



The Institute of
Internal Auditors
Malaysia



2023/WEB09 AUDITING CYBERSECURITY

OVERVIEW

Cybersecurity is one of the biggest risks facing today's organisations. Recent cybersecurity attacks indicate more threatening ones ahead as evidenced by numerous disruptive breaches that often require affected organisations to pay hundreds of millions of US dollars to cover costs of the attacks.

While these enterprises share similar misfortune of experiencing incidents, the incidents themselves are normally not all the same.

In its 18th Global Risks Report on January 2023 the World Economic Forum mentioned widespread cybercrime & cyber insecurity as one of the top technological risks and cybersecurity on critical infrastructure amongst the top 5 currently manifesting risks that will have a severe impact at a global level in 2023.

As breaches become more significant, they are causing increased financial impact. The WannaCry, Petya and NotPetya attacks of 2017 had unprecedented financial effect some which are still being felt even today more than 5 years after they occurred.

Cybersecurity is probably the most discussed topic amongst Board of Directors, Senior Executives, Internal Auditors, Audit Committees, and Risk Management Committees.

In today's world of increased digital vandalism Auditors play an integral role in ensuring that cybersecurity risks are addressed appropriately; It has become imperative that risk-based Auditors should include cybersecurity in their agile risk-based audit plans.

TARGET AUDIENCE

At the end of the course, participants will be able to:

- Internal Auditors
- Cybersecurity practitioners
- Audit Managers
- IT Audit Consultants, Senior Consultants, Managers & Directors
- Risk & Audit Committee Members
- IT Professionals
- Audit & Risk Committee Members
- IT Assurance, Risk, Security and Governance Professionals
- IT practitioners



COURSE OBJECTIVES

At the end of this course delegates will be able to:

- Define & understand cybersecurity
- Understand the difference between information security and cybersecurity
- Comprehend cybersecurity concepts and definitions
 - Threats
 - Threat process
 - Attack phase
 - Threat actors
 - Vulnerabilities
 - Ransomware
 - Definition
 - Types
 - Malware Analysis Concepts and Methodology
 - Critical Infrastructure
 - SoC
 - SIEM
 - CIRT
- Appreciate in-depth Incident Response Plan [IRP]
 - Clearly articulate what an incident is and what it isn't
 - Has it been tested? Test, Test and Test again.
 - Has it been reviewed? Robust, flexible, and up to date
 - Are the IRP specific guiding specific activities during a crisis?
 - Are roles and responsibilities clearly defined, communicated, and accepted?
 - Governance structure - who is in charge in an event and during a phase of the event
 - Is the IR aligned to what is important to the business?
 - Training
 - Stakeholders buy-in, involvement and continuous commitment - inter business collaboration
 - Define key performance indicators - align to key business measures
 - Regulations governing the IRP - e.g., GDPR requires that security incidents be reported within 72 hours, SEC
 - Is there an incident response team - include a range of skills - memory analysis experts, malware analysis and threat intelligence skills, hosts and network forensics, penetration and good hunt skills
 - Network detection of attacker, communication, alerting and good liaison
- Understand Automotive Cybersecurity
- Define Cybersecurity Governance
 - Why cyber security the number one issue for Boards and management?
 - Cybersecurity Insurance
 - Cybersecurity Strategy
 - Frameworks:
 - NIST Cybersecurity Framework
 - COBIT
 - ISO27000
 - CIS
 - SANS
 - Cybersecurity rules and regulations
- Gain Skills and Knowledge to Perform a Value-Adding Cybersecurity Auditing
 - Comprehend the critical role of internal audit in cybersecurity?
 - Understand what an audit plan to assist organisations to mitigate cyber threats looks like
 - Defining Cybersecurity Auditing Scope
 - Define and establish cybersecurity testing procedures
 - Gain skills to report cybersecurity audit findings to different stakeholders
- Learn Practical Ways of Auditing Cybersecurity and Auditing Lessons from some renowned Cybersecurity Attacks:
 - NHS
 - Equifax
 - Sony Pictures
 - Target shops
 - Yahoo
 - Uber
 - Swift
 - Standard Bank
 - FedEx
- Learn emerging trends in cybersecurity



