28 สิงหาคม 2569

เรื่อง เรียนเชิญส่งอาจารย์และบุคลากรเข้าร่วมอบรมเกี่ยวกับ Cybersecurity พร้อมส่วนลดพิเศษ

เรียน รองศาสตราจารย์ ดร.วัชรินทร์ กาสลัก อธิการบดีมหาวิทยาลัยบูรพา

สิ่งที่แนบมาด้วย 1. เอกสารรายละเอียดผู้จัดโครงการ
2. เอกสารรายละเอียดโครงการ Cybersecurity BootKamp รุ่นที่ 2
3. เอกสารรายละเอียดโครงการ IT & Security Audit BootKamp

SKILLKAMP ร่วมกับสมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ (Cyber Innovation Promotion Association of Technology: CIPAT) ได้ตระหนักถึงความสำคัญของการพัฒนาองค์ความรู้และทักษะด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์ ซึ่งมีการเปลี่ยนแปลงอย่างรวดเร็วและเป็นหัวใจสำคัญในการปกป้องค์กรในยุคดิจิทัล

จึงได้จัดโครงการอบรมเชิงปฏิบัติการเข้มข้น 2 หลักสูตร เพื่อยกระดับศักยภาพบุคลากรสาย IT ดังนี้:

1. โครงการ Cybersecurity BootKamp รุ่นที่ 2 (กำหนดการอบรม: วันที่ 31 ตุลาคม 2569 – 28 พฤศจิกายน 2569 รวมทั้งสิ้น 5 สัปดาห์)

ด้วยผู้จัดโครงการเห็นถึงความสำคัญของการเรียนรู้ด้านวิชาการไปพร้อมกับการได้ลงมือทำจริง จึงออกแบบหลักสูตรให้มีภาคทฤษฎีประกอบกับการปฏิบัติ อาทิ การศึกษาเชิงปฏิบัติการ (Workshop) และการฝึกจำลองด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Laboratory Experimentation) ในสถานการณ์จำลองหลากหลายรูปแบบ เพื่อเสริมทักษะด้าน Cybersecurity ให้กับบุคลากรด้าน IT นำองค์ความรู้ไปประยุกต์ใช้ในหน่วยงานของตนต่อไป (Train the Trainers)

2. โครงการ IT & Security BootKamp (กำหนดการอบรม: วันที่ 11 ตุลาคม 2569 – 22 พฤศจิกายน 2569 รวมทั้งสิ้น 7 สัปดาห์)

ผู้จัดโครงการเน้นการพัฒนาทักษะการตรวจสอบระบบสารสนเทศ (IT & Security Audit) แบบครบวงจรผ่านการลงมือทำจริง (Hands-on) กลั่นองค์ความรู้จากการใช้เกณฑ์มาตรฐานสากล (ISO/IEC 27001, NIST CSF และ PDPA) ครอบคลุมตั้งแต่การจัดทำ Audit Checklist, การปฏิบัติการตรวจ, การเขียนรายงาน ตลอดจนการกำหนดแนวทางแก้ไข (Corrective Action Plan) เพื่อยกระดับความมั่นคงปลอดภัยตามหลักการบริหารความเสี่ยงยุคใหม่

ในการนี้ ทางธนาคารกสิกรไทยร่วมกับสมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ **จึงขอเรียนเชิญส่งบุคลากรขององค์กรท่านเข้าร่วมโครงการ Cybersecurity BootKamp รุ่นที่ 2 และ/หรือ โครงการ IT & Security BootKamp พร้อมมอบส่วนลดพิเศษ ดังนี้**

โครงการ Cybersecurity BootKamp รุ่นที่ 2

มอบส่วนลดพิเศษ 5% ถึง 20 กันยายน 2569 เพียง 27,455 บาทต่อท่าน รวมภาษีมูลค่าเพิ่มแล้ว (จากราคาปกติ 28,900 บาท) สามารถแจ้งความประสงค์ลงทะเบียน ภายในวันที่ 25 ตุลาคม 2569

