MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

COSO FOR CYBERSECURITY RISK MANAGEMENT

"Leveraging COSO to Strengthen Cybersecurity Governance, Controls, and Resilience"

Schedule

Venue (InHouse)	Fees
At Your Organization Premises	Ask For The Quotation

► **Available delivery methods:** In-House Training

Introduction

Cybersecurity risks are among the most significant threats facing organizations today. The COSO framework, widely recognized for its role in internal controls and risk management, can also serve as a powerful tool to strengthen cybersecurity governance and integrate cyber risk into enterprise risk management strategies.

This intensive 5-day training equips professionals with the knowledge and tools to apply COSO's principles specifically to cybersecurity risk management. Participants will explore how to align cyber controls with business objectives, build risk-aware cultures, and use COSO's guidance to assess, monitor, and report cybersecurity risk effectively.

Objectives

By the end of this course, participants will be able to:

- Understand the integration of COSO and cybersecurity risk frameworks
- Apply COSO principles to assess and manage cybersecurity risks
- Align cyber risk governance with enterprise strategy and risk appetite
- Design internal controls to prevent, detect, and respond to cyber threats
- Develop and implement cybersecurity risk assurance programs

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Why Attend

- Learn to apply the globally respected COSO model to cybersecurity risk
- Bridge the gap between risk management, IT, and cybersecurity functions
- Gain practical tools to assess and strengthen your organization’s cyber posture
- Improve regulatory compliance, stakeholder confidence, and digital resilience
- Lead and contribute to integrated cyber risk governance and assurance

Target Audience

This program is designed for:

- Cybersecurity professionals and managers
- Risk, audit, and compliance officers
- Internal and IT auditors
- CIOs, CISOs, and governance executives
- Anyone responsible for cyber risk oversight

Individual Benefits

Key competencies that will be developed include:

- Knowledge of COSO’s cybersecurity guidance and ERM integration
- Ability to design and assess cyber controls using COSO’s five components
- Understanding of cyber risk indicators, reporting, and assurance techniques
- Capability to contribute to cyber governance and incident response planning

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Stronger cybersecurity governance and risk-based decision-making
- Integration of cyber risk into broader risk management and control processes
- Improved alignment between IT/cybersecurity and business strategy
- Enhanced resilience to digital threats and regulatory challenges

Instructional Methodology

The course follows a blended learning approach combining theory with practice:

- Strategy Briefings – COSO\'s 5 components and 17 principles in a cybersecurity context
- Case Studies – Cyber breach investigations and lessons learned
- Workshops – Designing cyber risk assessments, control matrices, and response plans
- Peer Exchange – Sharing best practices across industries and regulatory environments
- Tools – Cyber control templates, cyber risk heat maps, and maturity models

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Course Outline

DETAILED 5-DAY COURSE OUTLINE (CUSTOMIZABLE)

Training Hours: 7:30 AM – 3:30 PM **Daily Format:** 3–4 Learning Modules | Coffee Breaks: 09:30 & 11:15 | Lunch Buffet: 01:00 – 02:00

Day 1: COSO Framework & Cybersecurity Risk Foundations

- Module 1: Overview of COSO for Cybersecurity (07:30 – 09:30)
- COSO's five components and relevance to cybersecurity
- Module 2: Cybersecurity Risk Landscape (09:45 – 11:15)
- Threat types, vulnerabilities, and digital risk trends
- Module 3: Case Study – Cybersecurity Failures (11:30 – 01:00)
- Module 4: Workshop – Mapping COSO to Cybersecurity Risks (02:00 – 03:30)

Day 2: Governance, Culture & Risk Appetite in Cybersecurity

- Module 1: Establishing Governance and Oversight (07:30 – 09:30)
- Role of the board, IT, and internal audit in cyber governance
- Module 2: Culture of Cybersecurity Awareness (09:45 – 11:15)
- Embedding risk-conscious behavior across the organization
- Module 3: Defining Cyber Risk Appetite (11:30 – 01:00)
- Module 4: Workshop – Cyber Risk Appetite Statement Development (02:00 – 03:30)

Day 3: Risk Assessment & Control Activities

- Module 1: Cyber Risk Identification and Assessment (07:30 – 09:30)
- Risk categories, impact, likelihood, and interdependence
- Module 2: Internal Controls for Cybersecurity (09:45 – 11:15)
- Designing detective, preventive, and responsive controls
- Module 3: Workshop – Building a Cyber Control Matrix (11:30 – 01:00)
- Module 4: Peer Exchange – Challenges in Cyber Risk Assessment (02:00 – 03:30)

Day 4: Information, Communication, and Monitoring

- Module 1: Cybersecurity Information and Reporting (07:30 – 09:30)
- Cyber metrics, dashboards, and reporting structures
- Module 2: Incident Reporting and Response (09:45 – 11:15)
- Communication protocols and stakeholder engagement
- Module 3: Monitoring and Assurance (11:30 – 01:00)
- Control testing, audits, and real-time monitoring tools
- Module 4: Workshop – Creating a Cyber Assurance Plan (02:00 – 03:30)

Day 5: Integration & Cyber Risk Management Maturity

- Module 1: Embedding Cyber Risk into Strategy and Planning (07:30 – 09:30)
- Integrating cybersecurity with ERM and strategic decision-making
- Module 2: COSO Maturity Models and Cyber Capability Frameworks (09:45 – 11:15)
- Module 3: Workshop – Self-Assessment of Cyber Governance Using COSO (11:30 – 01:00)
- Module 4: Final Presentation, Action Planning, and Wrap-Up (02:00 – 03:30)

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Certification

Certificate of Completion in COSO for Cybersecurity Risk Management, confirming their ability to apply COSO's internal control and risk management principles in the context of cybersecurity. This certification demonstrates practical expertise in aligning cyber governance with enterprise objectives and enhancing digital risk resilience.

Why Choose MAWA Events

- **Global Expertise:** More than 17 years of experience in professional training and consulting.
- **Industry-Leading Faculty:** Courses delivered by seasoned professionals with hands-on experience.
- **Practical Insights:** Learn to turn theory into actionable strategies for real-world business impact.
- **Client-Focused Solutions:** Customized programs designed to achieve your organisation's unique goals.

In-House / Customized Training Interested in running this course for your team? Please contact us:	TEL: **+601116373203**	EMAIL: **info@mawaevents.net**

Follow us: **Facebook** **Twitter** **YouTube** **LinkedIn** **Instagram**

© Material published by MAWA Events shown here is copyrighted. All rights reserved. Any unauthorized copying, distribution, use, dissemination, downloading, storing (in any medium), transmission, reproduction or reliance in whole or any part of this course outline is prohibited and will constitute an infringement of copyright.