Institute of Internal Auditors Malaysia

2026 INTERMEDIATE IT AUDITING

(Developed By Global IIA)

IIAM GLOBAL SERIES

PROGRAM OVERVIEW

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 – whether caused by external bad actors or a trusted insider – can be disastrous, precipitating complex legal obligations, costly remediation, and long-lasting reputational damage. Cyberattacks and accidental misconfigurations are top concerns among boards, executive management, and other organizational stakeholders. Internal auditors are expected to assess an organization's defenses and its ability to recover should an event occur.

Are you up to the challenge?
This course examines various technology concepts that can be used to facilitate integrated auditing efforts within an organization, including:

- Applying Risk Management Techniques to Assess Technology
- Insider Threats
- Auditing Operational Resiliency in Technology and Beyond
- Vulnerability and Patch Management
- Incident Management
- Identity Access Management, Zero Trust, and Micro-segmentation for Auditors
- Auditing the Cloud
- Auditing Mobile Computing and Connected Devices
- Auditing Social Media and Digital Presence
- Auditing the Automation Center of Excellence (CoE)

Participants of this course will examine the connection between cybersecurity and network security, obtaining greater insight into the pros and cons of technology insurance and exploring how to apply the audit process to key areas, including operational resilience, identity access management, cloud computing, mobile computing, cloud environments, and social media. Finally, the course explores common cyber-related frameworks, standards, and guidelines, and explains how to audit common cybersecurity solutions.

IIA MALAYSIA CPD POINTS 16

CLAIMABLE UNDER THE SBL KHAS SCHEME HRDC

ADMINISTRATIVE DETAILS

TARGET AUDIENCE	**LEVEL II-IV**
MEMBER'S FEE	**RM2,916.00** All Fees is inclusive of 8% SST
NON-MEMBER'S FEE	**RM3,348.00** All Fees is inclusive of 8% SST. *EARLY BIRD FEE 10% discount for registration received one (1) month prior to respective workshop dates*
DATE	**10 & 11 August 2026**
TIME	**9:00 am – 5:00 pm** (Registration will be on Day 1 at 8.30 am)
DELIVERY MODE	**Physical Class**
LOCATION	**Kuala Lumpur**
PROGRAMME CODE	**2026/KL69**
TRAINER	**Divakaren Sivagurunathan**
CPD POINTS	**16**

Disclaimer
This course has been planned as a classroom training session. In the event that the training session is converted to virtual format, a rebate of RM300 will be given for each participant. T&C apply.

Institute of Internal Auditors Malaysia

IIAM GLOBAL SERIES

WHO WILL BENEFIT FROM THIS COURSE?

This course is intended to enhance your understanding of cybersecurity concepts- including common frameworks, standards and guidelines - to apply the audit process to emerging threats to associated with social media, mobile computing, cloud environments and more.

This course is designed for internal auditors with a basic understanding of IT and cybersecurity concepts or who have been involved in integrated audits. This course will also benefit those internal auditors who have been involved in internal audit activities that require an understanding of how to manage the impact of cybersecurity events on organizational risks.

COURSE OBJECTIVES

- Define cybersecurity from an internal audit perspective.
- Explore the business process – cybersecurity connection and the importance of classifying and assessing controls.
- Explain cyber liability insurance and its impact on cybersecurity.
- Describe cyber standards, state notification laws, and how they affect an organization.
- Express how to assess an organization's cyber capabilities from an attacker perspective, using threat modeling.
- Evaluate applicable controls and considerations associated with mobile computing and connected devices.
- Analyze applicable controls and considerations associated with social media and digital presence.
- Explain how to assess a cloud environment taking into consideration the organization's liabilities when utilizing cloud solutions.
- Examine how to audit the automation CoE and assurance within established organizational risk appetite.
- 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.

OUTLINE

Unit 1: Network and Cybersecurity Overview

- Exploring Connections between Network and Cybersecurity, including:
  - Cybersecurity connection to network security.
  - Cybersecurity triad.
  - Connection to the OSI Model.
  - Defense in depth and layered security.
  - Boundary controls.
- Understanding the Breach, including:
  - Assessing a breach.
    - Attack view.
    - Detective view.
    - Corrective view.