โครงการ IT & Security BootKamp

มอบส่วนลดพิเศษ 5% ถึง 9 กันยายน 2569 เพียง 20,805 บาทต่อท่าน รวมภาษีมูลค่าเพิ่มแล้ว (จากราคาปกติ 21,900 บาท) สามารถแจ้งความประสงค์ลงทะเบียน ภายในวันที่ 2 ตุลาคม 2569

ทั้งนี้สามารถติดต่อผ่านผู้ประสานงาน นางสาวธัญญลักษณ์ สุริยศศิธร หมายเลขโทรศัพท์ 02-273-3963 **ต่อ** 38562 **อีเมล** Thanyalak.sur@kasikornbank.com หากองค์กรของท่าน สนใจส่งผู้เข้าร่วมมากกว่า 1 ท่านขึ้นไป ทางธนาคารฯ ยินดีพิจารณาให้เป็นกรณีพิเศษ รายละเอียดดังเอกสารแนบ

จึงเรียนมาเพื่อโปรดพิจารณา และขอขอบคุณมา ณ โอกาสนี้

เรียน รองอธิการบดีฝ่ายแผนยุทธศาสตร์และนโยบาย

ด้วย ธนาคารกสิกรไทยร่วมกับสมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ขอเรียนเชิญส่งอาจารย์และบุคลากรเข้าร่วมอบรมโครงการ Cybersecurity BootKamp รุ่นที่ ๒ และ/หรือ โครงการ IT & Security BootKamp พร้อมส่วนลดพิเศษ

จึงเรียนมาเพื่อ

๑. เพื่อโปรดทราบ

๒. เห็นควรเผยแพร่ให้ทราบทั่วกันและสามารถดาวน์โหลดหนังสือได้ที่ http://docshare.buu.ac.th

๐๑ ก.ย. ๒๕๖๙

๐๑ ก.ย. ๒๕๖๙

(นางสาวพอตา พูนสถาพร)

ผู้อำนวยการฝ่าย

สายงาน Corporate Strategy and Innovation

ธนาคารกสิกรไทย

ทราบ/ดำเนินการตามเสนอ

๐๑ ก.ย. ๒๕๖๙

1. เอกสารรายละเอียดผู้จัดโครงการ

โครงการ Cybersecurity BootKamp รุ่นที่ 2 และ โครงการ IT & Security Audit BootKamp เกิดขึ้นภายใต้ความร่วมมือระหว่างแพลตฟอร์ม SKILLKAMP (สกิลแคมป์) และ สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ (Cyber Innovation Promotion Association of Technology หรือ CIPAT)

แพลตฟอร์ม SKILLKAMP (สกิลแคมป์) คือ แพลตฟอร์มภายใต้การดูแลของธนาคารกสิกรไทย สำหรับพัฒนาทักษะและศักยภาพด้านดิจิทัลแห่งอนาคต ให้บริการทั้งลูกค้าทั่วไป (B2C) และลูกค้าองค์กร (B2B) เป็นศูนย์กลางระบบ e-learning เชื่อมโยงผู้เรียน ผู้สอน และองค์กร (Marketplace) เพื่อยกระดับทักษะดิจิทัลของแรงงาน โดยในแพลตฟอร์มมีคอร์สออนไลน์กว่า 470 คอร์สจากผู้ให้บริการชั้นนำกว่า 25 รายทั่วประเทศไทย ซึ่งครอบคลุมทักษะในหลากหลายด้าน เช่น Technology, Data & AI, Business, Marketing, Creativity & Design, Finance and Investment, Cybersecurity เป็นต้น

สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ (Cyber Innovation Promotion Association of Technology หรือ CIPAT) ก่อตั้งขึ้นในปี 2560 โดยกลุ่มบริษัทเอกชนด้านนวัตกรรม และอาจารย์มหาวิทยาลัย มีเป้าหมายในการพัฒนานวัตกรรมและบุคลากรด้านไซเบอร์ของไทยอย่างปลอดภัยและยั่งยืน มีเครือข่ายความร่วมกับภาครัฐและเอกชน ร่วมถึงพันธมิตรในอุตสาหกรรมชั้นนำ อาทิ NT, Fortinet, Amazon Web Services (AWS) เป็นต้น โดยได้รับการแต่งตั้งเป็น Cisco Networking Academy อย่างเป็นทางการ ทั้งยังมีบทบาทหลักในการปั้นเยาวชนไทยสู่ทีมชาติสาขา Cybersecurity ผ่านเวทีแข่งขันฝีมือแรงงานแห่งชาติและระดับนานาชาติ (WorldSkills)

