

ที่ อว 6001/ว 653

22 มกราคม 2568

มหาวิทยาลัยราชภัฏเชียงใหม่
เลขรับ 3440
วันที่ ๑๐ มี.ค. ๒๕๖๘
เวลา 13.05 น.

เรื่อง ขอเชิญส่งบุคลากรเข้าร่วมการฝึกอบรม
เรียน อธิการบดี มหาวิทยาลัยราชภัฏเชียงใหม่
สิ่งที่ส่งมาด้วย แผ่นพับแนะนำหลักสูตร

ด้วยสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) โดยสถาบันพัฒนาบุคลากรแห่งชาติ มีกำหนดจัดฝึกอบรมหลักสูตรด้าน
เทคโนโลยีสารสนเทศและการจัดการขั้นสูง ดังนี้

1. หลักสูตรฝึกอบรมเชิงปฏิบัติการ การเขียนข้อกำหนดและขอบเขตงานสำหรับสินค้า/บริการดิจิทัล ให้จัดซื้อและตรวจรับได้ง่าย (Terms of Reference (TOR) Writing Guide for Purchasing Digital Devices and Services) รุ่นที่ 6 ระหว่างวันที่ 26 - 27 มิถุนายน 2568 เวลา 9.00 - 16.00 น. ณ โรงแรม เซ็นจูรี พาร์ค กรุงเทพฯ โดยมีเนื้อหามุ่งเน้นให้ผู้เข้าร่วมอบรมได้เรียนรู้เกี่ยวกับสาระสำคัญของพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 เข้าใจเทคโนโลยี สินค้า/บริการดิจิทัล และแนวทางในการเขียน TOR อย่างถูกต้องและเหมาะสม พร้อมทั้งฝึกปฏิบัติการเขียน TOR สำหรับการจัดหาสินค้า/บริการดิจิทัล เพื่อให้จัดซื้อและตรวจรับได้ง่าย

2. หลักสูตรศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operations Center: SOC) รุ่นที่ 5 ระหว่างวันที่ 22 - 25 กรกฎาคม 2568 เวลา 9.00 - 16.00 น. ณ โรงแรมเซ็นจูรี พาร์ค กรุงเทพฯ โดยมีเนื้อหามุ่งเน้นเสริมสร้างความรู้ แนวความคิด และหลักการของศูนย์เฝ้าระวังด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยเน้นการฝึกปฏิบัติการจัดตั้งศูนย์ฯ การจัดทำรายงาน การวิเคราะห์ข้อมูลล็อก และการจัดเก็บหลักฐานเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อเข้าถึงและแก้ไขการบุกรุกเครือข่ายและระบบสารสนเทศต่าง ๆ ที่ผิดปกติอย่างรวดเร็วและมีประสิทธิภาพ

3. หลักสูตรมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยบนระบบคลาวด์ ตามมาตรฐาน CSA 4.x และ ISO/IEC 27001:2022 (Cloud Security Standard: CSS) รุ่นที่ 6 ระหว่างวันที่ 13 - 15 สิงหาคม 2568 เวลา 9.00 - 16.00 น. ณ โรงแรมเซ็นจูรี พาร์ค กรุงเทพฯ โดยมีเนื้อหามุ่งเน้นให้ผู้เข้าอบรมทราบแนวทางและวิธีการนำระบบงานขึ้นคลาวด์ให้มีความมั่นคงปลอดภัยตามมาตรฐาน CSA 4.x และ ISO/IEC 27001: 2022 ระบบบริหารจัดการฐานข้อมูล ระบบบริหารจัดการเว็บ ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้อง แอปพลิเคชันของระบบงาน จนกระทั่งสามารถใช้งานระบบได้ โดยสามารถนำแนวทางดังกล่าวไปต่อยอดหรือปรับใช้กับระบบงานของตนเองได้อย่างมีประสิทธิภาพ

ในการนี้ สวทช. จึงขอเชิญท่านหรือบุคลากรในสังกัดเข้าร่วมฝึกอบรมในหลักสูตรดังกล่าว ตามวัน เวลา และสถานที่ข้างต้น โดยท่านสามารถพิจารณารายละเอียดเพิ่มเติมได้จากเว็บไซต์ <https://www.career4future.com> หรือสอบถามเพิ่มเติมได้ที่ สถาบันพัฒนาบุคลากรแห่งอนาคต หมายเลขโทรศัพท์ 0 2644 8150 ต่อ 81892 และ 81904 โดยผู้เข้าร่วมอบรมจากหน่วยงานราชการสามารถเบิกค่าลงทะเบียนจากต้นสังกัดได้ตามระเบียบกระทรวงการคลัง และไม่ถือเป็นวันลาเมื่อได้รับการอนุมัติจากผู้บังคับบัญชา ทั้งนี้ ค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมของบริษัทหรือห้างหุ้นส่วนนิติบุคคลสามารถนำไปลดหย่อนภาษีได้ 200%

จึงเรียนมาเพื่อโปรดพิจารณา
หนังสือนี้ใช้ลายมือชื่ออิเล็กทรอนิกส์ซึ่งมีผลใช้บังคับได้

เรียน อธิการบดี
 เพื่อโปรดทราบ
 เพื่อโปรดพิจารณา
เห็นควร...
.....

