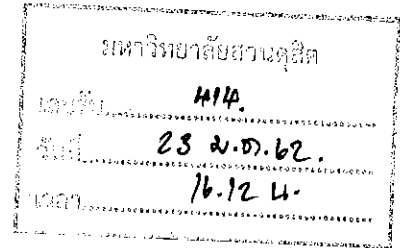


ที่ วท ๕๕๐๑/ว.๐๓๙๖

๑๔ มกราคม ๒๕๖๒

เรื่อง ขอเชิญส่งบุคลากรเข้าร่วมการฝึกอบรม
เรียน อธิการบดี
มหาวิทยาลัยสวนดุสิต

สิ่งที่ส่งมาด้วย แผ่นพับแนะนำหลักสูตร



ด้วย สถาบันวิทยาการ สวทช. สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ มีกำหนดจัดอบรม หลักสูตรเทคโนโลยีสารสนเทศและการจัดการขั้นสูง ประกอบด้วย

๑. หลักสูตรศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operations Center : SOC) รุ่นที่ ๒ อบรมระหว่างวันที่ ๕ - ๘ มีนาคม ๒๕๖๒ เวลา ๐๙.๐๐ - ๑๖.๐๐ น. ณ โรงแรมโนโวเทล แพลทินัม ประตูน้ำ วัตถุประสงค์เพื่อเสริมสร้างความรู้ แนวความคิด และหลักการของศูนย์เฝ้าระวังด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยเน้นการฝึกปฏิบัติการจัดตั้งศูนย์ฯ การจัดทำ รายงาน การวิเคราะห์ข้อมูลล็อก และการจัดเก็บหลักฐานเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อเข้าถึงและแก้ไขการบุกรุกเครือข่ายและระบบสารสนเทศต่างๆ ที่ผิดปกติอย่างรวดเร็วและมีประสิทธิภาพ

๒. หลักสูตรฝึกอบรมเชิงปฏิบัติการการจัดทำสถาปัตยกรรมระบบขององค์กร (Enterprise Architecture Workshop) รุ่นที่ ๔ อบรมระหว่างวันที่ ๑๕ - ๑๗ พฤษภาคม ๒๕๖๒ เวลา ๐๙.๐๐ - ๑๖.๐๐ น. ณ โรงแรมเซ็นจูรี พาร์ค กรุงเทพ วัตถุประสงค์เพื่อเสริมสร้างความเข้าใจ หลักการ และองค์ประกอบของสถาปัตยกรรมระบบ แนวทางการจัดทำสถาปัตยกรรมขององค์กร โดยเน้นการฝึกปฏิบัติจัดทำสถาปัตยกรรมระบบของ องค์กรจากกรณีศึกษา และสามารถต่อยอดความรู้ที่ได้กลับไปปรับใช้งานกับองค์กรของตนเองได้

๓. หลักสูตรฝึกอบรมเชิงปฏิบัติการ การบริหารจัดการความต่อเนื่องทางธุรกิจตามมาตรฐานสากล ISO 22301:2012 รุ่นที่ ๓ อบรมระหว่างวันที่ ๒๙ - ๓๑ พฤษภาคม ๒๕๖๒ เวลา ๐๙.๐๐ - ๑๖.๐๐ น. ณ โรงแรมเซ็นจูรี พาร์ค กรุงเทพ วัตถุประสงค์เพื่อเสริมสร้าง ความเข้าใจ แนวความคิดและหลักการของมาตรฐาน ISO 22301-2012 และการเตรียมความพร้อมการกู้คืนระบบงานไอทีที่มีกระบวนการออกแบบการป้องกันและ รับมือภัยคุกคามที่ซับซ้อน โดยเน้นการฝึกปฏิบัติเพื่อให้สามารถนำไปปรับใช้งานได้มีประสิทธิภาพ

๔. หลักสูตร IT Audit for Non - IT Auditor Masterclass รุ่นที่ ๑๕ อบรมระหว่างวันที่ ๑๗ - ๒๑ มิถุนายน ๒๕๖๒ เวลา ๐๙.๐๐ - ๑๖.๐๐ น. ณ โรงแรมเซ็นจูรี พาร์ค กรุงเทพ วัตถุประสงค์เพื่อเสริมสร้างศักยภาพของผู้ตรวจสอบภายใน ให้มีความรู้ ความเข้าใจ ขั้นตอนกระบวนการการตรวจสอบความเสี่ยงด้านเทคโนโลยี พร้อมทั้งสามารถวางแผนการตรวจสอบตามหลักการบริหารความเสี่ยง และสามารถ ตรวจสอบเทคโนโลยีสารสนเทศตามมาตรฐานและเทคนิคการตรวจสอบที่เกี่ยวข้อง เพื่อสนองความต้องการของผู้บริหารทุกระดับได้

ในการนี้ สถาบันฯ จึงขอเชิญท่านหรือผู้แทนเข้าร่วมการฝึกอบรมหลักสูตรดังกล่าวตามวันและเวลาข้างต้น โดยท่านสามารถพิจารณา รายละเอียดได้จากเว็บไซต์ www.NSTDAcademy.com/advancedtraining หรือสอบถามรายละเอียดเพิ่มเติมได้ที่ สถาบันวิทยาการ สวทช. หมายเลขโทรศัพท์ ๐ ๒๖๔๔ ๘๑๕๐ ต่อ ๘๑๘๙๑, ๘๑๘๙๒ ทั้งนี้ ผู้เข้าร่วมการฝึกอบรมสามารถเบิกค่าลงทะเบียนและไม่ถือเป็นวันลาตามระเบียบ กระทรวงการคลัง และค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมของบริษัทหรือหน่วยงานส่วนนิติบุคคลสามารถนำไปลดหย่อนภาษีได้ ๒๐๐%

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ



(นายศิริชัย กิตติวารพงศ์)

ผู้อำนวยการ

สถาบันวิทยาการ สวทช.