2. เอกสารรายละเอียดโครงการ Cybersecurity BootKamp รุ่นที่ 2

1. วัตถุประสงค์ของโครงการ

1. **เพื่อยกระดับและพัฒนาทักษะ** (Upskill & Reskill) มุ่งเน้นการเสริมสร้างขีดความสามารถของบุคลากรด้าน IT ทั้งในมิติด้านทฤษฎีและทักษะเชิงปฏิบัติการให้มีมาตรฐานสากล
2. **เพื่อสร้างบุคลากรต้นแบบและผู้นำการเปลี่ยนแปลง** (Changemakers) มุ่งพัฒนาผู้นำด้าน Cybersecurity ภายในองค์กรที่มีศักยภาพในการถ่ายทอดองค์ความรู้ พร้อมทั้งเสริมสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ให้แก่บุคลากรอื่นในหน่วยงานอย่างเป็นรูปธรรม
3. **เพื่อสร้างเครือข่ายความร่วมมือของผู้มีศักยภาพสูง** (High-caliber Networking) พัฒนาเครือข่ายความสัมพันธ์ระหว่างบุคลากรด้าน IT และ Cybersecurity เพื่อเป็นกลไกในการแลกเปลี่ยนองค์ความรู้ ประสบการณ์ และการต่อยอดทางวิชาชีพในอนาคต
4. **เพื่อสร้างพื้นที่แห่งนวัตกรรมและการสร้างสรรค์** (Innovation Space) ส่งเสริมให้เกิดพื้นที่สำหรับการระดมความคิดสร้างสรรค์ การแลกเปลี่ยนทัศนคติ และการพัฒนานวัตกรรมด้าน Cybersecurity เพื่อรองรับความท้าทายในยุคดิจิทัล

2. กลุ่มผู้เรียนเป้าหมาย

- บุคลากรด้าน Cybersecurity และ IT จากหน่วยงานและองค์กร
- อาจารย์และบุคลากรด้าน Cybersecurity และ IT สังกัดสถาบันอุดมศึกษา
- ผู้ดูแลระบบเครือข่าย (Network Administrator) นักพัฒนาซอฟต์แวร์ (Software Developer) รวมถึงผู้ประกอบวิชาชีพในสายงานอื่นที่เกี่ยวข้อง
- ผู้เรียนที่มีความรู้เรื่องเครือข่ายคอมพิวเตอร์เบื้องต้น

3. จุดเด่นของโครงการ

1. **รูปแบบการเรียนรู้ที่หลากหลาย** อาทิ การเรียนรู้ผ่านระบบออนไลน์ (Online Module) การฝึกอบรมเชิงปฏิบัติการ (Onsite Workshop) และการทดลองปฏิบัติการในสภาพแวดล้อมจำลอง (Virtual Laboratory) โดยมีผู้ทรงคุณวุฒิและผู้เชี่ยวชาญเฉพาะด้าน Cybersecurity เป็นผู้กำกับดูแลตลอดระยะเวลาโครงการ
2. **การฝึกจำลองด้านความมั่นคงปลอดภัยไซเบอร์** (Cybersecurity Laboratory Experimentation) มุ่งเน้นการเรียนรู้ผ่านการลงมือปฏิบัติจริงในสภาพแวดล้อมจำลอง (Virtual Laboratory) แบบรายบุคคล (One-on-One) ซึ่งครอบคลุมเนื้อหาการกำหนดค่าอุปกรณ์เครือข่ายระดับองค์กร และการเสริมสร้างความปลอดภัยให้กับระบบปฏิบัติการ (System Hardening) รวมทั้งสิ้นกว่า 15 หน่วยการเรียนรู้

