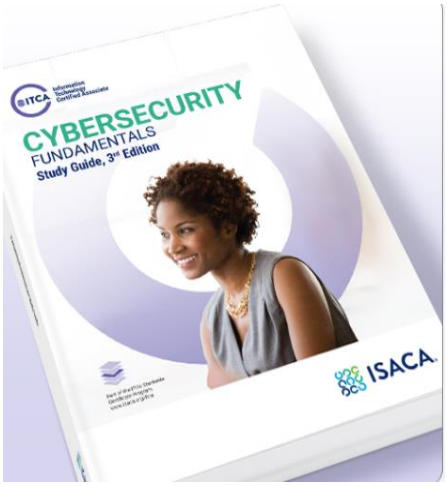
ISACA Bangkok Chapter

หลักสูตร

# ความรู้พื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการเตรียมสอบวุฒิบัตร

# Cybersecurity Fundamentals Examination Preparation Program And Mock Exam

**ครั้งที่ 1/2565 วันที่ 19 – 21 สิงหาคม 2565**




ภัยคุกคามทางด้านไซเบอร์มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่องในหลายปีที่ผ่านมา จำนวนองค์กรและผู้ที่ได้รับผลกระทบจากภัยคุกคามมีแนวโน้มเพิ่มขึ้น ประกอบกับข้อกำหนดทางด้านกฎหมายที่ต้องการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ ก่อให้เกิดความต้องการผู้มีทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มีมากขึ้นทั้งในภาครัฐและภาคเอกชน สมาคม ISACA ได้ตระหนักถึงความต้องการดังกล่าว จึงได้จัดให้มีวุฒิบัตรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ขึ้นมาเพื่อยกระดับมาตรฐานของวิชาชีพด้านนี้ โดยแบ่งวุฒิบัตรออกเป็น 3 ระดับ คือ

1. ระดับพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ( CYBERSECURITY FUNDAMENTALS CERTIFICATE)
2. ระดับพื้นฐานทางเทคนิคด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (CSX TECHNICAL FOUNDATIONS CERTIFICATES)
3. ระดับผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (CSX CYBERSECURITY PRACTITIONER)

หลักสูตรความรู้พื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ **(CYBERSECURITY FUNDAMENTALS)** เป็นหลักสูตรที่ออกแบบมาสำหรับวางพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ที่เริ่มต้นปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ ให้เข้าใจถึงหลักการ กรอบดำเนินการ แนวปฏิบัติ และกระบวนการควบคุมที่สำคัญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ นอกจากนี้ เพื่อให้มั่นใจว่าความรู้ที่ได้รับเป็นไปตามมาตรฐานที่ยอมรับ หลักสูตรนี้ได้เสริมเนื้อหาเกี่ยวกับการสอบวุฒิบัตร **CYBERSECURITY FUNDAMENTALS CERTIFICATE** เพื่อเพิ่มศักยภาพให้ผู้เข้ารับการอบรมมีความมั่นใจในการสอบวุฒิบัตร

สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ-ภาคพื้นกรุงเทพ (ISACA Bangkok Chapter) เป็นหน่วยงานที่ได้รับอนุญาตอย่างเป็นทางการจากสมาคม ISACA ในการจัดหลักสูตร Cybersecurity Fundamentals Examination Preparation Program and Mock Exam โดยจะครอบคลุมเนื้อหาดังนี้

- หัวข้อหลักสำหรับการสอบ Cybersecurity fundamentals certificate
  - Cyber security concepts
  - Cyber security architecture principles
  - Cyber security of networks, systems, applications and data Incident response
  - The security implications of the adoption of emerging technologies
- Lab เรื่องช่องโหว่ของ Web application
- Cybersecurity Fundamentals Certificate ‘s Mock Exam

## CPE

**ที่ได้รับ**: 12 หน่วย

## ระยะเวลา

19 – 21 สิงหาคม 2564 (3 วัน)

## วิทยากร

คุณสมชัย แพทย์วิบูลย์ CIA,CISA,CISM,CFE,CISSP,CSSLP,CRISC,CSX Fundamental

## อัตราค่าธรรมเนียม

| ผู้สมัครเข้าร่วมสัมมนา | อัตราค่าธรรมเนียม |
|---|---|
| สมาชิกของ ISACA | **14,445** บาท |
| สมาชิก ITSMF, IIAT และกลุ่มบุคคลจากองค์กรเดียวกันตั้งแต่ 3 คนขึ้นไป | **16,050** บาท |
| บุคคลทั่วไป | **19,260** บาท |

