หลักสูตรความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (CYBERSECURITY FUNDAMENTALS PROGRAM) และการเตรียมสอบวุฒิบัตร

ภัยคุกคามทางด้านไซเบอร์มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่องในหลายปีที่ผ่านมา จำนวนองค์กรและผู้ที่ได้รับผลกระทบจากภัยคุกคามมีแนวโน้มเพิ่มสูงขึ้น ประกอบกับข้อกำหนดทางด้านกฎหมายที่ต้องการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ ก่อให้เกิดความต้องการผู้มีทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มีมากขึ้นทั้งในภาครัฐและภาคเอกชน ดังนั้น Information Systems Audit and Control Association ได้ตระหนักถึงความต้องการดังกล่าว จึงได้จัดให้มีวุฒิบัตรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ขึ้นมาเพื่อยกระดับมาตรฐานของวิชาชีพด้านนี้ โดยแบ่งวุฒิบัตรออกเป็น 2 ระดับ คือ

1. ระดับพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Fundamentals Certificate)
2. ระดับผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Practitioner Certificate)

สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ - ภาคพื้นกรุงเทพฯ (ISACA Bangkok Chapter) จึงได้จัดหลักสูตร ความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ **(Cybersecurity Fundamental Program & Workshop)** ซึ่งเป็นหลักสูตรที่ออกแบบมาสำหรับวางพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ที่เริ่มต้นปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ ให้เข้าใจถึงหลักการ กรอบดำเนินการ แนวปฏิบัติ และกระบวนการควบคุมที่สำคัญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ นอกจากนี้ เพื่อให้มั่นใจว่าความรู้ที่ได้รับเป็นไปตามมาตรฐานที่ยอมรับ หลักสูตรนี้ได้เสริมเนื้อหาเกี่ยวกับการสอบวุฒิบัตร CYBERSECURITY FUNDAMENTALS CERTIFICATE เพื่อเพิ่มศักยภาพให้ผู้เข้ารับการอบรมมีความมั่นใจในการสอบวุฒิบัตร โดยครอบคลุมเนื้อหาดังนี้

- Cybersecurity concept, incident response, implication & adoption of evolving technology
- Workshop เรื่องช่องโหว่ของ Web application
- หัวข้อสำหรับการสอบ Cybersecurity fundamentals certificate
  - Cybersecurity concepts
  - Cybersecurity architecture principles
  - Cybersecurity of networks, systems, applications and data Incident response
  - The security implications of the adoption of emerging technologies
- Cybersecurity Fundamentals Certificate 's Mock Exam

CPE ที่ได้รับ: 12 หน่วย

ระยะเวลา

20 – 22 ตุลาคม 2568 (3 วัน)

วิทยากร

คุณสมชัย แพทย์วิบูลย์
CISA,CISM,CRISC,CGEIT,CIA,CFE,CISSP,CSSLP
กรรมการสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ-ภาคพื้นกรุงเทพฯ

อัตราค่าธรรมเนียม

ผู้สมัครเข้าร่วมสัมมนา	อัตราค่าธรรมเนียม
สมาชิกของ ISACA	16,050.00
สมาชิก IIA และกลุ่มบุคคลจากองค์กรเดียวกันตั้งแต่ 3 คนขึ้นไป	17,120.00
บุคคลทั่วไป	18,190.00

อัตราค่าธรรมเนียมข้างต้นรวมภาษีมูลค่าเพิ่ม 7% แล้ว
(สมาคมได้รับการยกเว้นไม่ต้องถูกหักภาษี ณ ที่จ่ายตามคำสั่งกรมสรรพากรที่ ท.ป. 4/2528 ข้อ 12/1)

หมายเหตุ : สำหรับในช่วงบ่านวันที่สองของหลักสูตรซึ่งเป็น workshop ผู้เข้าอบรมต้องเตรียม Computer Notebook มาใช้ในการอบรม โดยเครื่องที่ใช้ต้องมีคุณสมบัติขั้นต่ำดังนี้

- CPU Core I3 ขึ้นไป มี RAM 4 GB ขึ้นไป และมีพื้นที่คงเหลือไม่ต่ำกว่า 10 GB
- ระบบปฏิบัติการ Windows 10 ขึ้นไป (64 bit)
- สามารถติดตั้ง VMPlayer ได้ (ทั้งนี้ ผู้ประสานงานของสมาคมจะส่ง VMPlayer ที่ได้รับจากวิทยากร ไปให้ผู้เข้าอบรมทางเมล์ เพื่อติดตั้งในเครื่องก่อนวันเข้าอบรม)

การลงทะเบียนและการชำระค่าอบรม

ผู้สมัครจะต้องลงทะเบียนออนไลน์ทาง www.isaca-bangkok.org/event และทำรายการโอนเข้าบัญชีเงินฝากออมทรัพย์ **ธนาคารไทยพาณิชย์จำกัด (มหาชน) สาขาเซ็นทรัลเวิลด์ หมายเลข 247-231087-1** ชื่อบัญชี: สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ-ภาคพื้นกรุงเทพฯ