3. **การจำลองสถานการณ์ภัยคุกคามเสมือนจริง** เพื่อพัฒนาประสบการณ์ในการรับมือกับเหตุการณ์ไม่พึงประสงค์ผ่านกิจกรรมการแข่งขันทางไซเบอร์ (Mini Capture The Flag: CTF) ซึ่งครอบคลุมทั้งมิติด้านการทดสอบเจาะระบบเชิงรุก (Offensive) และการตั้งรับเพื่อป้องกันเชิงลึก (Defensive) ภายใต้สภาวะจำลองที่สอดคล้องกับสถานการณ์ปัจจุบัน

4. ตารางการอบรม (รายละเอียดอาจมีการเปลี่ยนแปลงได้ตามความเหมาะสม)

ตุลาคม	พฤศจิกายน										
31 ต.ค. (เสาร์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน	1-6 พ.ย. วิดีโอ ออนไลน์ 4 คอร์ส	7 พ.ย. (เสาร์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน	8-13 พ.ย. วิดีโอ ออนไลน์ 2 คอร์ส	11 พ.ย. (พุธ) เรียนสด ออนไลน์	14 พ.ย (เสาร์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน	15-20 พ.ย. วิดีโอ ออนไลน์ 1 คอร์ส	18 พ.ย. (พุธ) เรียนสด ออนไลน์	22 พ.ย. (อาทิตย์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน	22-27 พ.ย. วิดีโอ ออนไลน์ 1 คอร์ส	25 พ.ย. (พุธ) เรียนสด ออนไลน์	28 พ.ย. (เสาร์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน

โครงการมีกำหนดการเรียนตั้งแต่วันที่ 31 ตุลาคม ถึงวันที่ 28 พฤศจิกายน 2569 รวมระยะเวลาทั้งสิ้น 5 สัปดาห์ ประกอบด้วย 12 หน่วยการเรียนรู้ รวมทั้งสิ้นกว่า 60 ชั่วโมง ซึ่งการเรียนรู้ผ่านระบบออนไลน์ (Video Learning) ผู้เข้ารับการอบรมสามารถเลือกเรียนได้ตามความเหมาะสมของเวลา จำนวน 8 บทเรียน พร้อมการสอนแบบถ่ายทอดสด(Live Session) จำนวน 3 ครั้ง และ การฝึกอบรมเชิงปฏิบัติการ (Onsite Workshop) จำนวน 5 ครั้ง โดยกำหนดจัดขึ้น ณ สถาบันเทคโนโลยีปทุมวัน (สทป.)

5. รายละเอียดหลักสูตร (รายละเอียดอาจมีการเปลี่ยนแปลงได้ตามความเหมาะสม)

วันกิจกรรม	รายละเอียด
31 ต.ค. (เสาร์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน *ผู้เรียนต้องนำ Laptop ส่วนตัวมาเข้าเรียน	1. **บรรยายเรื่องสายงาน cybersecurity ในตลาดแรงงานไทย และแนะนำภาพรวมหลักสูตร** 2. **ปรับพื้นฐานการเรียนรู้ Network Basic & Network Security** 1. การออกแบบและวางโครงสร้างเครือข่าย (Network Design) 2. การตั้งค่าระบบเครือข่ายพื้นฐาน (IP & Routing) 3. การแบ่งและบริหารจัดการเครือข่าย (Switching & VLANs) 4. การวิเคราะห์การวิ่งของข้อมูล (Simulation Mode)
1-6 พ.ย. วิดีโอ ออนไลน์ 4 คอร์ส	1. Core Networking and Operating System 5. การออกแบบโครงสร้างเครือข่ายระดับองค์กร 6. การบริหารจัดการสิทธิ์ผู้ใช้งาน 7. การกำหนดค่า Linux Security Baseline 8. พื้นฐาน Cloud Computing 9. พื้นฐาน Operation Technology หรือ OT
	2. Fundamental of Cyber security practitioner 1. General Security Concepts 2. Threats, Vulnerabilities, and Mitigations 3. Security Architecture 4. Security Operations 5. Security Program Management and Oversight
	3. Digital law and compliance 1. มาตรฐาน ISO27001 (ISMS) 2. มาตรฐาน ISO27701 (PIMS) 3. มาตรฐาน ISO 22301 (BCMS) 4. PDPA, Computer Crime Act (พรบ คอมพิวเตอร์/ พรบ ไซเบอร์) 5. มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ 6. Cloud Security Guideline
	4. Network Security and Firewall Appliances 1. การติดตั้งและกำหนดค่า Firewall 2. การแบ่ง Segment เครือข่าย 3. การจัดทำระบบ Remote Ac
7 พ.ย. (เสาร์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน *ผู้เรียนต้องนำ Laptop ส่วนตัวมาเข้าเรียน	5. Enterprise Infrastructure Build-up Workshop 1. Cybersecurity Virtual Laboratory การบริหารจัดการและตั้งค่า Firewall ระดับองค์กร 2. ลงมือตั้งค่าบนอุปกรณ์แบบ 1 ต่อ 1 เรียนรู้ทั้ง 15 โมดูล อาทิ ตั้งค่า DHCP, DNS, สร้าง Firewall Policy และ NAT Rules, ติดตั้ง Private CA Certificate, ตั้งค่า IPS Sensor

