assurance in an increasingly complex digital environment.

## Target audience

This course is designed for professionals responsible for governance, risk, assurance and oversight of cybersecurity, including:

- **Internal Audit Practitioners:** Audit professionals who assess cybersecurity frameworks, IT governance and incident response readiness as part of their assurance activities.
- **IT Audit Professionals:** Specialists who review IT governance, security controls and cyber risk management processes from an independent assurance perspective.
- **Risk Specialists:** Professionals responsible for identifying, evaluating and monitoring cyber risks within the organization's enterprise risk management framework.
- **Compliance Officers:** Individuals tasked with ensuring alignment with regulatory expectations, cybersecurity standards, and industry requirements.

- **Assurance and Control Professionals:** Second and third-line professionals involved in evaluating the effectiveness of cybersecurity controls and resilience capabilities.
- **Cybersecurity Specialists:** Security professionals who want to strengthen their understanding of governance expectations, control assurance and how auditors and risk functions evaluate cybersecurity programs and incident response readiness.

## Detailed Training Program

### Day 1: Applying the IIA Cybersecurity Topical Requirement

*Strengthening Cybersecurity Assurance*

This day focuses on understanding and applying the **IIA Cybersecurity Topical Requirement** in real-world audit engagements.

**Participants will learn to:**

- Understand the **structure, intent and mandatory elements** of the IIA Cybersecurity Topical Requirement
- Identify governance expectations for boards and senior management
- Assess cybersecurity risk management alignment with enterprise risk management
- Evaluate key control domains *(access management, data protection, vulnerability management, third-party risk, etc.)*
- Integrate cybersecurity into audit planning and risk-based audit programs
- Develop practical audit procedures and testing approaches
- Recognize common gaps and red flags in cybersecurity oversight
- Align audit work with frameworks such as NIST Cybersecurity Framework and COBIT

The course includes case discussions and practical audit scenarios.

### Day 2: Cybersecurity Incident Response

*From Preparedness to Post-Incident Assurance*

Cyber resilience is tested during incidents. This day equips participants to evaluate and audit incident response capabilities.

**Participants will learn to:**

- Understand the lifecycle of cybersecurity incidents
- Evaluate the design and effectiveness of incident response frameworks
- Assess roles and responsibilities *(CISO, SOC, management, board)*
- Review incident detection, escalation, and communication processes
- Evaluate regulatory notification and reporting requirements
- Assess digital evidence handling and forensic readiness
- Identify weaknesses through post-incident reviews
- Audit lessons learned processes and resilience improvements
- Understand the auditor's role during and after major cyber incidents

Includes tabletop exercise and real-life incident case analysis.

## Instructor Bio

**Komitas Stepanyan** is an internationally certified professional and esteemed expert. Mr. Stepanyan is recognized by the International Monetary Fund (IMF) for his exceptional work in financial regulation and supervision, as well as IT and cybersecurity risk management and IT fraud examination. Additionally, he is a distinguished expert for The World Bank Group, specializing in digital transformation and GovTech activities.

Mr. Stepanyan is the Director of Technology and Cybersecurity Directorate at the Central Bank of ARMENIA. He has **20+ years of experience** working as an **information security professional**, **Internal Audit consultant, cybersecurity consultant**. More than 10 years he was the **Head of IT Auditing Division** at the Central Bank of Armenia, providing audit and consulting services including information and cybersecurity audits.

Working as a short-term expert for cyber risk management, regulation and supervision and IT fraud examination for **International Monetary Fund**, he conducted and led many Technical Assistance and capacity-building missions covering a diverse range of countries and topics in Africa, Asia and Pacific.

Since 2018, he has worked as a short-term consultant for **The World Bank**, supporting various jurisdictions in digital transformation projects, including cybersecurity.

Mr. Stepanyan holds several international certificates: **Certified in Risk and Information Systems Control** (*CRISC- issued by ISACA*) and **Certification in Risk Management Assurance** (*CRMA- issued by IIA*), **Cobit Foundation Certificate** (*CobitF - issued by ISACA*) and **Social Engineering and Phishing Mastery Certificate**.

In 2007, he earned his PhD in applied physics. In 2012, he graduated from the “Public Policy and Public Administration” Certificate Program at Tufts University (USA). In 2016, he completed the online course "Digital Money" and in 2017 “Operationalizing Mobile Money” from the Digital Frontiers Institute in partnership with The Fletcher School, Tufts University.

**IMPORTANT FINANCIAL DATA**

Cost per participant: **AIIA Members ALL 29,000** *(total amount, the subject is VAT excluded)*

**Non-members ALL 34,000** *(total amount, the subject is VAT excluded)*

Price includes course attendance and educational material.
Payment* can be made by bank transfer or direct deposit by using the following account info: Account Holder**: Albanian Institute of Internal Auditors** Acc.no**: 0000039700**

Swift: **SGSBALTX** IBAN: **AL93 2021 1044 0000 0000 0003 9700**

**Raiffeisen Bank Albania**

** Important: The transferred amount **must include** the entire amount as stated above. No shortfalls due to exchange fee/or other administration charges may arise. Albanian Institute of Internal Auditors has to receive the amount that is stated in your invoice.*

**REGISTRATION**
**FORM**

# Cybersecurity Assurance & Incident Response

*From Requirements to Readiness; From Incidents to Resilience*

3 & 4 March 2026

| | | | |
|---|---|---|---|
| Full name | | | |
| Position | | | |
| Company name | | VAT No. | |
| Contact Tel. | | Email | |
| Address | | | |

**Cancellation Policy:**

Places on AIIA Training courses are limited so we therefore operate a cancellation policy regarding refund.

1. *In case of cancellation of a training event by AIIA or related partner, we will endeavour to inform all participants 10 days before the course is due to take place, although please be aware that this is not always possible. All course fees paid will be reimbursed in full, but we are unable to reimburse any other costs that may have been incurred, including flights, accommodation etc.*
2. *No refund will be made for:*
   a. *Bookings cancelled less than two weeks before the event, except in exceptional circumstances and then only at the discretion of Albanian Institute of Internal Auditors.*
   b. *Non-attendance on the course.*
3. *For bookings cancelled two or more weeks before a course is due to start, 100% per cent of course fees paid will be refunded to the applicant.*

• I confirm all the data I provided is true and accurate.
• I confirm that I read the training program and I agree to have such content delivered during the course.

Name Surname Signature _____

Date, location _____