อัตราค่าธรรมเนียมข้างต้นรวมภาษีมูลค่าเพิ่ม 7% แล้ว

(สมาคมได้รับการยกเว้นไม่ต้องถูกหักภาษี ณ ที่จ่ายตามคำสั่งกรมสรรพากรที่ ท.ป. 4/2528 ข้อ 12/1)

**หมายเหตุ** : สำหรับหลักสูตรนี้ ผู้เข้าอบรมต้องเตรียม Computer Notebook มาใช้ในการเรียนในวันที่สองของหลักสูตร โดยเครื่องต้องมีคุณสมบัติขั้นต่ำดังนี้

- CPU Core I3 ขึ้นไป มี RAM 4 GB ขึ้นไป และมีพื้นที่คงเหลือไม่ต่ำกว่า 10 GB
- ระบบปฏิบัติการ Windows 7 ขึ้นไป (64 bit)
- สามารถติดตั้ง VMPlayer ได้

**ติดต่อสอบถามรายละเอียดเพิ่มเติมได้ที่ คุณประทักษ์ วงศ์สินคงมั่น โทรศัพท์หมายเลข 081-840-5835**
Email: conference@isaca-bangkok.org

## การสมัครเข้าอบรมและชำระค่าธรรมเนียมในการเข้าสัมมนา

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

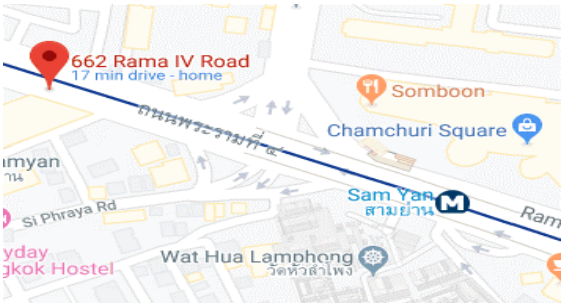
หลังจากชำระเงินกรุณาแจ้งการชำระเงินและส่งหลักฐานการโอนเงิน (Pay-in Slip) ไปที่เว็บไซต์ **www.isaca-bangkok.org/payment**

ผู้สมัครจะต้อง**โอนเงินก่อนวันที่ 13 สิงหาคม 2565** จำนวนเงินค่าสัมมนาที่ชำระจะต้องเป็นจำนวนเงินตามที่ระบุไว้ข้างต้น โดยไม่มีการหักค่าธรรมเนียมการโอนเงินของธนาคารหรือค่าธรรมเนียมอื่นใด ทั้งนี้สมาคมฯ ไม่มีนโยบายรับและชำระเงินในวันสัมมนาหรือภายหลังการสัมมนา

เนื่องจากการสัมมนาในครั้งนี้ **จำกัดจำนวนที่ 20 ท่าน** หากมีผู้สมัครเข้ามามากกว่าจำนวนที่รับได้ จะให้สิทธิ์ผู้ที่ส่งหลักฐานการชำระเงินเข้ามาก่อน

## สถานที่จัดสัมมนา

**โรงแรมแมนดาริน สามย่าน https://g.page/mandarinhotelbkk?share**




**<u>หมายเหตุ</u>** เพื่อป้องกันการแพร่ระบาดของไวรัส COVID-19 มีมาตรการดังต่อไปนี้

1. จำกัดเพียง 20 คนต่อหลักสูตร
2. จัดให้ผู้เข้าอบรม/สัมมนา นั่งเพียงโต๊ะละ 1 ท่านเพื่อรักษาระยะห่างทางสังคม(Social Distancing)
3. มีการวัดอุณหภูมิผู้เข้าอบรม/สัมมนา ทุกท่าน ทุกวัน ก่อนเข้าห้องอบรม/สัมมนา
4. ผู้เข้าอบรม/สัมมนาต้องสวมหน้ากากอนามัย และกรณี
   - ในช่วง 14 วันที่ผ่านมา ก่อนมาอบรม /สัมมนานั้น มีประวัติการเดินทางไปยัง หรือมาจากต่างประเทศหรือไม่ หรือมีอาการไอ/เจ็บคอ/มีน้ำมูก/ไม่ได้กลิ่น/ไม่รับรู้รส หรือไม่ ถ้ามี กรุณางดลงทะเบียนเข้าร่วมอบรม/สัมมนา

     **** ในกรณีที่ผู้เข้าอบรม/สัมมนา มีไข้ ตั้งแต่ 37.5 C หรือมีอาการเสี่ยง สมาคมฯ ต้องขอให้บุคคลนั้นงดเข้าห้องอบรมก่อนเข้าห้องทันที**

# 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
- Defense 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.