วันกิจกรรม	รายละเอียด
8-13 พ.ย. วิดีโอ ออนไลน์ 2 คอร์ส	6. Monitoring and Centralized Logging 1. ระบบ OT/ICS และโครงสร้างพื้นฐานสำคัญ 2. ความแตกต่างระหว่างของ IT Security กับ OT Security 3. IT/OT Network Segmentation and Zone & Conduit 4. Industrial Network and OT Protocol Security 5. PLC Security and Secure Configuration 6. OT Endpoint and Asset Security 7. การรับส่งข้อมูลอย่างปลอดภัยระหว่างเครือข่าย IT และ OT 8. การรับมือและตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัยในระบบ OT/ICS (Incident Response) 9. Critical Infrastructure Cyberattack Case Studies
	7. SOC Operations, SIEM and Centralized Logging 1. กระบวนการวิเคราะห์เหตุการณ์ในศูนย์ปฏิบัติการความมั่นคงปลอดภัย (SOC) 2. Log Collection and Log Management 3. การเฝ้าระวังและการวิเคราะห์เหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัย 4. Security Operations Center (SOC) Operations 5. พื้นฐานระบบ SIEM (Security Information and Event Management) 6. กฎการตรวจจับ (Detection Rules) และการบริหารจัดการการแจ้งเตือน (Alert Management) 7. Threat Detection and Investigation 8. AI-assisted Log and Security Event Analysis
14 พ.ย (เสาร์) อบรม ณ สถาบันเทคโนโลยี ปทุมวัน *ผู้เรียนต้องนำ Laptop ส่วนตัวมาเข้าเรียน	8. Virtual Lab SOC Analyst using FortiAnalyzer 1. การบริหารจัดการ Log และสถาปัตยกรรม Security Fabric 2. การวิเคราะห์ภัยคุกคามและการสืบสวน (Threat Hunting & Investigation) 3. การตั้งค่าการแจ้งเตือนและการจัดการ Incident (Incident Management) 4. การตอบสนองภัยคุกคามอัตโนมัติ (Automation & Playbooks) 5. การสร้างรายงานเพื่อการบริหารและการทำ Compliance (Reporting)
15-20 พ.ย. วิดีโอ วิดีโอ ออนไลน์ 1 คอร์ส	9. นิติวิทยาดิจิทัล (Digital Forensics) 1. กระบวนการทางนิติวิทยาดิจิทัล (Digital Forensics Process) 2. การตรวจพิสูจน์คอมพิวเตอร์และไฟล์ (Computer and File Forensics) 3. การตรวจพิสูจน์ดิสก์และหน่วยความจำ (Disk and Memory Forensics) 4. การตรวจพิสูจน์เครือข่าย (Network Forensics) 5. หลักการทางวิทยาการอำพรางข้อมูล (Steganography)