ปฏิบัติการแทนผู้อำนวยการ

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

สถาบันวิทยาการ สวทช.

โทร. ๐ ๒๖๔๔ ๘๑๕๐ ต่อ ๘๑๘๙๒ (เมธภักดิ์ วงษ์ตา)

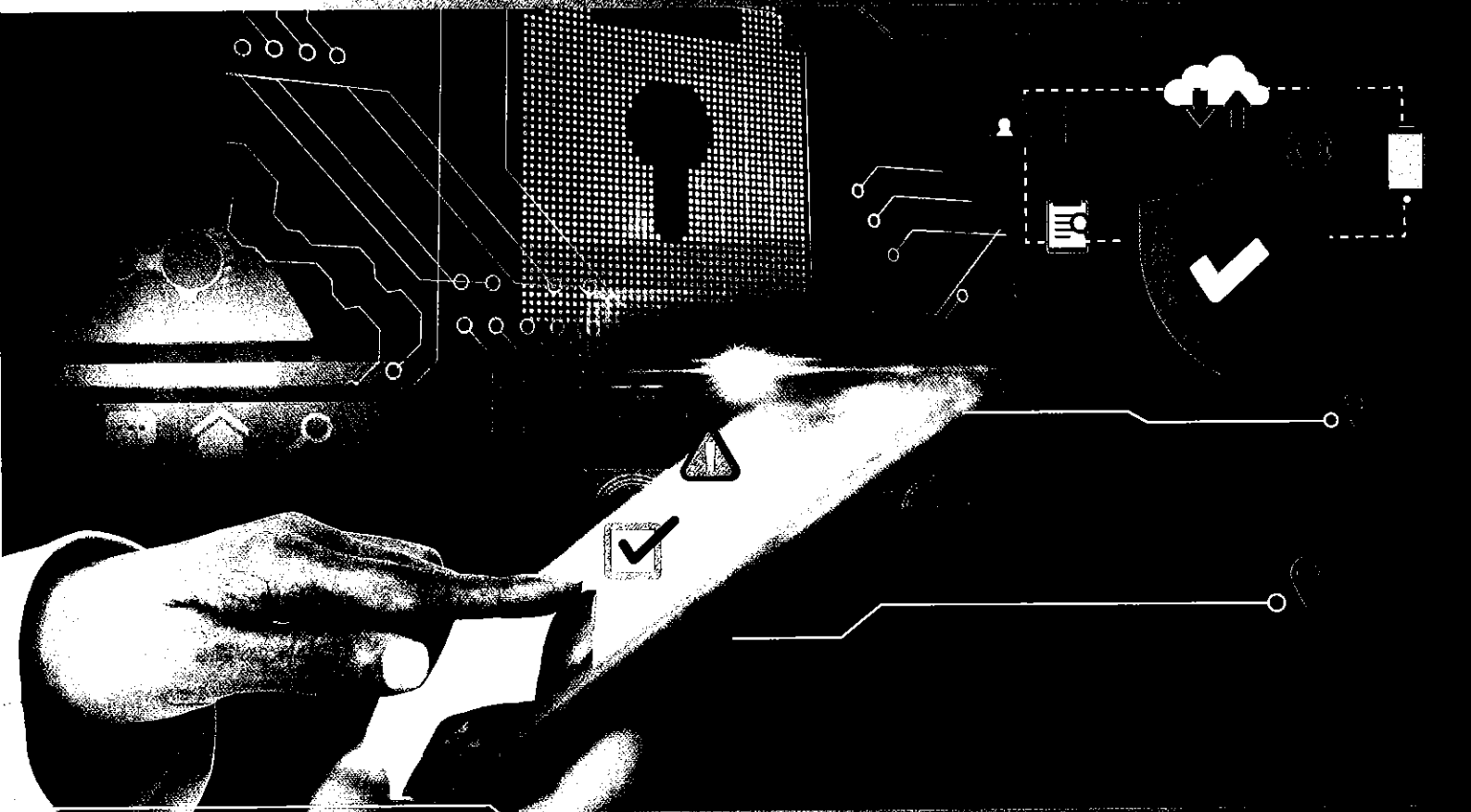
โทรสาร ๐ ๒๖๔๔ ๘๑๑๐

NPD569

หลักสูตรศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ รุ่นที่ 2

Security Operations Center: ภัยคุกคาม

มุ่งเน้นการฝึกปฏิบัติเฝ้าระวังความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (SOC) และ "ภัยคุกคาม"