ขอแสดงความนับถือ
กัญญา อุดมวิทิต
(นางสาวกัญญา อุดมวิทิต)
รองผู้อำนวยการ

๑ - นสทช. (๑)
- มอว ราชภัฏเชียงใหม่
สวทช. ภาชนท.,
Fak

(นายณทศภัต นาคะรัมย์)

รักษาการในตำแหน่งหัวหน้างานบริหารทั่วไป สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

สำนักงานกลาง 10 มี.ค. 2568
สถาบันพัฒนาบุคลากรแห่งอนาคต
โทรศัพท์ 0 2644 8150 ต่อ 81892 (เมธภัค) หรือ 08 5211 9709
โทรสาร 0 2644 8110

รักษาการแทนผู้อำนวยการ (รองศาสตราจารย์ ดร.ชาติรี มณีโกศล)
รักษาราชการแทน
อธิการบดีมหาวิทยาลัยราชภัฏเชียงใหม่
11 มี.ค. 2568

(นายสยาม กันทาสีลา) 10 มี.ค. 68
รักษาการในตำแหน่งผู้อำนวยการกองกลาง

NPD1-279

Investment	100
Cost	100
Profit	0

1. Investment
 2. Cost
 3. Profit

1. Investment
 2. Cost
 3. Profit

1. Investment
 2. Cost
 3. Profit



TOR

Terms of Reference (TOR) Writing Guide for Purchasing Digital Devices and Services

หลักสูตรฝึกอบรมเชิงปฏิบัติการ
การเขียนข้อกำหนดและขอบเขตงาน
สำหรับสินค้า/บริการดิจิทัล ให้จัดซื้อและตรวจรับได้ง่าย รุ่นที่ 6



“มุ่งเน้นการเขียน TOR เพื่อจัดหาสินค้า/บริการดิจิทัล ให้จัดซื้อและตรวจรับได้ง่าย”

Key Highlights

- ① เรียนรู้และเข้าใจสาระสำคัญของพระราชบัญญัติการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐ พ.ศ. 2560
- ① เข้าใจเทคโนโลยี สินค้า/บริการดิจิทัล และแนวทางในการเขียน TOR อย่างถูกต้องและเหมาะสม
- ① ฝึกปฏิบัติเข้มข้น การเขียน TOR การจัดหาสินค้า/บริการดิจิทัล เพื่อให้จัดซื้อและตรวจรับได้ง่าย



หลักสูตรฝึกอบรมเชิงปฏิบัติการ การเขียนข้อกำหนดและขอบเขตงาน สำหรับสินค้า/บริการดิจิทัล ให้จัดซื้อและตรวจรับได้ง่าย รุ่นที่ 6 (Terms of Reference (TOR) Writing Guide for Purchasing Digital Devices and Services)

ในปัจจุบันวิทยาศาสตร์และเทคโนโลยีมีความก้าวหน้าเป็นอย่างมาก มีความสำคัญต่อการทำงานในยุคเศรษฐกิจดิจิทัลที่ต้องพึ่งพาระบบงานที่ทันสมัย รวดเร็ว เข้าถึงได้ง่าย ประกอบกับรัฐบาลมีนโยบายที่จะแปรรูปบริการของรัฐทั้งหมดให้เป็นรัฐบาลดิจิทัล ในปี 2566-2570 หน่วยงานรัฐทุกหน่วยจึงต้องปรับตัวเพื่อให้สามารถตอบสนองต่อสังคมเศรษฐกิจดิจิทัลได้อย่างทันต่่วงที่ โดยในการให้บริการต่าง ๆ ที่กล่าวมานี้ จะต้องมีเครื่องมือที่ทันสมัยและใช้งานได้อย่างมีประสิทธิภาพสูงสุด สามารถตอบสนองการเปลี่ยนแปลงได้อย่างต่อเนื่อง ซึ่งหน่วยงานภาครัฐจำเป็นต้องจัดหาสินค้า/บริการดิจิทัลที่จะนำมาใช้เพื่อตอบสนองงานต่าง ๆ ผ่านการจัดซื้อ จัดจ้าง เช่น อยู่เป็นจำนวนมาก

ดังนั้นเพื่อให้การจัดซื้อ จัดจ้าง เช่น สินค้า/บริการดิจิทัล เป็นไปอย่างเหมาะสมและตรวจรับได้ง่าย โดยคำนึงถึงวัตถุประสงค์ของการทำงานเป็นสำคัญ หลักสูตรนี้จึงถูกพัฒนาขึ้น เพื่อให้ผู้บริหาร เจ้าหน้าที่ และผู้มีส่วนเกี่ยวข้องกับการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐที่จำเป็นต้องจัดหาสินค้า/บริการดิจิทัล ได้มีความรู้ ความเข้าใจ ตลอดจนทักษะที่จำเป็น สามารถดำเนินการจัดหาสินค้า/บริการดิจิทัลได้อย่างเหมาะสม ตรงตามวัตถุประสงค์การใช้งาน และช่วยลดปัญหาในการพิจารณาตรวจรับ

โครงสร้างหลักสูตร

หลักสูตรนี้เป็นหลักสูตรที่สร้างความรู้ความเข้าใจเกี่ยวกับการเขียน TOR สำหรับการจัดซื้อจัดจ้างสินค้า/บริการดิจิทัลอย่างเหมาะสม และถูกต้องตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 ตลอดจนฝึกปฏิบัติเพื่อพัฒนาทักษะที่จำเป็นในการเขียน TOR อย่างเข้มข้น เพื่อให้สามารถจัดซื้อและตรวจรับได้ง่าย รวมจำนวน 12 ชั่วโมง / 2 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	6	1
ฝึกปฏิบัติการ (Workshop)	6	1
รวม	12	2

เนื้อหาหลักสูตร ประกอบด้วย

- กฎหมายที่เกี่ยวข้องกับการจัดซื้อจัดจ้าง
- รู้จักสินค้า/บริการดิจิทัล และเทคโนโลยีขั้นสูง
- การเขียน TOR อย่างไรให้จัดซื้อ/ตรวจรับ ได้ง่าย
- การเขียน TOR ให้ใช้ประโยชน์ได้จริงในระยะยาว
- Workshop 1 ฝึกปฏิบัติเขียน TOR เบื้องต้น (กรณีศึกษา)
- Workshop 2 ฝึกปฏิบัติเขียน TOR เพื่อใช้งานจริง (ตัวอย่างจริง)

หลักสูตรนี้เหมาะสำหรับ

- ผู้บริหารและบุคลากรที่เกี่ยวข้องกับการจัดซื้อจัดหาสินค้า/บริการดิจิทัล
- ผู้ให้บริการตรวจสอบและรับรองสินค้า/บริการดิจิทัล
- ผู้ขายสินค้าและผู้ให้บริการดิจิทัล
- ผู้สนใจทั่วไปที่มีโอกาสเป็นคณะกรรมการจัดซื้อตรวจรับ