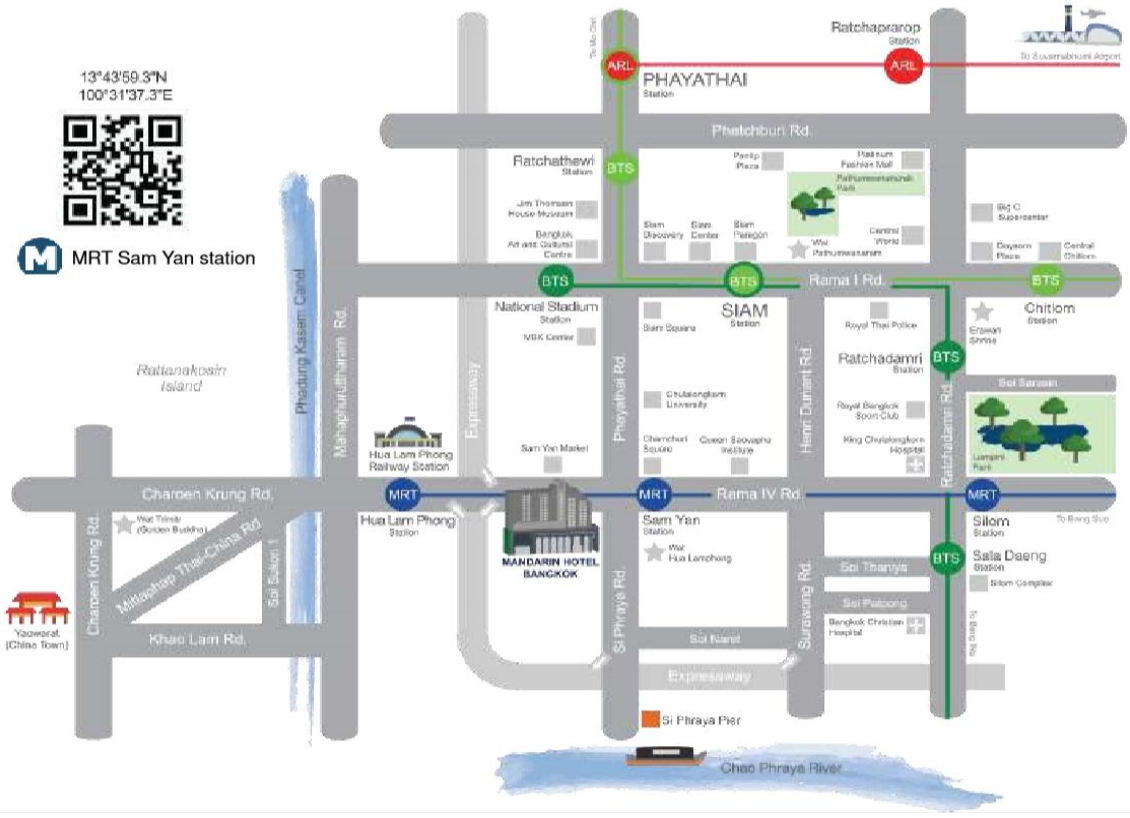
หลังจากชำระเงินกรุณาแจ้งการชำระเงินและส่งหลักฐานการโอนเงิน (Pay-in Slip) ไปที่เว็บไซต์ www.isaca-bangkok.org/payment หรือแนบหลักฐานการนำเงินเข้าบัญชีของสมาคมส่งเมล์ไปที่ training@isaca-bangkok.org

ผู้สมัครจะต้อง**ชำระโดยการโอนเงินก่อนวันที่ 12 ตุลาคม 2568** จำนวนเงินค่าอบรมที่ชำระจะต้องเป็นจำนวนเงินตามที่ระบุไว้ข้างต้น โดยไม่มีการหักค่าธรรมเนียมการโอนเงินของธนาคารหรือค่าธรรมเนียมอื่นใด ทั้งนี้สมาคมฯ ไม่มีนโยบายรับและชำระเงินในวันอบรมหรือภายหลังการอบรม

ติดต่อสอบถามรายละเอียดการอบรมได้ที่ คุณประทักษ์ วงศ์สินคงมั่น โทรศัพท์หมายเลข 089-777-0900 Email: training@isaca-bangkok.org

สถานที่อบรม

แผนที่โรงแรมแมนดาริน สามย่าน



หัวข้อการบรรยาย

SECTION 1: CYBER SECURITY INTRODUCTION AND OVERVIEW

- Introduction to cyber security
- Different between information security and cyber security
- Cyber security objectives
- Cyber security roles
- Cyber security domains

SECTION 2: CYBER SECURITY CONCEPT

- Risks
- Common attack types and vectors
- Policies and procedures
- Cyber security controls

SECTION 3 SECURITY ARCHITECTURE PRINCIPLES

- Overview of security architecture
- The OSI model
- Défense in depth
- Firewalls
- Isolation and segmentation
- Monitoring detection and logging
- Encryption

SECTION 4 SECURITIES OF NETWORKS, SYSTEMS, APPLICATION AND DATA

- Risk assessment
- Vulnerability management
- Penetration testing
- Network security
- Operating system security
- Application security
- Data security

SECTION 5 INCIDENT RESPONSES

- Event VS incident
- Security incident response
- Investigations, Legal Holds and preservation
- Forensics
- Disaster Recovery and Business Continuity Plan

SECTION 6 SECURITY IMPLICATIONS AND ADOPTIONS OF EVOLVING TECHNOLOGY

- Current threat Landscape
- Advance persistent threats
- Mobile technology
- Consumerization of IT and mobile devices
- Cloud and digital Collaboration

SECTION 7 Workshops

- Web Application Penetration Testing with Damn Vulnerable Web App (DVWA)
- Learn how hackers exploit web applications such as Brute force, Command Injection, XSS, SQL injection etc.

SECTION 8 Mock Exam