Key Highlights

- ① เรียนรู้แนวทางการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศกับวิทยาการผู้ทรงคุณวุฒิด้านความมั่นคงปลอดภัยระบบสารสนเทศระดับประเทศ
- ② เจาะลึกกระบวนการปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
- ③ ฝึกปฏิบัติกับซอฟต์แวร์เชิงพาณิชย์ในระดับแนวหน้า เช่น Sprunk Arcsight เพื่อใช้ในการวิเคราะห์ข้อมูลล็อกที่เกี่ยวข้องกับการบุกรุกระบบ
- ④ ฝึกปฏิบัติเข้มข้นมากถึง 10 Workshop ในการปฏิบัติงานเฝ้าระวังความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อให้สามารถนำไปปฏิบัติได้จริงด้วยตนเอง



โครงสร้างหลักสูตร

เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับมาตรฐานในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย แนวทางการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operations Center: SOC) และฝึกปฏิบัติเข้มข้นทักษะพื้นฐานที่จำเป็นสำหรับการปฏิบัติงานภายใต้ ศูนย์ปฏิบัติการฯ ประกอบด้วย การบรรยาย การฝึกอบรมเชิงปฏิบัติการ รวมจำนวน 24 ชั่วโมง/4 วันทำการ ดังนี้

บรรยาย และกรณีศึกษา	14	2
ฝึกปฏิบัติการ (Workshop)	10	2
รวม	24	4

เนื้อหาหลักสูตร ประกอบด้วย

- มาตรฐานและกระบวนการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- กระบวนการ บทบาท และหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการเฝ้าระวังด้านความมั่นคง ปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ
- การแบ่งแยกเหตุการณ์แจ้งเตือน (Event) หรือ เหตุการณ์ด้านความมั่นคงปลอดภัยให้ชัดเจน (Security Incident)
- การประเมินผลกระทบหรือระดับความรุนแรงของเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น
- การจำลองสถานการณ์การโจมตีในรูปแบบต่างๆ เช่น SQL Injection, Cross-site Scripting (XSS), Brute Force เป็นต้น
- การติดตั้ง Agent บนระบบต่างๆ สำหรับการบันทึกข้อมูลล็อก
- การกำหนดกฎเกณฑ์ (Correlation Rules) ที่ใช้ในกาวิเคราะห์ข้อมูลจากล็อก
- การวิเคราะห์ข้อมูลจากล็อก
- การวิเคราะห์หาสาเหตุของเหตุการณ์ด้านความมั่นคงปลอดภัย
- การจัดเก็บหลักฐานด้านคอมพิวเตอร์จากข้อมูลล็อกที่จัดเก็บไว้
- การวิเคราะห์หรือตรวจสอบข้อมูลในระบบที่ถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต
- การจัดทำรายงานประเภทต่างๆ ที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัย ได้แก่ การแจ้งเตือนประเภทต่างๆ (Alert) และรายงานประเภทสถิติต่างๆ (Dashboard) ที่จำเป็นต่อการใช้งาน
- การใช้เครื่องมือและจัดเก็บข้อมูลล็อกให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยขององค์กร ตลอดจนกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง
- การวิเคราะห์หาช่องโหว่ในระบบคอมพิวเตอร์ เพื่อตรวจสอบหาช่องทางการบุกรุกหรือการเข้าถึงเครือข่ายและระบบสารสนเทศที่ผิดปกติ และหาแนวทางป้องกันระบบ
- การใช้เครื่องมือในการเฝ้าระวังและติดตามการทำงานของระบบและอุปกรณ์ต่างๆ

หลักสูตรนี้เหมาะสำหรับ

- ผู้ปฏิบัติงานในศูนย์ปฏิบัติการป้องกันและระงับเหตุความมั่นคงปลอดภัย (เช่น CERT NOC เป็นต้น)
- ผู้ดูแลระบบ
- ผู้ดูแลเครือข่าย
- ผู้จัดการด้านไอที
- ผู้ปฏิบัติงานที่เกี่ยวข้องกับการเฝ้าระวังระบบและอุปกรณ์ต่างๆ ขององค์กร

ค่าลงทะเบียน

ท่านละ 34,900 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)
 “พิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไปรับส่วนลดทันที 10% เหลือชำระเพียงท่านละ 31,410 บาท (ออกใบเสร็จรับเงินรวมกัน 1 ใบ)

ระยะเวลาของหลักสูตร

ระหว่างวันที่ 5 - 8 มีนาคม 2562
 เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 4 วัน)

สถานที่ฝึกอบรม

โรงแรมโนโวเทล กรุงเทพ
 แพลตทินัม ประตูน้ำ

วิทยากรประจำหลักสูตร



ดร. บรรจง หะรังษี
 รองกรรมการผู้จัดการ และที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ บริษัท ที-เน็ต จำกัด
 ISO/IEC 27001 (Certified of Lead auditor),
 ISO/IEC 20000 (Auditor Certificate) BCMS 25999,
 Introduction to Capability Maturity Model Integration V1.2 Certificate

นายเจษฎา ทองกันเหลือง
 ผู้จัดการฝ่ายความมั่นคงปลอดภัย บริษัท ที-เน็ต จำกัด
 Cisco Certified Network Associate (CCNA),
 Certified Ethical Hacker (CEH),
 Certified Hacking Forensic Investigator (CHFI),
 Certified Security Analyst (ECSA),
 Peplink Certified Engineer (PCE),
 Peplink Sales Specialist (PSS), CompTIA Network+,
 CompTIA CySA+