วิทยากรประจำหลักสูตร



ดร. กมล เอื้อชินกุล

ผู้จัดการ สถาบันประเมินและรับรองเทคโนโลยีดิจิทัล (DTEC)
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC)



คุณสมเดช แสงสุรศักดิ์

ผู้เชี่ยวชาญวิจัย งานวิศวกรรมซอฟต์แวร์และทดสอบผลิตภัณฑ์ (SEPT)
ฝ่ายสนับสนุนบริการทางวิศวกรรมและเทคโนโลยี (TSS)
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC)



ผู้แทนจาก

กรมบัญชีกลาง/สำนักงานคลังจังหวัด

ค่าลงทะเบียน

ท่านละ 9,900 บาท (ยังไม่รวมภาษีมูลค่าเพิ่ม)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐที่ไม่ใช่รัฐกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม

ระยะเวลาหลักสูตร

ระหว่างวันที่ 26 - 27 มิถุนายน 2568

เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 2 วัน)

สถานที่อบรม

โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ

เลขที่ 9 ถนนราชปรารภ เขตราชเทวี กรุงเทพมหานคร

หมายเหตุ

- หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิก เป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/tor>

สอบถามรายละเอียดเพิ่มเติมได้ที่ 085-211-9709, 084-051-3564 E-mail: npd@nstda.or.th



SOC

Security Operations Center



หลักสูตร

ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

รุ่นที่ 5

มุ่งเน้นการฝึกปฏิบัติ
เฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
ภายใต้ศูนย์ SOC อย่างเข้มข้น



Key Highlights

- เรียนรู้แนวทางการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ กับวิทยากรผู้ทรงคุณวุฒิด้านความมั่นคงปลอดภัยระบบสารสนเทศระดับประเทศ
- เจาะลึกกระบวนการปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
- ฝึกปฏิบัติกับซอฟต์แวร์เชิงพาณิชย์ในระดับแนวหน้า เช่น Sprunk Arcsight เพื่อใช้ในการวิเคราะห์ข้อมูลล็อกที่เกี่ยวข้องกับการบุกรุกระบบ
- ฝึกปฏิบัติเข้มข้นมากถึง 10 Workshop ในการปฏิบัติงานเฝ้าระวังความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถนำไปปฏิบัติได้จริงด้วยตนเอง



หลักสูตรศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ รุ่นที่ 5 (Security Operations Center: SOC)

ยุคสารสนเทศหรือยุคดิจิทัลในปัจจุบัน ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศถือเป็นสิ่งสำคัญและมีความจำเป็นอย่างยิ่งต่อองค์กรสำหรับการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยในโลกไซเบอร์ไม่ว่าจะเป็นสถาบันการเงิน ผู้ให้บริการด้านเครือข่าย ผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการ Cloud ผู้ให้บริการดูแล Application และอื่นๆ ทั้งนี้เนื่องมาจากการทำงานขององค์กร ผู้ใช้งาน ตลอดจนลูกค้าขององค์กรมีความจำเป็นต้องอาศัยระบบคอมพิวเตอร์ อินเทอร์เน็ต เครื่องมือไร้สาย อุปกรณ์ประเภท Smartphone รวมถึงอุปกรณ์ประเภท Internet of Things เหล่านี้ส่วนก่อให้เกิดความจำเป็นที่จะต้องมีการเฝ้าระวังและป้องกันระบบและอุปกรณ์ขององค์กรให้มีความมั่นคงปลอดภัยอย่างเพียงพอและตลอดเวลา

Security Operation Center หรือ SOC คือศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่ทำหน้าที่เฝ้าระวังและป้องกันระบบหรืออุปกรณ์สำคัญขององค์กรจากการถูกบุกรุกหรือการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งหากมีเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident) เกิดขึ้น เช่น ระบบถูกบุกรุก หรือการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต SOC จะทำหน้าที่ประเมิน ตรวจสอบและแก้ไขเหตุการณ์ที่เกิดขึ้นเพื่อลดผลกระทบและความเสียหายที่อาจเกิดขึ้นกับองค์กรให้อยู่ในระดับที่ไม่รุนแรง

โครงสร้างหลักสูตร

เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับมาตรฐานในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย แนวทางการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operations Center: SOC) และฝึกปฏิบัติเข้มข้นกับทักษะพื้นฐานที่จำเป็นสำหรับการปฏิบัติงานภายใต้ ศูนย์ปฏิบัติการฯ ประกอบด้วย การบรรยาย การฝึกอบรมเชิงปฏิบัติการ รวม 24 ชั่วโมง / 4 วันทำการ

	หัวข้อ	ชั่วโมง	ครั้ง (วัน)
	บรรยาย และกรณีศึกษา	14	2
	ฝึกปฏิบัติการ (Workshop)	10	2
	รวม	24	4

เนื้อหาหลักสูตร ประกอบด้วย

- มาตรฐานและกระบวนการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- กระบวนการ บทบาท และหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการเฝ้าระวังด้านความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ
- การแบ่งแยกเหตุการณ์แจ้งเตือน (Event) หรือเหตุการณ์ด้านความมั่นคงปลอดภัยให้ชัดเจน (Security Incident)
- การประเมินผลกระทบหรือระดับความรุนแรงของเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น
- การจำลองสถานการณ์การโจมตีในรูปแบบต่างๆ เช่น SQL Injection, Cross-site Scripting (XSS), Brute Force เป็นต้น
- การติดตั้ง Agent บนระบบต่างๆ สำหรับการบันทึกข้อมูลล็อก
- การกำหนดกฎเกณฑ์ (Correlation Rules) ที่ใช้ในการวิเคราะห์ข้อมูลจากล็อก
- การวิเคราะห์ข้อมูลจากล็อก
- การวิเคราะห์ภาษาเหตุของเหตุการณ์ด้านความมั่นคงปลอดภัย
- การจัดเก็บหลักฐานด้านคอมพิวเตอร์จากข้อมูลล็อกที่จัดเก็บไว้
- การวิเคราะห์หรือตรวจสอบข้อมูลในระบบที่ถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต
- การจัดทำรายงานประเภทต่างๆ ที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัย ได้แก่ การแจ้ง เตือนประเภทต่างๆ (Alert) และรายงานประเภทสถิติต่างๆ (Dashboard) ที่จำเป็นต่อการใช้งาน
- การใช้เครื่องมือและจัดเก็บข้อมูลล็อกให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยขององค์กร ตลอดจนกฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง
- การวิเคราะห์หาช่องโหว่ในระบบคอมพิวเตอร์ เพื่อตรวจสอบหาช่องทางการบุกรุกหรือการเข้าถึง เครื่องมือและระบบสารสนเทศที่ผิดปกติ และหาแนวทางป้องกันระบบ
- การใช้เครื่องมือในการเฝ้าระวังและติดตามการทำงานของระบบและอุปกรณ์ต่างๆ