วันกิจกรรม	รายละเอียด
22 พ.ย. (อาทิตย์) อบรม ณ สถาบันเทคโนโลยี ปทุมวัน *ผู้เรียนต้องนำ Laptop ส่วนตัวมาเข้าเรียน	10. มินิซีทีเอฟด้านนิติวิทยาดิจิทัลและทีมป้องกัน (Mini CTF: Digital Forensics and Blue Team) 1. การติดตั้งและใช้งานเครื่องมือด้านนิติวิทยาดิจิทัลและทีมป้องกัน (Digital Forensics and Blue Team) 2. การแข่งขัน Mini CTF ในหัวข้อนิติวิทยาดิจิทัลและทีมป้องกัน
22-27 พ.ย. วิดีโอ ออนไลน์ 1 คอร์ส	11. การทดสอบเจาะระบบ (Penetration Testing) 1. กระบวนการทดสอบเจาะระบบ (Penetration Testing Process) 2. การประเมินช่องโหว่ของระบบ (Vulnerability Assessment) 3. การเจาะระบบเครือข่ายและเครื่อง (Network and Machine Exploitations) 4. การเจาะระบบเว็บ (Web Exploitations) 5. หลักการเขียนโค้ดอย่างปลอดภัย (Secure Coding)
28 พ.ย. **(เสาร์)** อบรม ณ สถาบันเทคโนโลยี ปทุมวัน *ผู้เรียนต้องนำ Laptop ส่วนตัวมาเข้าเรียน	12. มินิซีทีเอฟด้านการทดสอบเจาะระบบและทีมโจมตี (Mini CTF: Penetration Testing and Red Team) 1. การติดตั้งและใช้งานเครื่องมือด้านการทดสอบเจาะระบบและทีมโจมตี (Penetration Testing and Red Team) 2. การแข่งขัน Mini CTF ในหัวข้อการทดสอบเจาะระบบและทีมโจมตี พิธีมอบประกาศนียบัตรแก่ผู้สำเร็จการฝึกอบรมตลอดหลักสูตร

3. **เอกสารรายละเอียดโครงการ** IT & Security Audit BootKamp

1. วัตถุประสงค์ของโครงการ

1. **เพื่อยกระดับและพัฒนาทักษะ** (Upskill & Reskill) มุ่งเน้นการเสริมสร้างขีดความสามารถของบุคลากรด้านการตรวจสอบระบบ IT และความมั่นคงปลอดภัย ทั้งในมิติด้านทฤษฎีและทักษะเชิงปฏิบัติการให้มีมาตรฐานสากล
2. **เพื่อสร้างบุคลากรต้นแบบและผู้นำการเปลี่ยนแปลง** (Changemakers) มุ่งพัฒนาผู้ตรวจสอบต้นแบบภายในองค์กรที่มีศักยภาพในการวางระบบตรวจสอบ ถ่ายทอดองค์ความรู้ และสร้างวัฒนธรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ที่ดีให้แก่บุคลากรอื่นในหน่วยงานอย่างเป็นรูปธรรม
3. **เพื่อสร้างเครือข่ายความร่วมมือของผู้มีศักยภาพสูง** (High-caliber Networking) พัฒนาเครือข่ายความสัมพันธ์ระหว่างบุคลากรสาย IT Audit, Security และ GRC เพื่อเป็นกลไกในการแลกเปลี่ยนองค์ความรู้ ประสบการณ์ และการต่อยอดทางวิชาชีพในอนาคต
4. **เพื่อสร้างมาตรฐานการกำกับดูแลและพื้นที่แห่งการเรียนรู้** (Governance & Innovation Space) ส่งเสริมแนวปฏิบัติที่ดีด้านการตรวจสอบและกำกับดูแล IT พร้อมพื้นที่แลกเปลี่ยนกรณีศึกษาจริง เพื่อรองรับความท้าทายด้านกฎระเบียบและภัยไซเบอร์ในยุคดิจิทัล