หมายเหตุ:
 1. สถาบันวิชาการ สวทช. ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการศึกษา
 2. ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ <http://www.NSTDAAcademy.com/soc>



EAW

Enterprise Architecture Workshop ชุดที่ 4

หลักสูตรฝึกอบรมเชิงปฏิบัติการการจัดการจัดทำสถาปัตยกรรมระบบขององค์กร

มุ่งเน้นฝึกปฏิบัติการจัดทำสถาปัตยกรรมระบบ ที่ครอบคลุมทั้ง 4 ระดับ

ได้แก่ กระบวนการ ข้อมูล ระบบงาน และเทคโนโลยีสารสนเทศ

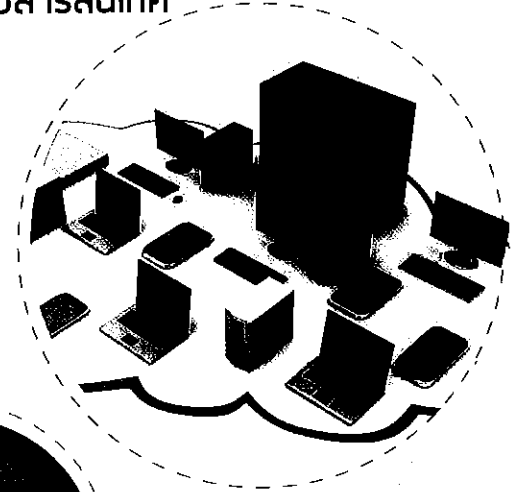
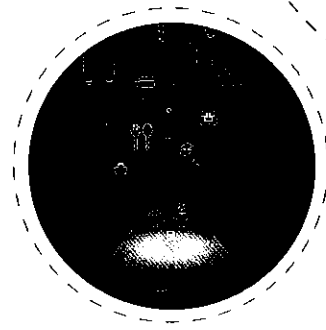


Image ref: <http://www.consortworld.com/>
Image ref: Selected by freepik

Key Highlights

- เรียนรู้หลักการสร้างสถาปัตยกรรมระบบด้านเทคโนโลยีสารสนเทศ เพื่อเพิ่มประสิทธิภาพในการบริหารจัดการตามยุทธศาสตร์ขององค์กร
- เข้าใจการจัดทำสถาปัตยกรรมระบบที่บูรณาการด้านเทคโนโลยีสารสนเทศเข้ากับกระบวนการธุรกิจอย่างเป็นระบบเพื่อการเติบโตของธุรกิจอย่างต่อเนื่องและยั่งยืน
- เห็นความสัมพันธ์ระหว่างสถาปัตยกรรมระบบกับแผนกลยุทธ์ด้านไอซีที เพื่อการบรรลุวิสัยทัศน์และพันธกิจขององค์กร พร้อมกรณีศึกษา
- เจาะลึกแนวทางการกำกับดูแลสถาปัตยกรรมระบบ บทบาทหน้าที่ของผู้รับผิดชอบ และกระบวนการที่เกี่ยวข้อง
- แนะนำ Software Tools ประเภท Open Source และการใช้งาน สำหรับการจัดทำสถาปัตยกรรมระบบ
- ฝึกปฏิบัติเข้มข้นการจัดทำสถาปัตยกรรมระบบจากกระบวนการและระบบงานทางธุรกิจ
ที่ใช้เป็นกรณีศึกษา พร้อมทั้งร่วมอภิปรายแพร่ประสบการณ์เพื่อการนำไปใช้ได้จริงในองค์กร



หลักสูตรฝึกอบรมเชิงปฏิบัติการการจกทำสถาปัตยกรรมระบบขององค์กร

การขับเคลื่อนธุรกิจที่ยั่งยืนจำเป็นต้องพึ่งพาเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ การวางแผนความเชื่อมโยงระหว่างเทคโนโลยีสารสนเทศ (Information Technology) กับธุรกิจ (Business) จึงเป็นสิ่งสำคัญที่หลาย องค์กรมองข้ามไป ซึ่งเป็นผลทำให้เกิดความล้มเหลวของการใช้เทคโนโลยีสารสนเทศในองค์กรตามมา เช่น การใช้เทคโนโลยีสารสนเทศไม่เต็มประสิทธิภาพ เกิดการลงทุนที่ซ้ำซ้อน ไม่สอดคล้องและไม่ตอบโจทย์กับวิสัยทัศน์ขององค์กร

การจัดทำสถาปัตยกรรมระบบขององค์กรเป็นการบูรณาการระบบเทคโนโลยีสารสนเทศเข้ากับธุรกิจอย่างเป็นระบบ ซึ่งก่อให้เกิดแผนกลยุทธ์ด้านระบบเทคโนโลยีสารสนเทศทั้งระยะสั้นและระยะยาว โดยแสดงให้เห็นความเชื่อมโยงกันใน 4 ระดับ ระหว่าง กระบวนการทางธุรกิจ (Business Processes) ข้อมูล (Data) ระบบงาน (Application) และ เทคโนโลยีสารสนเทศสนับสนุน (Related Information technology) ที่รองรับกับความต้องการของผู้ที่เกี่ยวข้องทั้งปัจจุบันและอนาคต สามารถผลักดันให้องค์กรดำเนินการตามนโยบายและวิสัยทัศน์ขององค์กรที่กำหนดไว้ได้