หลักสูตรนี้เหมาะสำหรับ

- ผู้ปฏิบัติงานในศูนย์ปฏิบัติการป้องกันเฝ้าระวังความมั่นคงปลอดภัย (เช่น CERT NOC เป็นต้น)
- ผู้ดูแลระบบคอมพิวเตอร์ / ผู้ดูแลเครือข่ายคอมพิวเตอร์
- ผู้จัดการด้านไอที
- ผู้ปฏิบัติงานที่เกี่ยวข้องกับการเฝ้าระวังระบบและอุปกรณ์ต่างๆ ขององค์กร

วิทยากรประจำหลักสูตร



ดร. บรรจง หะรังษี
รองกรรมการผู้จัดการ และ
ที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ
บริษัท ที-เน็ต จำกัด



อาจารย์ เจษฎา กองกันเหลือง
กรรมการผู้จัดการ
บริษัท ที-เน็ต ไอที โซลูชัน จำกัด

ระยะเวลาหลักสูตร

ระหว่างวันที่ 22 - 25 กรกฎาคม 2568
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 4 วัน)

ค่าลงทะเบียน

ท่านละ 32,100 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)
• เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ
ที่ไม่ใช้รัฐกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม

สถานที่อบรม



โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

หมายเหตุ

- หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิก เป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/soc>

สอบถามรายละเอียดเพิ่มเติมได้ที่ 085-211-9709, 084-051-3564 E-mail: npd@nstda.or.th



CSS

Cloud Security Standard

หลักสูตรมาตรฐานการบริหารจัดการ
ความมั่นคงปลอดภัยบนระบบคลาวด์
ตามมาตรฐาน CSA 4.x และ ISO/IEC 27001: 2022 **รุ่นที่ 6**



มุ่งเน้นการบริหารจัดการระบบงานให้มีความมั่นคงปลอดภัยและสอดคล้อง
ตามมาตรฐาน CSA 4.x และ ISO/IEC 27001: 2022

Key Highlights

- ❖ เจาะลึกแนวทางในการนำระบบงานขึ้นคลาวด์ให้มีความมั่นคงปลอดภัย
- ❖ เรียนรู้มาตรฐานสากล CSA 4.x และ ISO/IEC 27001: 2022 ในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ ที่นำไปติดตั้งและใช้งานบนคลาวด์
- ❖ เข้าใจโดเมนและมาตรฐาน ด้านความมั่นคงปลอดภัย CSA 4.x และ ISO/IEC 27001: 2022 พร้อมอัปเดตข้อมูลล่าสุด
- ❖ เรียนรู้มาตรการ CSA 4.x ทั้ง 17 โดเมน เพื่อลดความผิดพลาดต่างๆ ก่อนที่จะเกิดขึ้น



หลักสูตรมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบคลาวด์ ตามมาตรฐาน CSA 4.x และ ISO/IEC 27001: 2022 รุ่นที่ 6 (Cloud Security Standard : CSS)

ปัจจุบันหลายองค์กรได้เริ่มปรับเปลี่ยนการทำงานจากการติดตั้ง ดูแล และบริหารจัดการเซิร์ฟเวอร์และระบบงานต่างๆ ภายในศูนย์คอมพิวเตอร์ไปติดตั้งและบริหารจัดการระบบโดยใช้บริการจากผู้ให้บริการคลาวด์แทน ซึ่งมีความรู้ ความสามารถ และน่าเชื่อถือ เพื่อประหยัดค่าใช้จ่ายในการลงทุนด้านเซิร์ฟเวอร์ โครงสร้างพื้นฐานด้านเครือข่าย และการจัดทำศูนย์คอมพิวเตอร์ จากความจำเป็นหรือความต้องการในการนำระบบงานต่างๆ ขององค์กรขึ้นไปติดตั้งบนคลาวด์ของผู้ให้บริการ ประเด็นปัญหาและอุปสรรคสำคัญในฐานะผู้ใช้บริการคลาวด์คือ ประเด็นความมั่นคงปลอดภัยด้านสารสนเทศที่ทุกองค์กรที่จะนำระบบงานไปติดตั้งบนคลาวด์ต้องเผชิญ หลักสูตรนี้จึงเล็งเห็นถึงความจำเป็นในการนำระบบงานขององค์กรไปขึ้นคลาวด์ให้มีความมั่นคงปลอดภัย ทั้งนี้เพื่อให้เกิดความมั่นใจต่อผู้ใช้บริการคลาวด์นั่นเอง

โดยมาตรฐานสากลสำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศบนคลาวด์ที่นิยมใช้หรืออ้างอิงกันอยู่คือมาตรฐาน CSA (Cloud Security Alliance) มาตรฐานนี้เป็นมาตรฐานที่พัฒนาต่อยอดมาจาก ISO/IEC 27001 ซึ่งเป็นมาตรฐานหลักด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เป็นที่นิยมและปัจจุบันมีหลายหน่วยงานทั้งภาครัฐและเอกชนปฏิบัติตามอยู่ หลักสูตรนี้ได้อ้างอิงตามมาตรฐาน CSA 4.x (เวอร์ชันปัจจุบันล่าสุด) และ มาตรฐาน ISO/IEC 27001: 2022 (เวอร์ชันปัจจุบันล่าสุด)