Unit 2: Applying Risk Management Techniques to Assess Technology

- Applying risk management techniques including:
  - Considerations for mitigating breach-related costs and risks.
- Mitigation through insurance.
  - Common characteristics of cyber liability insurance and why it is important.
- Cybersecurity and breach notification laws.
  - Impact of federal notification regulations (SEC Cybersecurity Law).
  - Current U.S. and international notification laws affecting security incident management.

Unit 3: Insider Threats

- Recognize the characteristics and warning signs related to insider threats.
- Describe common risks related to insider threats.
- Describe common controls to protect against insider threats.
- Articulate the necessary components of an insider threat program.
- Identify the key activities to include an insider threat audit.
- Identify how to provide assurance of an insider threat program to the board of directors.

Institute of Internal Auditors Malaysia

IIAM GLOBAL SERIES

Unit 4: Auditing Operational Resiliency in Technology

- Operational Resiliency Overview, including:
  - Prioritizing critical technologies and operations impacting customers, markets, and other stakeholders if disrupted.
  - Identifying measures needed to ensure the business remains operational.
  - Operational resiliency essential terminology.
- Governance & Ownership, including:
  - Establishing internal control networks.
  - Ownership, roles, responsibilities, and reporting lines.
  - Third party considerations.
  - Other risk and control groups.
- Operational and Technological Resiliency Controls for Business Services, including:
  - Establishing lines of defense.
  - Scheduling regular audits, testing, and continuous improvement.
  - Designing processes to ensure incremental change in response to disruption.
  - Understanding and mapping business services inventory to technology assets, processes, and owners.
  - Identifying impact and risk tolerances.

Unit 5: Vulnerability and Patch Management

- Auditing the Vulnerability Management Program, including:
  - Vulnerability management program overview.
  - Understand common vulnerability management maturity models used to assess organizational cybersecurity vulnerabilities.
  - Review key metrics for auditing the vulnerability program.
  - How to implement appropriate actions when auditing vulnerabilities.
- Patch Management, including:
  - Key concepts of patch management.
  - Patch management program.
  - Patch management metrics.
  - Patch management controls.
  - Patch management and MSP risks.
  - How the patch management program reduces cybersecurity risk and organizational vulnerabilities.
  - How the patch management program reduces data breach risk and loss.
  - Auditing the patch management program.

Unit 6: Incident Management

- Incident Management, including:
  - Incident and incident management overview.
  - Common incident management activities.
  - Incident preparation plans and playbooks.
  - Incident response.
  - Post incident.
- Red Team, Blue Team, Purple Team Testing, including:
  - Introduction to Red, Blue, and Purple Teams. Understanding the "cyber kill chain."
  - Common cyberattack methods.
  - Vulnerabilities related to people, processes, and technologies.
  - Improving incident response.
  - Red Team activities.
  - Auditing the exercise.

Unit 7: Auditing Identity Access Management, Zero Trust, and Micro-Segmentation

- Overview of Identity Access Management, Zero Trust, and Micro-Segmentation, including:
  - Identity access management components.
  - Zero trust and micro-segmentation components.
  - Protection, privacy, and resilience overview.
- Related Risk and Control Groups, including:
  - Risk management.
  - Event logging.
  - Log monitoring.
  - Other risk and control groups.
- Risk Assessment Concerns for Internal Audit, including:
  - Determining who has access to the organization's most valuable information.
  - Understanding which systems would cause the most significant organizational disruption if compromised.
  - Analyzing which organizational data would cause financial or competitive loss, legal ramifications, or reputational damage to the organization if exposed.
  - Assessing if management is prepared to react timely in the event of a cybersecurity incident.
- Frameworks and Controls for Assurance, including:
  - Understand internal audit's role related to identity access management and zero trust assurance, governance, risk, and cyber threats.
  - Identify assurance gaps, implementation frameworks, and controls.
  - Reporting responsibilities of the internal audit function.

Institute of Internal Auditors Malaysia

IIAM GLOBAL SERIES

Unit 8: Understanding the Cloud Environment

- Cloud Overview, including:
  - The cloud, what it is, and how it works.
  - Common cloud standards and guidelines.
  - Cloud models and deployments.
  - Cloud provider selection criteria.
  - Connectivity between the cloud provider and the client site.
- Examining Cloud-Based Risks and Controls, including:
  - Cloud governance and strategy.
  - Cloud-based asset and configuration management.
  - Risks related to cloud providers and conducting cloud-based risk assessments.
  - Cybersecurity threats associated with cloud utilization.
  - Key cloud contract considerations.
  - Annual assessment/service organization control (SOC) reports.
- Assessing the Cloud Environment, including:
  - Assessing cloud tools.
  - Assessing the cloud provider contract.
  - Assessing cloud controls at the cloud vendor and client sites.