ABOUT THE TRAINER

TICHAONA ZORORO

CIA, CISA, CISM, CRMA, CDPSE, CRISC, CGEIT, COBIT Certified Assessor

Tichaona Zororo, CIA, CISA, CISM, CRMA, CDPSE, CRISC, CGEIT, COBIT Certified Assessor, is Director, Digital & Cybersecurity Advisory, with EGIT | Enterprise Governance of IT (Pty) Ltd – An Information & Technology [IT] Advisory firm based in South Africa, Namibia, Zambia and Zimbabwe focusing on Cybersecurity Assessments & Advisory, Governance of Enterprise Information & Technology, IT Auditing, IT Enabled Investments [Projects] Advisory, and Social Media Auditing & Governance.

He has several years of in-depth experience in Mainstream IT, IT Auditing, Cybersecurity, Corporate Governance, Enterprise Governance of IT, Digital & Innovation Governance, Enterprise Risk Management and IT Risk across private and public sectors in Africa, Europe, the USA and Asia.

Tichaona is an advisor to a number of Boards of Directors, IT and Business Leaders on Cybersecurity, Digitalisation, Innovation, Governance of Enterprise IT, IT Strategy, COBIT, IT Risk and IT Auditing. He is a Non-Executive Director and an ARC member of a number of organisations. Tichaona is a member of the Council [Board of Directors] of the Vaal University of Technology, Chair of the Business Innovation Technology Committee and a Member of its Audit & Risk and Governance Committees.

A Globally renowned COBIT Subject Matter Expert, Trainer and Advisor, Tichaona is credited for being the first COBIT Certified Assessor in Southern Africa and the 40th world-wide, the first African and person from Africa to sit on the ISACA Board of Directors [2016 – 2020] to chair its Audit and Risk Committee [2017 – 2019] and instrumental in establishing an internal audit function. Tichaona participated in the development and review of numerous COBIT publications and ISACA research papers on Big Data, Cloud Computing, BYOD, Digital Trust Ecosystem Framework and Outsourced IT Services to mention but a few. He has presented and participated in COBIT expert panels at several COBIT conferences world-wide and was voted the best speaker Africa and Asia CACS 2017.

Passionate about everything Corporate Governance, Digital, Governance of Enterprise IT, Cybersecurity, Digital and Innovation Governance, Risk and IT Auditing, He is a 2017 recipient of the prestigious ISACA Harold Weiss Award for Outstanding Achievement for his exceptional dedication and achievement that far exceeds the norm in Digital and Innovation Governance. Tichaona is an ISACA Hall of Fame Inductee. He is a member of the Institute of Internal Auditors Global Content Advisory Council, a Board Member [2012 - current] and Past Board Chair of ISACA South Africa Chapter [2012 - 2022].

A natural strategist, Tichaona is married to Ruth. They are blessed with 5 Children.

ADMINISTRATIVE DETAILS

TARGET AUDIENCE	LEVEL II-IV
MEMBER'S FEE	RM1,350.00 <i>All Fees will be subject to 6% SST</i>
NON-MEMBER'S FEE	RM1,550.00 <i>All Fees will be subject to 6% SST</i>
DATE	12 & 13 April 2023
TIME	1:00pm – 5:30pm
DELIVERY MODE	Virtual Platform
PROGRAMME CODE	2023/WEB09
TRAINER	Tichaona Zororo CIA, CISA, CISM, CRMA, CDPSE, CRISC, CGEIT, COBIT Certified Assessor
CPD POINTS	10



COURSE DETAILS

Course Title Auditing Cybersecurity

Course Code 2023/WEB09 Course Date(s) 12 & 13 April 2023

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 _____

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



PAYMENT DETAILS

Payment Details	Member Rate (per person) for KL-code related courses	Non-Member (per person)	6% 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@iam.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* and Certificate of Attendance.
- Full payment is to be made before the date of the course. Fee is subject to 6% SST.
- Walk-in delegates will only be allowed if full payment is made, subject to the availability of the seat.

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.

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.
 - Written cancellations should be received by 14 working days before the workshop date to get the refund.
 - 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.
 - 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.
 - 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 signing 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@iam.com.my Website: www.iam.com.my

Follow and like us on - IIA Malaysia - IIA Malaysia - IIA Malaysia - IIA Malaysia