โครงสร้างหลักสูตร

หลักสูตรนี้มุ่งเน้นให้ผู้เข้าอบรมทราบแนวทาง วิธีการนำระบบงานขึ้นคลาวด์ให้มีความมั่นคงปลอดภัย ตามมาตรฐาน CSA 4.x และ ISO/IEC 27001: 2022 การบริหารจัดการฐานข้อมูล ระบบบริหารจัดการเว็บเซอร์เวอร์ต่างๆ ที่เกี่ยวข้อง แอปพลิเคชันของระบบงาน จนกระทั่งสามารถใช้งานระบบได้ โดยสามารถนำแนวทางดังกล่าวไปต่อยอดหรือปรับใช้กับระบบงานของตนเองได้ รวม 18 ชั่วโมง / 3 วันทำการ

	หัวข้อ	ชั่วโมง	ครั้ง (วัน)
	บรรยาย และกรณีศึกษา	12	2
	ฝึกปฏิบัติการ (Workshop)	6	1
	รวม	18	3

หลักสูตรนี้เหมาะสำหรับ

- เจ้าหน้าที่เทคนิค ได้แก่ ผู้ดูแลระบบ ผู้ดูแลเครือข่าย ผู้พัฒนาระบบ Helpdesk
- เจ้าหน้าที่ด้านความมั่นคงปลอดภัยระบบสารสนเทศ (IT Security)
- ผู้ที่อยู่ในตำแหน่งงานด้านไอซีทีต่างๆ ที่สนใจงานด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ

วิทยากรประจำหลักสูตร



ดร. บรรจง หะรังษี
รองกรรมการผู้จัดการ และ
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 V12 Certificate

สิ่งที่คาดว่าจะได้รับ

- ผู้เข้าอบรมจะได้รับ
- ความรู้ความเข้าใจในการนำระบบงานขึ้นคลาวด์ให้มีความมั่นคงปลอดภัยด้านสารสนเทศตามมาตรฐาน CSA และ ISO/IEC 27001: 2022
 - ได้แนวทางที่สอดคล้อง ในการบริหารจัดการระบบงานให้เข้ากับมาตรฐานในโดเมนต่างๆ
 - ความรู้จากกรณีศึกษาในห้องเรียน ที่จะนำไปปรับใช้งานกับองค์กรของตนเองได้อย่างมีประสิทธิภาพ

cloud
CSA security
alliance®



ระยะเวลาหลักสูตร

ระหว่างวันที่ 13 - 15 สิงหาคม 2568
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 3 วัน)

ค่าลงทะเบียน

ท่านละ 22,470 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ
ที่ไม่ใช่รัฐกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม

สถานที่อบรม



โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

หมายเหตุ

- หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิก เป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งชาติ ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/css>

สอบถามรายละเอียดเพิ่มเติมได้ที่ 085-211-9709, 084-051-3564 E-mail: npd@nstda.or.th

Information Technology and Management Professional Training Program: ITM

Common Course/Skill Framework	Major Category	Middle Category	Course ID	#	Course Title	Days	Price (Excluding Vat)		Price (Including Vat)		Month																																
							Onsite	Online	Onsite	Online	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC																					
Technical Element	Network	Database	DBM032	5	SQL Server 2022 Programming and Implementation	5	15,000.00	16,000.00																																			
			DBM049	5	SQL Server 2022 Database Queries and Analysis	5	16,000.00	16,000.00																																			
			NMA001	3	Understanding Network Fundamentals	3	11,200.00	12,800.00																																			
			NMA080	5	Fundamentals Linux for System Administration: การบริหารระบบปฏิบัติการลินุกซ์	5	15,000.00	16,000.00																																			
			NMA113		Linux Networking and Security Administration	2	10,000.00	10,700.00																																			
			ITM109	New	การตระหนักรู้ด้านความปลอดภัย (Cybersecurity Awareness)	2	10,000.00	10,700.00																																			
			NMA004		Troubleshooting TCP/IP Networking	4	14,000.00	14,900.00																																			
			NMA067		Network System Administration Techniques for IT Professionals: การบริหารเทคนิคการแก้ไขปัญหาเครือข่าย	5	18,000.00	18,500.00																																			
			NMA082		Network Administration and Monitoring Tools	4	14,000.00	15,150.00																																			
			TEC016		Wireshark Certified Network Analyst	3	16,500.00	18,300.00																																			
			ITM170	New	WAZUH	2	10,000.00	10,700.00																																			
			ITM171	New	Certified Information Security Manager (CISM)	4	21,000.00	22,500.00																																			
			ITM172	New	Certified Information Systems Security Professional (CISSP)	5	22,000.00	18,500.00																																			
CLS030	New	CompTIA Cloud+	5	22,000.00	28,500.00																																						
NMA054		Network and Internet Security for IT Professionals	5	16,000.00	17,100.00																																						
SEC004		Cyber Security for Smart User	2	4,500.00	4,900.00																																						
SEC008		Computer Forensic and Investigation	5	26,500.00	27,250.00																																						
SEC012		Certified Ethical Hacker v12 (CEHv12)	5	26,000.00	27,400.00																																						
SEC016		CompTIA Security+	5	25,000.00	31,400.00																																						
TEC006		Cybersecurity Analyst	5	26,500.00	27,250.00																																						

[New] หลักสูตรใหม่ ปี 2568

[Stemplus] ผู้ประกอบการที่ผลิตและจำหน่ายสินค้าทางการศึกษาในประเทศไทยได้รับการรับรองโดยสภาวิชาชีพการศึกษามูลนิธิ (สพช.) ครอบคลุมสินค้าการศึกษาทุกประเภท 250% หากสนใจข้อมูลเพิ่มเติม กรุณาติดต่อ Call Center 0-2564-8150 หรือ 81886-7 หรือเว็บไซต์ www.stemplus.or.th