2. กลุ่มผู้เรียนเป้าหมาย

1. ผู้ตรวจสอบภายใน / IT Auditor ที่ต้องการกรอบมาตรฐานและระเบียบวิธีการตรวจที่เป็นระบบ
2. บุคลากรทีมความมั่นคงปลอดภัย ความเสี่ยง และการปฏิบัติตามกฎเกณฑ์ (IT / Security / GRC) จากหน่วยงานและองค์กร
3. ผู้บริหาร IT / เจ้าของระบบ ที่ต้องเตรียมความพร้อมรับการตรวจหรือการรับรองมาตรฐาน
4. ผู้เตรียมสอบใบรับรอง CISA / ISO/IEC 27001 Lead Auditor และผู้สนใจเริ่มต้นสายงานนี้
5. ผู้ดูแลระบบ / DevOps ที่ต้องเข้าใจการควบคุมและหลักฐานที่ผู้ตรวจสอบต้องการ
6. นักศึกษา / ผู้เปลี่ยนสายงาน (มีปรับพื้นฐานให้ ไม่มีพื้นฐานก็สามารถเรียนได้)

3. จุดเด่นของโครงการ

1. รูปแบบการเรียนรู้แบบผสมผสาน (Hybrid Learning) ประกอบด้วยสื่อวิดีโอเสริมความรู้ก่อนเรียน (Pre-course Video) จำนวน 4 ครั้ง เพื่อปูพื้นฐานในทุกบทเรียน ก่อนเข้าสู่การฝึกอบรมเชิงปฏิบัติการ (Onsite Workshop) แบบเข้มข้น 5 วันเต็ม โดยมีวิทยากรผู้มีประสบการณ์ตรงในสายงานตรวจสอบ IT และความมั่นคงปลอดภัยเป็นผู้กำกับดูแลตลอดหลักสูตร

2. การฝึกปฏิบัติผ่าน Workshop 5 ชุดครอบคลุมทุกขั้นตอนของงานตรวจสอบ ตั้งแต่การวางแผนตรวจสอบ (Audit Plan) การประเมินความเสี่ยงและจัดทำ Statement of Applicability (SoA) การจัดทำ Audit Checklist การจำลองตรวจหน้างาน (Fieldwork Role-play) จนถึงการเขียนรายงานผลการตรวจสอบและแผนแก้ไข

3. แม่แบบเอกสารใช้งานจริง (Ready-to-use Templates) ได้แก่ Audit Plan, Checklist, Working Papers, รายงานผลการตรวจสอบ และ Corrective Action / Follow-up Tracker ที่ผู้เรียนนำไปใช้งานได้ทันทีหลังจบหลักสูตร

4. การวัดผลเชิงพัฒนาการ (Pre-test / Post-test) เพื่อวัดความก้าวหน้าของผู้เรียนแต่ละคนอย่างเป็นรูปธรรม เหมาะสำหรับใช้รายงานผลลัพธ์การอบรมต่อผู้บริหารหรือฝ่าย HRD

4. ตารางการอบรม (รายละเอียดอาจมีการเปลี่ยนแปลงได้ตามความเหมาะสม)

ตุลาคม			พฤศจิกายน				
3-10 ต.ค. วิดีโอ ออนไลน์ 2 คอร์ส	11 ต.ค. (อาทิตย์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน	12-31 ต.ค. วิดีโอ ออนไลน์ 1 คอร์ส	1 พ.ย. (อาทิตย์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน	8 พ.ย. (อาทิตย์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน	9-14 พ.ย. วิดีโอ ออนไลน์ 1 คอร์ส	15 พ.ย. (อาทิตย์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน	22 พ.ย. (อาทิตย์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน

โครงการมีกำหนดการเรียนตั้งแต่วันที่ 11 ตุลาคม ถึงวันที่ 22 พฤศจิกายน 2569 รวมระยะเวลาทั้งสิ้น 7 สัปดาห์ ประกอบด้วย 9 หน่วยการเรียนรู้ 4 กรอบมาตรฐานสากล รวมทั้งสิ้นกว่า 30 ชั่วโมง ซึ่งการเรียนรู้ผ่านระบบออนไลน์ (Video Learning) ผู้เข้ารับการอบรมสามารถเลือกเรียนได้ตามความเหมาะสมของเวลา จำนวน 4 บทเรียน และ การฝึกอบรมเชิงปฏิบัติการ (Onsite Workshop) จำนวน 5 ครั้ง โดยกำหนดจัดขึ้น ณ สถาบันเทคโนโลยีปทุมวัน (สทป.)