หลักสูตรนี้มีจุดมุ่งหมายให้ผู้เข้าร่วมอบรมเข้าใจหลักการและองค์ประกอบของสถาปัตยกรรมระบบ ทราบแนวทางการจัดทำสถาปัตยกรรมระบบขององค์กร ฝึกปฏิบัติจัดทำสถาปัตยกรรมระบบขององค์กรจากกรณีศึกษา และสามารถต่อยอดความรู้ที่ได้กลับไปปรับใช้งานกับองค์กรของตนเองได้

หลักสูตรนี้เหมาะสำหรับ

- ผู้บริหารด้านไอซีทีในทุกระดับ หัวหน้าศูนย์เทคโนโลยีสารสนเทศ ผู้จัดการด้านไอซีที
- เจ้าหน้าที่ทางเทคนิคด้านไอซีที เช่น ผู้วิเคราะห์และออกแบบระบบ ผู้พัฒนาระบบ ผู้ดูแลระบบ ผู้ดูแลเครือข่าย
- เจ้าหน้าที่ฝ่ายแผนงานขององค์กร
- ผู้ตรวจสอบไอซีที

วิทยากรประจำหลักสูตร



ดร.บรจจ หะรังษี

ที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ บริษัท ที-เน็ต จำกัด

ISO/IEC 27001 (Certified of Lead auditor),

ISO/IEC 20000 (Auditor Certificate) BCMS 25999,

Introduction to Capability Maturity Model Integration

V1.2 Certificate

ค่าลงทะเบียน

ท่านละ 24,500 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

พิเศษ!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 คนขึ้นไป

รับส่วนลดทันที 10% เหลือชำระเพียงท่านละ 22,050 บาท

(ออกใบเสร็จรับเงินรวมกัน 1 ใบ)

ระยะเวลาของหลักสูตร

อบรมระหว่างวันที่ 15-17 พฤษภาคม 2562

เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม 3 วัน)

เนื้อหาหลักสูตร ประกอบด้วย

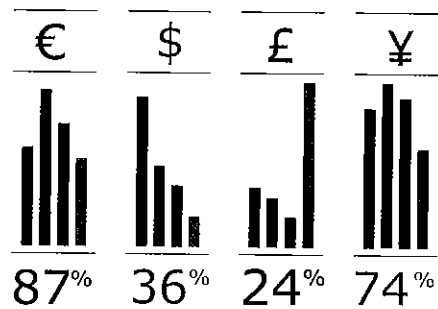
- ทฤษฎี หลักการ และองค์ประกอบของสถาปัตยกรรมระบบ ความสำคัญและความจำเป็นของการมีสถาปัตยกรรมระบบขององค์กร
- กระบวนการวางแผนกลยุทธ์ด้านไอซีทีกับการจัดทำสถาปัตยกรรมระบบขององค์กร
- แนวทางการกำกับดูแลสถาปัตยกรรมระบบขององค์กร ผู้รับผิดชอบ และหน้าที่ความรับผิดชอบ
- กรณีศึกษาการวางแผนกลยุทธ์ด้านไอซีทีกับการจัดทำสถาปัตยกรรมระบบขององค์กร โดยมีการจัดลำดับโครงการด้านระบบงานตามลำดับความสำคัญของโครงการในการบรรลุซึ่งวิสัยทัศน์และพันธกิจขององค์กร
- การแนะนำ Software Tools และการใช้งาน Software สำหรับใช้ในการจัดทำสถาปัตยกรรมระบบ
- การฝึกปฏิบัติการจัดทำสถาปัตยกรรมระบบขององค์กรร่วมกับซอฟต์แวร์ ที่สามารถนำไปปฏิบัติได้จริง

หมายเหตุ

ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

สถานที่อบรม

โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ



ศึกษารายละเอียดเพิ่มเติมได้ที่ <http://www.nstdaacademy.com/eaw>

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0-2644-0180 ต่อ 61891, 61892