[สสจ.] หลักสูตรนี้ได้รับการรับรองมาตรฐานการศึกษาจาก สสจ. กรุงเทพมหานคร ทั่วประเทศ และได้รับอนุญาตให้ดำเนินการเรียนการสอนได้ทั่วประเทศ โดยสามารถสมัครเรียนได้ทั้งในรูปแบบออนไลน์และเรียนภาคปฏิบัติที่ศูนย์การเรียนการสอน

360 องศา
 เรียนจบแล้วได้ใบประกาศนียบัตรวิชาชีพชั้นสูง (อนุปริญญา) 2 สาขา พร้อมใบรับรองการประเมินผลสัมฤทธิ์ทางการเรียน (ใบรับรองการประเมินผลสัมฤทธิ์ทางการเรียน) และใบรับรองการประเมินผลสัมฤทธิ์ทางการเรียน (ใบรับรองการประเมินผลสัมฤทธิ์ทางการเรียน)

National Science and Technology Development Agency
สภาการศึกษา สถาบันพัฒนาบุคลากร (สสจ.)
 เลขที่ห้อง: 080-0-00001-0 ประเภทห้อง: วิชาอาชีวศึกษา
สภาการศึกษา สถาบันพัฒนาบุคลากร (สสจ.)
 เลขที่ห้อง: 152-1-32668-1 ประเภทห้อง: วิชาอาชีวศึกษา

สมัครเรียนได้ที่ Call Center 0-2564-8150 หรือ 81886-7 หรือเว็บไซต์ <https://www.stemplus.or.th>

ฝ่ายพัฒนาระบบการเรียน | <https://www.careerfuture.com/cta> | **Call Center 0 2564 8150 หรือ 81886-7** | **Email: training@nsda.or.th**

สิทธิประโยชน์
 ● ผู้ลงทะเบียนเรียนแล้วจะได้รับสิทธิประโยชน์ในการลดหย่อนภาษีเงินได้บุคคลธรรมดา (มาตรา 26(3) แห่งประมวลรัษฎากร) โดยไม่ต้องเสียเงินลงทุน
 ● ผู้ลงทะเบียนเรียนแล้วจะได้รับสิทธิประโยชน์ในการลดหย่อนภาษีเงินได้บุคคลธรรมดา (มาตรา 26(3) แห่งประมวลรัษฎากร) โดยไม่ต้องเสียเงินลงทุน

ข้อควรระวัง
 ● ผู้ลงทะเบียนเรียนแล้วจะได้รับสิทธิประโยชน์ในการลดหย่อนภาษีเงินได้บุคคลธรรมดา (มาตรา 26(3) แห่งประมวลรัษฎากร) โดยไม่ต้องเสียเงินลงทุน

เงื่อนไขการสมัครเรียน
 ● ผู้ลงทะเบียนเรียนแล้วจะได้รับสิทธิประโยชน์ในการลดหย่อนภาษีเงินได้บุคคลธรรมดา (มาตรา 26(3) แห่งประมวลรัษฎากร) โดยไม่ต้องเสียเงินลงทุน

หมายเหตุ
 ● ผู้ลงทะเบียนเรียนแล้วจะได้รับสิทธิประโยชน์ในการลดหย่อนภาษีเงินได้บุคคลธรรมดา (มาตรา 26(3) แห่งประมวลรัษฎากร) โดยไม่ต้องเสียเงินลงทุน



AIG

AI Governance Workshop

หลักสูตรฝึกอบรมเชิงปฏิบัติการ
การกำกับดูแล AI อย่างมีธรรมาภิบาลและความรับผิดชอบ

มุ่งเน้นการฝึกปฏิบัติเข้มข้นถึง 9 Workshops

เพื่อกำหนดมาตรการต่าง ๆ ที่จำเป็นที่เกี่ยวกับการพัฒนาระบบ AI ขององค์กร
เพื่อลดความเสี่ยงต่าง ๆ ของระบบให้อยู่ในระดับที่องค์กรยอมรับได้ และเป็นระบบที่มีความน่าเชื่อถือ
รวมถึงสอดคล้องกับมาตรฐานสากลที่มีการอ้างอิงและใช้งานในปัจจุบัน



Key Highlights

- เรียนรู้มาตรฐาน AI ที่เกี่ยวข้อง สอดคล้องกับมาตรฐานสากลที่มีการอ้างอิงและใช้งานในปัจจุบัน
- เรียนรู้วิธีการและมาตรการที่ช่วยป้องกันปัญหาความเสี่ยงในระบบ AI ซึ่งสามารถนำไปใช้ได้จริงในการพัฒนาระบบ
- ฝึกการประเมินและจัดการความเสี่ยงในโครงการ AI เพื่อให้สามารถควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- สามารถนำมาตรการ และวิธีปฏิบัติ ไปปรับใช้กับระบบงานขององค์กร เพื่อให้ได้ระบบ AI ที่มีความน่าเชื่อถือและพร้อมใช้งานได้จริงในธุรกิจ



หลักสูตรฝึกอบรมเชิงปฏิบัติการ การทำกับดูแล AI อย่างมีธรรมาภิบาลและความรับผิดชอบ (AI Governance Workshop)

ปัจจุบันมีการพัฒนาระบบงานเพื่อทำงานร่วมกับหรือทดแทนการทำงานของมนุษย์เป็นจำนวนมาก เช่น ระบบ ChatGPT ระบบงานที่พัฒนาขึ้นมาเหล่านั้นใช้เทคโนโลยีที่เรียกว่าปัญญาประดิษฐ์หรือ AI (Artificial Intelligence) ซึ่งทำให้เครื่องคอมพิวเตอร์สามารถคิดและดำเนินการในลักษณะเดียวกับหรือใกล้เคียงกับที่มนุษย์สามารถทำได้ ในบางกรณีการคิดและดำเนินการเหล่านั้นจะเป็นส่วนหนึ่งของกลไกการตัดสินใจโดยมนุษย์ เช่น ระบบผู้ชำนาญการ ระบบช่วยในการตัดสินใจ เป็นต้น ในขณะที่ในบางกรณีระบบ AI บางระบบจะสามารถดำเนินการแทนมนุษย์ได้โดยอัตโนมัติได้ เช่น ระบบขับขี่ยานยนต์อัตโนมัติ เป็นต้น เนื่องจากระบบ AI ดังกล่าวไม่ใช่มนุษย์ ดังนั้นการคิดและดำเนินการต่างๆ จึงมีโอกาสผิดพลาดและมีความเสี่ยงในลักษณะต่างๆ ได้ จึงทำให้จำเป็นต้องมีวิธีการที่เป็นรูปธรรมเพื่อบริหารจัดการการนำระบบ AI มาใช้งานเพื่อก่อให้เกิดประโยชน์ต่อองค์กร ลดความเสี่ยงและผลกระทบต่างๆ ที่อาจจะเกิดขึ้นได้ให้อยู่ในระดับที่องค์กรยอมรับได้