Unit 9: Auditing Mobile Computing and Connected Devices

- Mobile Computing and Connected Device Essentials, including:
  - Mobile computing characteristics.
    - Enterprise mobility management solutions.
    - Mobile apps.
  - Connected device characteristics.
    - Smart home/office.
    - E readers, tablets, phablets.
    - Mobile phones, smart watches, and other wearables.
- Mobile Computing and Connected Device Risks and Controls, including:
  - Compliance risks.
  - Privacy risks.
  - Security risks.
  - Mobile computing and connected device controls (home office vs. organizational headquarters).
- Assessing Mobile Computing and Connected Device Related Controls, including:
  - Connected device risk and control matrix.
  - Planning the internal audit.
  - Data collection and analytics opportunities.
  - Testing connected devices (home office vs. organizational headquarters).
  - Reporting on effectiveness of connected device security.

Unit 10: Auditing Social Media and Digital Presence

- Social Media and Digital Presence Overview, including:
  - Social media strategies and objectives of the organization.
  - Digital presence strategies and objectives to the organization.
  - Digital presence governance.
- Social Media and Digital Presence Risks and Controls, including:
  - Compliance risks.
  - Privacy risks.
  - Security risks.
  - Social Media site vulnerabilities (e.g., site security, impersonation, public posting, employee access).
  - Social media and digital presence controls.
- Assessing Social Media and Digital Presence, including:
  - Assessing digital presence controls.
  - Assessing social media controls.
  - Evaluation and interpretation of social media contracts.

Unit 11: Automation Center of Excellence

- How to Audit the Automation Center of Excellence (CoE) and Cognitive Technologies, including:
  - Common terminology.
  - Automation risk frameworks and CoE mandates.
  - Governance and oversight.
  - Planning and alignment.
  - Return on automation CoE investment.
  - Policies and procedures.
  - Development standards.
  - Controls.
- Automated Auditing Processes and Benefits, including:
  - Business processes.
  - System access control testing.
  - Internal audit processes.
  - Sarbanes-Oxley (SOX) testing.
  - Database control testing.
  - Compliance testing.
- Automation CoE Risks, including:
  - Account management and separation of duties in the bot development lifecycle.
  - Operational risk stemming from confusion around ownership of automation.
  - Additional artificial intelligence (AI) risks.

Institute of Internal Auditors Malaysia

IIAM GLOBAL SERIES

ABOUT THE TRAINER

DIVAKAREN SIVAGURUNATHAN
MBA, CISA, Cybersecurity Audit Certificate

Divakaren Sivagurunathan is currently heading the audit function of a telco, performing both IT and non-IT audits. He also serves as the secretary of the Board Audit Committee for the telco and provides consultation on IT assurance within the larger Group. He has 16 years of IT auditing experience covering all aspects of application and infrastructure auditing.

Prior to this, he was in various senior auditor roles within the oil and gas industry, providing assurance for both IT and non-IT systems, covering all aspects of applications and infrastructure, including servers, networking, and plant industrial control systems.

On top of his Master of Business Administration (MBA), Diva is also a Certified Information Systems Auditor (CISA) and obtained his Certificate in Cybersecurity Auditing. He is also serving on the Board of Directors on the Information System Audit & Control Association (ISACA) Malaysia's chapter.

Institute of Internal Auditors Malaysia

REGISTRATION FORM

Are you claiming under HRDC SBL Khas?

☐ Yes ☐ No

COURSE DETAILS

Course Title 2026 Intermediate IT Auditing

Course Code 2026/KL69 Course Date(s) 10 & 11 August 2026

DELEGATE 1

Full Name (as per IC) _____

Designation _____

NRIC _____ Gender ☐ Male ☐ Female Race _____

Mobile No. _____ Email Address _____

☐ Member ☐ Non-Member Membership No. (only applicable for members) _____

Dietery Preferences ☐ Vegetarian ☐ Non-Vegetarian

DELEGATE 2

Full Name (as per IC) _____

Designation _____

NRIC _____ Gender ☐ Male ☐ Female Race _____

Mobile No. _____ Email Address _____

☐ Member ☐ Non-Member Membership No. (only applicable for members) _____

Dietery Preferences ☐ Vegetarian ☐ Non-Vegetarian

If you are sending more than 2 delegates, kindly send the delegates details in an Excel File format.