อีเมล: qa@nstda.ac.th

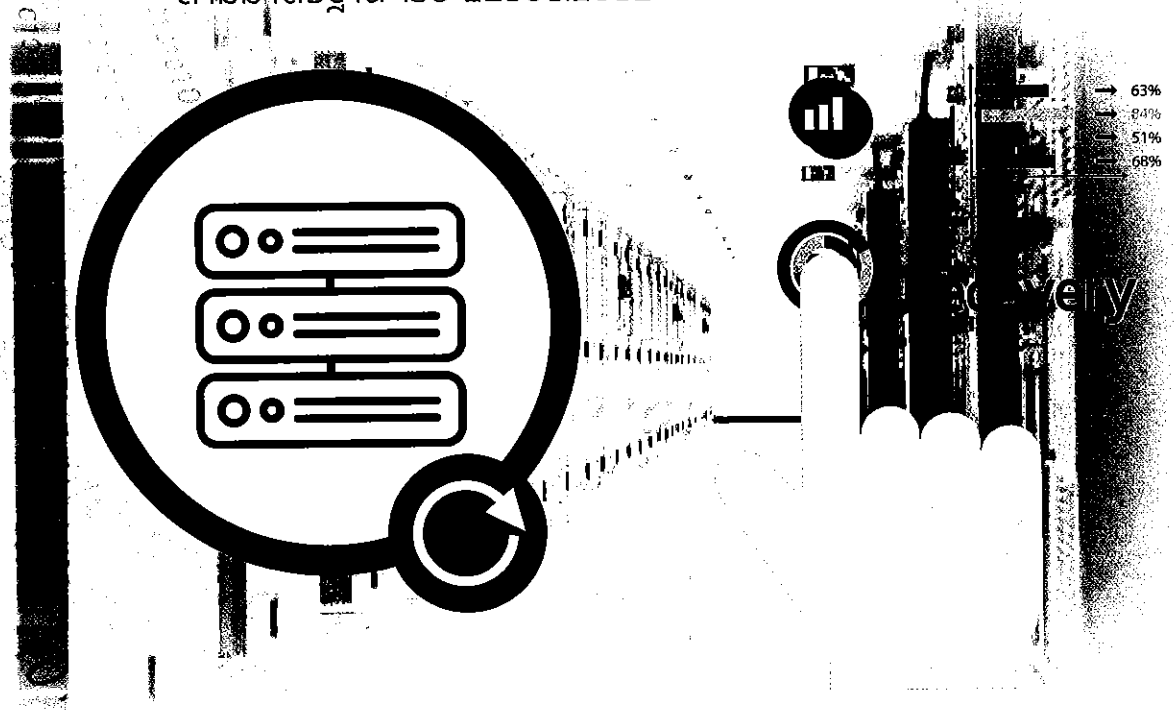
หลักสูตรฝึกอบรมเชิงปฏิบัติการ

การบริหารจัดการความต่อเนื่องทางธุรกิจตามมาตรฐานสากล ISO 22301:2012

BCS | Business Continuity Management Standard

รุ่นที่ 3

มุ่งเน้นการเตรียมความพร้อมเรื่องการกู้คืนระบบงาน และการรับมือกับเหตุการณ์หยุดชะงัก หรือสภาวะวิกฤติ เพื่อให้เกิดความต่อเนื่องในกระบวนการบริหารจัดการงาน ตามมาตรฐาน ISO 22301:2012



Key Highlights

- เจาะลึก ISO 22301:2012 มาตรฐานสากลหลักที่ใช้ในการอ้างอิงและบริหารจัดการความต่อเนื่องทางธุรกิจ เพื่อการบริหารจัดการภัยคุกคามแบบองค์รวม
- ทราบหลักการประเมินความเสี่ยง ผลกระทบ การกำหนดลำดับของงานในการกู้คืนระบบ ตลอดจนการกำหนดระยะเวลา เป้าหมายในการกู้คืนระบบงานที่เหมาะสม
- วางแผนเตรียมความพร้อมด้านกลยุทธ์ในการป้องกันหรือรับมือกับเหตุวิกฤติ หรือภัยพิบัติ เพื่อลดความเสียหาย สร้างความยืดหยุ่น และสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง
- เรียนรู้วิธีการจัดทำแผนกู้คืนระบบงาน (Business Continuity Plan) และแผนรับมือกับเหตุการณ์หยุดชะงักที่เกิดขึ้น (Incident Management Plan) โดยอ้างอิงตามมาตรฐาน ISO 22301:2012
- ฝึกปฏิบัติเข้มข้นกว่า 10 Workshop กับกรณีศึกษาที่สามารถนำกลับไปประยุกต์ใช้งานได้จริงในองค์กร



โครงสร้างหลักสูตร

การดำเนินธุรกิจในปัจจุบันจำเป็นต้องพึ่งพาระบบงานไอทีมาสนับสนุนในการบริหารจัดการ เพื่อให้องค์กรสามารถดำเนินการไปได้อย่างรวดเร็วและมีประสิทธิภาพ แต่ด้วยปัจจัยการเปลี่ยนแปลงที่รวดเร็ว และความไม่แน่นอนของสถานการณ์ที่ไม่สามารถคาดการณ์ได้ ไม่ว่าจะเป็นสถานการณ์น้ำท่วม ไฟไหม้ หรือถูกปิดล้อมโดยฝูงชน หากระบบงานหรือบุคลากรหยุดทำงานเป็นระยะเวลาสั้นเกินกว่าระยะเวลาที่รับได้ จะก่อให้เกิดความเสียหายและส่งผลกระทบต่อการทำงานดำเนินธุรกิจ ชื่อเสียง ภาพลักษณ์ ความเชื่อมั่น และกิจกรรมที่สร้างมูลค่าเพิ่มให้กับองค์กร ดังนั้นหลายองค์กรจึงได้ให้ความสำคัญกับการเตรียมพร้อมในการรับมือกับเหตุการณ์ สภาวะวิกฤติ หรือภัยคุกคามที่อาจเกิดขึ้น และเตรียมพร้อมในเรื่องของการกู้คืนระบบงานไอทีให้กลับคืนมาดำเนินการกิจกรรมได้ภายในระยะเวลาที่เหมาะสม