มาตรฐาน AI จึงถือกำเนิดขึ้นมาขึ้นมาเพื่อบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการนำระบบ AI มาใช้งานให้อยู่ในระดับที่องค์กรทั่วไปยอมรับได้ มาตรฐาน AI หลักที่จะนำมาใช้ในหลักสูตรนี้ประกอบด้วยมาตรฐาน 3 รายการดังนี้

1. Artificial Intelligence Risk Management Framework (AI RMF 1.0)
2. AI RMF PLAYBOOK
3. ISO/IEC 42001:2023(E) Artificial Intelligence Management system

โครงสร้างหลักสูตร

หลักสูตรนี้เป็นหลักสูตรที่ให้ความรู้และความเข้าใจเกี่ยวกับมาตรฐานของ AI เพื่อนำไปใช้ในการบริหารและจัดการความเสี่ยงที่เกี่ยวข้องกับการนำระบบ AI มาใช้งานกับองค์กร ตลอดจนวงจรชีวิตของระบบ ตลอดจนนำความรู้ที่ได้รับมาฝึกทดลองปฏิบัติตามมาตรฐานดังกล่าว เพื่อให้ได้ทักษะอย่างแท้จริง และสามารถนำกลับไปปรับใช้งานกับองค์กรของผู้เรียนได้ รวมจำนวน 12 ชั่วโมง / 2 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	6	1
ฝึกปฏิบัติการ (Workshop)	6	1
รวม	12	2

เนื้อหาหลักสูตร ประกอบด้วย

- ความรู้พื้นฐานของ AI ที่ควรทราบ
- ประเภทของ AI ที่มีการใช้งานกันโดยทั่วไป
- วงจรการพัฒนาของระบบ AI
- มาตรฐาน AI ที่เกี่ยวข้อง
- การกำกับดูแล AI ที่ครอบคลุมถึง
 - นโยบาย กระบวนการ ขั้นตอนปฏิบัติ และวิธีปฏิบัติสำหรับการกำหนด วัตถุประสงค์ และบริหารความเสี่ยงของ AI ขององค์กร
 - โครงสร้างของการกำกับดูแล บทบาท และหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการบริหารความเสี่ยงของ AI ขององค์กร
- การกำหนดความเสี่ยงของ AI ที่ครอบคลุมถึง
 - การทำความเข้าใจและกำหนดบริบทขององค์กร
 - การกำหนดหมวดหมู่ของระบบ AI ที่องค์กรมีการใช้งาน
 - ความเสี่ยงและประโยชน์หรือคุณค่าที่คาดว่าจะได้รับ ซึ่งรวมถึงความเสี่ยงจากผู้ให้บริการภายนอกที่เกี่ยวข้องกับซอฟต์แวร์หรือข้อมูลที่องค์กรมีการใช้งาน
 - ผลกระทบที่เกิดขึ้นต่อผู้มีส่วนได้ส่วนเสีย กลุ่ม สังคม และองค์กร
- การวัดความเสี่ยงของ AI ที่ครอบคลุมถึง
 - การกำหนดวิธีการและตัวชี้วัดที่เหมาะสมในการวัดความเสี่ยง
 - การประเมินคุณสมบัติความน่าเชื่อถือของระบบ AI
 - การกำหนดกลไกในการเฝ้าระวังและติดตามความเสี่ยงของระบบ AI
- การบริหารความเสี่ยงของ AI ที่ครอบคลุมถึง
 - การจัดลำดับความเสี่ยงที่ได้มีการประเมินไว้ เพื่อรับมือและบริหารจัดการ
 - การกำหนดกลยุทธ์ในการจัดการกับความเสี่ยง
 - การบริหารจัดการกับความเสี่ยงที่เกี่ยวข้องกับผู้ให้บริการภายนอก

หลักสูตรนี้เหมาะสำหรับ

- ผู้ปฏิบัติงานที่เกี่ยวข้องกับมาตรฐานด้านไอที
- ผู้บริหารองค์กรที่จำเป็นต้องกำกับดูแลการนำ AI มาใช้ภายในองค์กร
- ผู้พัฒนาระบบ
- นักวิเคราะห์และออกแบบระบบ
- ผู้ปฏิบัติงานทั่วไปที่จำเป็นต้องพัฒนาระบบของตนเองที่มีการใช้งาน AI เป็นส่วนหนึ่งของระบบ

วิทยากรประจำหลักสูตร



ดร. บรรจง หะรังษี
รองกรรมการผู้จัดการและที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ บริษัท ที-เน็ต จำกัด


ค่าลงทะเบียน

ท่านละ 12,840 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)
• เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ
ที่ไม่ใช่รัฐกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
• โปรโมชันพิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไป
รับส่วนลดทันที 10%

ระยะเวลาหลักสูตร

ระหว่างวันที่ 1 – 2 เมษายน 2568
เวลา 9:00 - 16:00 น. (รวมระยะเวลาอบรม จำนวน 3 วัน)

สถานที่อบรม

 โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

หมายเหตุ

- หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิก เป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/aig>