CORPORATE DETAILS (only applicable for corporations)

☐ Corporate Member Corporate Membership No: _____

☐ Corporate Non-Member

CONTACT DETAILS

Organisation Name _____ Company Registration No. _____

Mailing Address _____

Contact Person _____ Designation _____

Telephone _____

Fax _____ Email Address _____

BILLING DETAILS

☐ please tick if billing details are the same as contact details.

Contact Person _____ Designation _____

Billing Address _____

Telephone _____ Fax _____

Email Address _____

For non-member, would you like to be contacted to know more about IIA Membership programme? ☐ Yes ☐ No

ENQUIRY & REGISTRATION
1-17-07, Menara Bangkok Bank, Berjaya Central Park, 105 Jalan Ampang, 50450, Kuala Lumpur, Malaysia
Tel: +603 2181 8008 ext 210/211/212/213 Fax: +603 2181 1717 Email: training@iiam.com.my Website: www.iiam.com.my
Follow and like us on - IIA Malaysia - IIA Malaysia - IIA Malaysia - IIA Malaysia

REGISTRATION FORM

Institute of Internal Auditors Malaysia

PAYMENT DETAILS

Payment Details	Member Rate (per person) for KL-code related courses	Non-Member (per person)	8% SST	Total with SST
Fee (per pax) RM				
No. of pax				
Subtotal				

All registrations **MUST** be accompanied with full payment. Upon receipt of your registration, you are deemed to have read and understood the registration procedures and accepted the terms and conditions contained therein. (Please tick (✓) the chosen method)

☐ Enclosed is a cheque/bank draft no. _____ for the sum of RM _____ payable to **THE INSTITUTE OF INTERNAL AUDITORS MALAYSIA**

☐ **LOCAL PAYMENTS BY CHEQUE / INTERBANK GIRO**
All payments should be crossed and made payable to **THE INSTITUTE OF INTERNAL AUDITORS MALAYSIA**
Bank Details: United Overseas Bank (M) Bhd. USJ Taipan Branch, No.7, Jalan USJ 10-1, USJ Taipan Triangle, 47620 UEP Subang Jaya, Selangor
Account No.: 165-301-514-9 Bank Swift Code: UOVBMYKL

☐ **OVERSEAS PAYMENTS BY WIRE TRANSFER (USD only)**
Beneficiary: **THE INSTITUTE OF INTERNAL AUDITORS MALAYSIA**
Address: 1-17-07, Menara Bangkok Bank, Berjaya Central Park, 105 Jalan Ampang, 50450 Kuala Lumpur, Malaysia
Beneficiary's Bank: STANDARD CHARTERED BANK MALAYSIA BERHAD
Beneficiary's Bank Address: Level 18, Menara Standard Chartered, No.30 Jalan Sultan Ismail, 50250 Kuala Lumpur
Account No.: 312-170-024-235 Bank Swift Code: SCBLM-YK-XXXX

All wire transfer payments should include USD$30.00 (overseas) and RM25.00 (local) for wire transfer processing fee. For GIRO, please include RM1.00 as bank charges.
(Please fax the bank-in slip to +603 2181 1717 or email to training@iiam.com.my)

☐ **CREDIT CARD**
I hereby authorise **THE INSTITUTE OF INTERNAL AUDITORS MALAYSIA** to charge to my credit card. to the value of

RM _____ Card Type: ☐ VISA ☐ MASTER

Card Number: ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐

Expiry Date: _____ Cardholder's Name _____

I understand that any amount drawn from my credit card will first be cleared with the credit card authorisation facility.

Signature (As per credit card) _____ Date _____

TERMS & CONDITIONS

FEE

- Fee is payable to "THE INSTITUTE OF INTERNAL AUDITORS MALAYSIA". Please state your name, payment advice number, phone number and Workshop Code number at the back of the cheque/bank-in slip. Admittance will only be permitted upon receipt of full payment
- The fee covers a copy of course material*, lunches, refreshment, and Certificate of Attendance.
- Full payment is to be made before the date of the course. Fee is inclusive of 8% SST.
- Walk-in delegates will only be allowed if full payment is made, subject to the availability of the seat.
- This course has been planned as a classroom training session. In the event that the training session is converted to virtual format, a rebate of RM300 will be given for each participant. T&C apply.

