

Institute of Internal Auditors Malaysia

2026 FUNDAMENTALS OF CYBERSECURITY AUDITING

(Developed By Global IIA)

IIAM GLOBAL SERIES

IIA MALAYSIA CPD POINTS 16

CLAIMABLE UNDER THE SBL KHAS SCHEME HRDC

ADMINISTRATIVE DETAILS

TARGET AUDIENCE	**LEVEL I-II**
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	**16 & 17 December 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/KL76**
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.

PROGRAM OVERVIEW

With innovations including automation, cloud, and mobile computing, not to mention customer preferences moving toward self-service from any device throughout the world, having a basic understanding of cybersecurity is crucial for today's operational auditor. It is no surprise that cybercrime is growing at an alarming rate and the cost of a breach affects an organization from regulatory, financial, and reputational perspectives.

This introductory course is a good place to start. Fused with critical thinking strategies, this program introduces cybersecurity threats, vulnerabilities, and common controls. During this program, you will develop an understanding of cybersecurity concepts that can be used to facilitate integrated audit efforts within your organization.

WHO WILL BENEFIT FROM THIS COURSE?

This course intends to provide a comprehensive overview of key cybersecurity concepts, along with practical applications, that can be used to facilitate audit efforts within your organization. This course is designed for internal auditors who are looking for a fundamental understanding of cybersecurity and common exploits. It is recommended for internal auditors that are involved in operational audit activities and need to know how to assess the strength of controls that influence the impact of cybersecurity events on organizational risks.

Institute of Internal Auditors Malaysia

IIAM GLOBAL SERIES

COURSE OBJECTIVES

- Define cybersecurity from an internal audit perspective.
- Describe the scope, purpose, and limitations of cybersecurity.
- Recognize how to measure effectiveness within the cybersecurity program.
- Express the importance of information security governance with the cybersecurity program.
- Examine the importance of cybersecurity and vendor risk assessments.
- Explore basic auditing considerations for cybersecurity-related compliance.
- Recognize typical cybersecurity-related preventive, directive, detective, mitigating, redundant, compensating, and corrective controls.
- Identify simple internal audit activities to assess cyber resiliency within existing operational audit programs.

OUTLINE

Overview of Cybersecurity

- An overview of cybersecurity, including its history and impact on organizations.
- The breach process, and the motivations and tactics of a bad actor.
- Control types to protect against or minimize cyberattacks.
- An overview of defense in depth, layered security, and the Open System Interconnection (OSI) model.

Information Security – Governance, Risk, and Control

- An overview of cybersecurity governance and the associated standards.
- An overview of cybersecurity risk management and the associated standards.
- The development of a cybersecurity risk management program, including the utilization of cybersecurity risk management frameworks and cybersecurity maturity models.
- Cybersecurity control areas and program development.
- Assurance on cybersecurity governance, risk, and controls, and auditing cybersecurity.

Control Primer

- The characteristics of the various controls – by function – that should be present in an organization's internal control environment to achieve and maintain a robust cybersecurity program, including:
  - Control design and maintenance.
  - Types of controls.
  - Control levels.
  - Control classifications.
  - Controls by function.
  - Asset and control inventory.
  - Controls and the Standards.

Directive Controls

- An overview of directive controls and their importance in cybersecurity.
- An exploration of common threats to directive controls.
- Utilizing cybersecurity frameworks, standards, and guidelines to establish directive controls.
- The importance of cybersecurity training as a directive control.
- Building directive controls to support incentive programs.

Preventive Controls

- An overview of preventive controls and their importance in cybersecurity.
- An exploration of the use of preventive controls regarding the anatomy of a breach, including:
  - Infiltration.
  - Propagation.
  - Aggregation.
  - Exfiltration.
- An introduction to techniques for monitoring and reporting.

Detective Controls

- An overview of detective controls and their importance in cybersecurity.
- The cybersecurity triad (CIA Triad).
- Detective controls for detecting cyber incidents.
- The Security Operations Center (SOC) in response to a cybersecurity breach.
- Containing any breaches in security and determining resulting data exposure and exfiltration.
- Audit logging and security information and event management (SIEM) for continuous monitoring.
- Considerations for auditing detective controls.
- Data classification, ownership, and detective controls.

Institute of Internal Auditors Malaysia

IIAM GLOBAL SERIES

OUTLINE

Corrective Controls

- An overview of corrective controls and their importance in cybersecurity.
- An exploration of common types of corrective controls:
  - Backup and restoration.
  - Business continuity.
  - Disaster recovery.
  - Incident response.
- Potential threats to the functionality of the common types of corrective controls.
- Essential auditing concepts for assessing cybersecurity corrective controls.

Mitigating Controls

- An overview of mitigating controls and their importance in cybersecurity.
- Potential threats to the functionality of the common types of mitigating controls.
- The cybersecurity risk management process and mitigating controls.
- An exploration of common types of mitigating controls.
- Essential auditing approaches for assessing cybersecurity-related mitigating controls.

Compensating and Redundant Controls

- An overview of compensating and redundant controls and their importance in cybersecurity.
- An exploration of common types of compensating and redundant controls.
- Potential threats to the functionality of the common types of compensating and redundant controls.
- Audit approaches for assessing cybersecurity-related compensating and redundant controls.

Assessing Cybersecurity in Operational Audit Programs

- An overview of the Global Internal Audit Standards related to work programs that account for cyber-related risks.
- An overview of GTAGs and Practice Guides related to work programs that account for cyber-related risks.
- An overview of industry-recognized cybersecurity and cloud control frameworks.
- Suggestions for enhancing operational audit programs with cyber-related audit activities.

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 Fundamentals of Cybersecurity Auditing

Course Code 2026/KL76 Course Date(s) 16 & 17 December 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**

☐ HRD CORP CLAIMABLE - Programme No.

☐ E-PEROLEHAN or INTERNAL PROCUREMENT SYSTEM (Both MYR & USD accepted)

☐ **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

☐ **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:
  - Claimants are advised to **APPLY** for HRDC Grant Approval at least three (3) weeks (21 days) prior to the commencement of the course(s).
  - It is **COMPULSORY** to provide IIA Malaysia with the HRDC grant approval notification (letter or email) 7 working days before 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