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

KBank

SKILLKAMP

5. รายละเอียดหลักสูตร (รายละเอียดอาจมีการเปลี่ยนแปลงได้ตามความเหมาะสม)

วันกิจกรรม	รายละเอียด
3-10 ต.ค. วิดีโอ ออนไลน์ 2 คอร์ส	EP.1 “ตรวจ IT ไปทำไม?” เมื่อช่องโหวเดียวสร้างความเสียหายหลักล้าน EP.2 ระเบียบวิธีตรวจตามมาตรฐานที่มืออาชีพใช้
11 ต.ค. (อาทิตย์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน *ผู้เรียนต้องนำ Laptop ส่วนตัวมาเข้าเรียน	Workshop 1: รากฐาน & ระเบียบวิธีตรวจ 1. ลงทะเบียน & Pre-test 2. การตรวจ IT/Security& ภูมิทัศน์มาตรฐาน 3. หลักการตรวจประเมิน 7 ข้อ 4. การบริหารโปรแกรมการตรวจ + PDCA 5. สมรรถนะและจรรยาบรรณผู้ตรวจ 6. Workshop วางแผนการตรวจ (Audit Plan)
12-31 ต.ค. วิดีโอ ออนไลน์ 1 คอร์ส	EP.3 “เทียบกับอะไร” รู้จักเกณฑ์ ISO/IEC 27001, NIST CSF, PDPA
1 พ.ย. (อาทิตย์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน *ผู้เรียนต้องนำ Laptop ส่วนตัวมาเข้าเรียน	Workshop 2: เกณฑ์I: ISO/IEC 27001 1. ISMS และ โครงสร้างข้อกำหนด 2. การประเมินและจัดการความเสี่ยง และ Statement of Applicability (SoA) 3. Annex A — 93 มาตรการ 4 กลุ่ม 4. Workshop ประเมินความเสี่ยง และ ร่าง Statement of Applicability (SoA)
8 พ.ย. (อาทิตย์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน *ผู้เรียนต้องนำ Laptop ส่วนตัวมาเข้าเรียน	Workshop 3: เกณฑ์II: NIST CSF · PDPA ในการทำ Checklist 1. NIST CSF 2.0 (เกณฑ์ความเสี่ยงไซเบอร์) 2. PDPA & กฎหมายที่เกี่ยวข้อง (เกณฑ์compliance) 3. จากเกณฑ์สู่รายการตรวจ + การควบคุมและเทคนิคทดสอบ 4. Workshop จัดทำ Audit Checklist (แม่แบบ Excel)
9-14 พ.ย. วิดีโอ ออนไลน์ 1 คอร์ส	EP.4 จากหลักฐานสู่รายงาน: Finding, Nonconformity, Corrective Action
15 พ.ย. (อาทิตย์) อบรม ณ สถาบันเทคโนโลยีปทุมวัน *ผู้เรียนต้องนำ Laptop ส่วนตัวมาเข้าเรียน	Workshop 4: การดำเนินการตรวจ 1. เริ่มต้น & เตรียมการตรวจ และ ประชุมเปิด (Opening) 2. การเก็บและประเมินหลักฐาน 3. สร้างสิ่งที่ตรวจพบ (Findings) และ ประชุมปิด 4. Workshop จำลองการตรวจหน้างาน (Fieldwork)

วันกิจกรรม	รายละเอียด
22 พ.ย. (อาทิตย์) **อบรม ณ** **สถาบันเทคโนโลยีปทุมวัน** *ผู้เรียนต้องนำ Laptop ส่วนตัวมาเข้าเรียน	Workshop 5: การทำรายงาน, วิธีปรับแก้ไข, การติดตาม และ Capstone 1. การเขียนรายงานการตรวจสอบ 2. แนวทางการแก้ไข (Corrective Action) 3. การตรวจติดตาม (Follow-up) และ ปิดการตรวจ 4. Workshop รายงาน + CAR + Follow-up