HUMAN RESOURCE DEVELOPMENT CORPORATION (HRDC) SBL KHAS CLAIM(S) [APPLICABLE TO HRDC SBL KHAS CLAIMABLE COURSE(S) ONLY]

- Claimants are fully responsible:
  - To provide IIA Malaysia with the HRDC grant approval notification (letter or email) minimum 7 working days before the commencement of the course(s).
  - To provide IIA Malaysia with Letter of Undertaking (LOU) for full settlement of the course fees if grant approval notification is received from HRDC prior to the commencement of the course(s).
  - To adhere to all terms and conditions set by HRDC (i.e., full attendance of the courses).
  - For timely completion and submission of all required HRDC documents as per their requirement.
  - To follow up and respond to any queries from HRDC and attain the approval of grant claim(s) within 60 days from the completion of the course(s). If no grant claim approval is attained within 60 days, claimants are responsible to arrange for an immediate full settlement of the course fee(s). Should a late approval is attained post the full settlement, IIA Malaysia will arrange for the reimbursement accordingly based on the approved grant claim.
  - The HRDC Grant Approval Amount falls within the purview of HRDC. IIA Malaysia is obligated to adhere to the HRDC procedure and permissible cost matrix. In the event that the approved amount is less than the total training cost, the participant or attending corporate entity is required to cover the remaining balance.

CANCELLATION

- Upon registering, participant(s) are considered successfully enrolled in the course. Should participant(s) decide to cancel/transfer their registration, a cancellation/ transfer policy shall be applied as follows.
  a) Written cancellations should be received by 14 working days before the workshop date to get the refund.
  b) Written cancellations should be received by 7 working days before the workshop date to get a partial refund after deduction of 50% administrative charge. Unpaid registrations will also be liable for 50% administrative charge.
  c) Written cancellations/no-show on the day of the workshop.
     - No refund will be entertained.
     - Unpaid registrations will also be liable to full payment of the registrations fee. Partial cancellation is not allowed.
  d) You can substitute an alternate delegate(s) if you wish to avoid cancellation charges. Any differences in fees will be charged accordingly.

RESERVATION

- The Institute reserves the right to make changes to the venue, date, topic, speaker including cancellation if warranted by circumstances beyond its control.
- The Institute reserves the right to utilize any recordings or photographs taken during the delivery of the course(s) for marketing and advertising purposes.
- The Institute is not responsible for the action, advise or representations of the trainer / speaker.
- Registration will be on first-come, first-serve basis.
- Certificates of Attendance will be issued an "E-certificate" via email. For this purpose, it is COMPULSORY to fill in the email address clearly. Certificate will only be given to participant who attended the session in full.
- Upon signing this form, you have deemed to have read and understand the registration term and condition and therefore have accepted the terms contained herein.

DATA PROTECTION

Personal Data is gathered in accordance with the Personal Data Protection Act 2010 (Act 709). The Institute of Internal Auditors Malaysia (IIA Malaysia) hereby inform you that your personal data will be processed, retained and used by IIA Malaysia in relation to this Workshop. Your personal data may also be retained and used by IIA Malaysia to market and promote other training programmes conducted by IIA Malaysia.

DISCLAIMER

The Institute of Internal Auditors Malaysia (IIA Malaysia) reserves the right to change the speaker(s), date(s) or to cancel workshop(s) should circumstances beyond its control arise. IIA Malaysia also reserves the right to make alternative arrangements without prior notice should it be necessary to do so. IIA Malaysia is not responsible for any incidental cost of participants (i.e. return flights, accommodation and etc) due to changes or cancellation of course(s). Upon submitting the registration form, you are deemed to have read and accepted the terms and conditions.

** Subject to approval of the proprietor.*

ENQUIRY & REGISTRATION
1-17-07, Menara Bangkok Bank, Berjaya Central Park, 105 Jalan Ampang, 50450, Kuala Lumpur, Malaysia
Tel: +603 2181 8008 ext 210/211/212/213 Fax: +603 2181 1717 Email: training@iiam.com.my Website: www.iiam.com.my
Follow and like us on - IIA Malaysia - IIA Malaysia - IIA Malaysia - IIA Malaysia

HRDC CLAIMABLE UNDER THE SBL KHAS SCHEME

IIA MALAYSIA CPD POINTS 16