หลักสูตรนี้มุ่งเน้นให้ผู้เรียนเข้าใจแนวคิดและหลักการของมาตรฐาน ISO 22301:2012 ซึ่งเป็นมาตรฐานสากลที่ใช้ในการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management Systems) ในการชี้แจงภัยคุกคาม เพื่อนำมาปรับปรุงประสิทธิภาพและสร้างกลไกเตรียมความพร้อมเรื่องการกู้คืนระบบงานไอทีในองค์กรที่มีความซับซ้อนในการออกแบบกระบวนการป้องกันและรับมือกับภัยคุกคาม นอกจากนี้หลักสูตรนี้ยังได้กำหนดให้มีการฝึกปฏิบัติตามกรณีศึกษาโดยผู้เรียนสามารถนำแผนกู้คืนระบบงานขององค์กรมาฝึกปฏิบัติได้ ซึ่งจะช่วยให้เข้าใจภาพรวมทั้งหมดของการกู้คืนระบบงานไอทีและสามารถต่อยอดความรู้ที่ได้กลับไปปรับใช้ทำงานกับองค์กรของตนเองได้อย่างมีประสิทธิภาพ

หลักสูตรนี้เหมาะสำหรับ

- ผู้บริหารด้านไอซีทีในทุกระดับ
- หัวหน้าศูนย์เทคโนโลยีสารสนเทศ
- ผู้จัดการด้านไอซีที
- เจ้าหน้าที่ทางเทคนิคด้านไอซีที เช่น ผู้วิเคราะห์และออกแบบระบบ ผู้พัฒนาระบบ ผู้ดูแลระบบ ผู้ดูแลเครือข่าย
- ผู้ตรวจสอบไอซีที

สิ่งที่คาดว่าจะได้รับ

- ผู้เข้าร่วมอบรมจะได้รับความรู้ที่สามารถนำไปใช้ในการปฏิบัติงานจริง ได้แก่
 - การนำบริบทขององค์กร หรือสภาพขององค์กรที่เป็นอยู่ในปัจจุบันมาใช้เป็นประเด็นสำคัญในการวางแผนงานสำหรับการบริหารความต่อเนื่องทางธุรกิจ
 - การกำหนด Scenario ซึ่งเป็นเหตุการณ์ความเสี่ยงที่ส่งผลกระทบต่อหยุดชะงักของระบบงานสำคัญขององค์กร
 - การประเมินผลกระทบกระเ็นระบบงานสำคัญขององค์กรเกิดการหยุดชะงัก
 - การกำหนดลำดับของงานในการกู้คืนระบบ
 - การกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบ
 - การประเมินความเสี่ยงเพื่อบริหารจัดการกับเหตุต่างๆ ที่จะทำให้เกิดการหยุดชะงัก
 - การระบุทรัพยากรที่จำเป็นสำหรับการกู้คืนระบบงาน
 - การจัดทำแผนการรับมือหรือจัดการกับเหตุหยุดชะงัก
 - การจัดทำแผนกู้คืนระบบ
 - การซ้อมการกู้คืนระบบ
 - การจัดทำแผนการสื่อสารในระหว่างที่เกิดเหตุ

หัวข้อการอบรม

- ISO 22301:2012 Requirements and Frameworks
- Scope of BCMS (Business Continuity Management System)
- Addressing Risks and Opportunities
- Business Impact Analysis (BIA)
- Sequence of IT Operations
- Risk Assessment
- Business Continuity Strategy
- Establishing and Implementing Procedures
- Exercising and Testing Plan Development

หมายเหตุ: ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% จึงจะได้รับวุฒิบัตรจาก สถาบันวิทยาการ สวทช.

ระยะเวลาของหลักสูตร

อบรมระหว่างวันที่ 29-31 พฤษภาคม 2562
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม 3 วัน)

ค่าลงทะเบียน

ท่านละ 23,000 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)
พิเศษ !! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 คนขึ้นไป
รับส่วนลดทันที 10% เหลือชำระเพียงท่านละ 20,700 บาท
(ออกใบเสร็จรับเงินรวมกัน 1 ใบ)

สถานที่อบรม

โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ



ดร. บรรจง หะรังษี

ที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ
บริษัท ที-เน็ต จำกัด

ISO/IEC 27001 (Certified of Lead auditor),

ISO/IEC 20000 (Auditor Certificate) BCMS 25999,

Introduction to Capability Maturity Model Integration

V1.2 Certificate

ศึกษารายละเอียดเพิ่มเติมได้ที่ <http://www.nstdaacademy.com/bcs>

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891, 81892 Email: npd@nstda.or.th

ITA

รุ่นที่ 14

IT AUDIT FOR NON - IT AUDITOR MASTERCLASS

การบูรณาการ IT Audit และ General Audit ให้เป็นหนึ่งเดียว
เพื่อเพิ่มประสิทธิภาพการตรวจสอบที่ยั่งยืน



วิทยากรผู้เชี่ยวชาญ



อาจารย์เมธา สุวรรณสาร
Audit Chair
ISACA



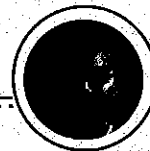
ดร. บรรจง ทะรังษี
IT Security Advisor
T-NET



อาจารย์ภิญโญ ตรีเพชรกรณ์
ผู้อำนวยการฝ่าย
Enterprise Risk Service
Deloitte



อาจารย์พิทักษ์พงษ์ อินเสื่อ
ผู้จัดการฝ่ายฝึกอบรม/
ผู้ตรวจประเมินมาตรฐาน
URS Thailand



ดร. ชยากร ปิยะบัณฑิตกุล
ผู้เชี่ยวชาญ
สวทช.

หลักสูตรนี้เหมาะสำหรับ

- ผู้ตรวจสอบภายในจากหน่วยงานภาครัฐ รัฐวิสาหกิจ และภาคเอกชน
- ผู้บริหารระดับกลางที่เกี่ยวข้องกับกระบวนการตรวจสอบ
- บุคคลสาขาอาชีพอื่นที่สนใจเป็นผู้ตรวจสอบภายใน
- บุคคลทั่วไปที่มีความสนใจในกระบวนการตรวจสอบภายใน และการบริหารเชิงรุก



“การบูรณาการ IT Audit และ General Audit ให้เป็นหนึ่งเดียว เพื่อเพิ่มประสิทธิภาพการตรวจสอบที่ยั่งยืน”

ปัจจุบันเทคโนโลยีสารสนเทศเข้ามามีบทบาทในกระบวนการดำเนินงานธุรกิจในทุกภาคส่วนทั้งหน่วยงานภาครัฐและเอกชน ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Auditor) จึงมีบทบาทสำคัญในการช่วยประเมินและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงาน ในทางปฏิบัติ พบว่าบุคลากรที่ทำหน้าที่ตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศส่วนมากเป็นผู้ตรวจสอบภายในทั่วไปที่ไม่มีพื้นฐานความรู้ด้านเทคโนโลยีสารสนเทศ ขาดทักษะ ความรู้ ความเข้าใจ องค์ความรู้และเครื่องมือต่างๆ ที่ช่วยในการตรวจสอบระบบเทคโนโลยีสารสนเทศ รวมถึงการจัดทำรายงานเสนอแนะเพื่อควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร

หลักสูตร IT Audit for Non - IT Auditor Masterclass มุ่งเน้นเสริมสร้างศักยภาพของผู้ตรวจสอบภายในให้มีความรู้ความเข้าใจในขั้นตอน กระบวนการ การตรวจสอบความเสี่ยงด้านเทคโนโลยี เรียนรู้มาตรฐานต่างๆ และเครื่องมือที่เกี่ยวข้อง เพื่อหลอมรวมการตรวจสอบทั่วไปและการตรวจสอบด้านเทคโนโลยีสารสนเทศเข้าไว้ด้วยกันเป็น Integrated Auditing

หลักสูตรนี้เหมาะสำหรับ

- ผู้ตรวจสอบภายในจากหน่วยงานภาครัฐ รัฐวิสาหกิจ และภาคเอกชน
- ผู้บริหารระดับกลางที่เกี่ยวข้องกับกระบวนการตรวจสอบ
- บุคคลสาขาอาชีพอื่นที่สนใจเป็นผู้ตรวจสอบภายใน และผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ
- บุคคลทั่วไปที่มีความสนใจในกระบวนการตรวจสอบภายใน และการบริหารเชิงรุก

สิ่งที่จะได้รับ

ในการอบรมครั้งนี้ผู้เข้าอบรมจะได้รับ

- ความรู้ความเข้าใจในบทบาทหน้าที่และความรับผิดชอบของผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศตามหลักการบริหารความเสี่ยงยุคใหม่
- ความรู้ความเข้าใจขั้นตอนและกระบวนการการตรวจสอบด้านเทคโนโลยีตามหลักการบริหารความเสี่ยง
- แนวทางการวางแผนการตรวจสอบภายในตามหลักการบริหารความเสี่ยงทั่วไปและด้านเทคโนโลยีสารสนเทศที่มีผลกระทบต่อการบริหารธุรกิจขององค์กร
- แนวปฏิบัติงานตรวจสอบเทคโนโลยีสารสนเทศโดยใช้เทคนิคการตรวจสอบและมาตรฐานที่เกี่ยวข้อง

หัวข้อการอบรม

- เทคโนโลยีสารสนเทศสำหรับผู้ตรวจสอบ
- บทบาทหน้าที่ของผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Auditor)
- การตรวจสอบเทคโนโลยีสารสนเทศตามหลักธรรมาภิบาล
- แนวปฏิบัติงานตรวจสอบด้านเทคโนโลยีสารสนเทศ
- ISO 27001:2013 กับการบริหารความเสี่ยงเทคโนโลยีสารสนเทศ
- แนวทางการตรวจประเมินตามมาตรฐาน ISO 19011 และประสบการณ์การตรวจสอบด้านเทคโนโลยีสารสนเทศ
- Integrated Audit in Practice

ค่าลงทะเบียน

21,400 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

สถานที่อบรม

โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ
เลขที่ 9 ถนนราชปรารภ แขวงประตูน้ำ เขตดินแดง กรุงเทพฯ

ระยะเวลาหลักสูตร

ระหว่างวันที่ 17-21 มิถุนายน 2562
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม 5 วัน)

ศึกษารายละเอียดเพิ่มเติมได้ที่ www.nstdaacademy.com/ita

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891, 81892

Email: npd@nstda.or.th