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891 E-mail: npd@nstda.or.th



ITA

IT Audit for Non - IT Auditor Masterclass

รุ่นที่ 20

การบูรณาการ IT Audit และ General Audit ให้เป็นหนึ่งเดียว
เพื่อเพิ่มประสิทธิภาพการตรวจสอบที่ยั่งยืน



วิทยากรผู้เชี่ยวชาญ



อาจารย์เมธา สุวรรณสาร

ผู้เชี่ยวชาญการตรวจสอบเทคโนโลยีสารสนเทศ
อดีตนายกสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ
(TISA)



ดร. บรรจง หะรังษี

รองกรรมการผู้จัดการ และ
ที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ
บริษัท ที-เน็ต จำกัด



ดร. ชัยกร ปิยะบัณฑิตกุล

ประธานเจ้าหน้าที่บริหาร
บริษัท ไอเอ็ม จำกัด



อาจารย์กัญญา ตรีเพชรารักษ์

ผู้อำนวยการฝ่ายกำกับและตรวจสอบความเสี่ยง
ด้านเทคโนโลยีสารสนเทศ
ธนาคารแห่งประเทศไทย



อาจารย์พิทักษ์พงษ์ อินเสอ

ผู้จัดการฝ่ายฝึกอบรม/
ผู้ตรวจประเมินระบบมาตรฐาน
URS Thailand

วันที่ 17 – 21 มีนาคม 2568 ณ. โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ

หลักสูตรนี้เหมาะสำหรับ

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



หลักสูตรนี้ได้รับการออกแบบตามมาตรฐานการประกันคุณภาพสำหรับการจัดฝึกอบรมและการศึกษา ISO 10015

หลักสูตร IT Audit for Non - IT Auditor Masterclass รุ่นที่ 20

การบูรณาการ IT Audit และ General Audit ให้เป็นหนึ่งเดียว เพื่อเพิ่มประสิทธิภาพการตรวจสอบที่ยั่งยืน

ปัจจุบันเทคโนโลยีสารสนเทศเข้ามามีบทบาทในกระบวนการดำเนินงานธุรกิจในทุกภาคส่วนทั้งหน่วยงานภาครัฐและเอกชน ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Auditor) จึงมีบทบาทสำคัญในการช่วยประเมินและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงาน ในทางปฏิบัติพบว่าบุคลากรที่ทำหน้าที่ตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศส่วนมากเป็นผู้ตรวจสอบภายในทั่วไปที่ไม่มีพื้นฐานความรู้ด้านเทคโนโลยีสารสนเทศ ขาดทักษะ ความรู้ ความเข้าใจองค์ความรู้และเครื่องมือต่างๆ ที่ช่วยในการตรวจสอบระบบเทคโนโลยีสารสนเทศ รวมถึงการจัดทำรายงานเสนอแนะเพื่อควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร

หลักสูตร IT Audit for Non - IT Auditor Masterclass มุ่งเน้นเสริมสร้างศักยภาพของผู้ตรวจสอบภายในให้มีความรู้ความเข้าใจขั้นตอน กระบวนการการตรวจสอบความเสี่ยงด้านเทคโนโลยี เรียนรู้มาตรฐานต่างๆ และเครื่องมือที่เกี่ยวข้อง เพื่อหลอมรวมการตรวจสอบทั่วไปและการตรวจสอบด้านเทคโนโลยีสารสนเทศเข้าไว้ด้วยกันเป็น Integrated Auditing

โครงสร้างหลักสูตร

หลักสูตรนี้เป็นหลักสูตรที่ให้ความรู้และความเข้าใจเกี่ยวกับ บทบาทของการบริหารและการจัดการ การตรวจสอบด้านเทคโนโลยีสารสนเทศตามหลักการบริหารความเสี่ยงยุคใหม่ได้ สามารถปฏิบัติงานการตรวจสอบเทคโนโลยีสารสนเทศตามมาตรฐานและเทคนิคการตรวจสอบที่เกี่ยวข้อง เพื่อสนองความต้องการของผู้บริหารทุกระดับได้ สามารถวางแผนการตรวจสอบตามหลักการบริหารความเสี่ยงทั่วไปและทางด้านเทคโนโลยีสารสนเทศที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กรได้อย่างมั่นใจ รวม 30 ชั่วโมง / 5 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	18	3
ฝึกปฏิบัติการ (Workshop)	12	2
รวม	30	5

หลักสูตรนี้เหมาะสำหรับ

- ผู้ตรวจสอบภายในจากหน่วยงานภาครัฐ รัฐวิสาหกิจ และภาคเอกชน
- ผู้บริหารระดับกลางที่เกี่ยวข้องกับกระบวนการตรวจสอบ
- บุคคลสาขาอาชีพอื่นที่สนใจเป็นผู้ตรวจสอบภายในและผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ
- บุคคลทั่วไปที่มีความสนใจในกระบวนการตรวจสอบภายในและการบริหารเชิงรุก

สิ่งที่จะได้รับ

- ความรู้ ความเข้าใจในบทบาทหน้าที่ และความรับผิดชอบของผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศตามหลักการบริหารความเสี่ยงยุคใหม่
- ความรู้ ความเข้าใจขั้นตอน และกระบวนการการตรวจสอบด้านเทคโนโลยีตามหลักการบริหารความเสี่ยง
- แนวทางการวางแผนการตรวจสอบภายในตามหลักการบริหารความเสี่ยงทั่วไปและด้านเทคโนโลยีสารสนเทศที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร
- แนวปฏิบัติงานตรวจสอบเทคโนโลยีสารสนเทศ โดยใช้เทคนิคการตรวจสอบและมาตรฐานที่เกี่ยวข้อง

ค่าลงทะเบียน

ท่านละ 21,400 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐที่ไม่ใช่ธุรกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม

หมายเหตุ

- หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิก เป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องใช้เวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

เนื้อหาหลักสูตร ประกอบด้วย

- เทคโนโลยีสารสนเทศสำหรับผู้ตรวจสอบ
- บทบาทหน้าที่ของผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Auditor)
- การตรวจสอบเทคโนโลยีสารสนเทศตามหลักธรรมาภิบาล
- แนวปฏิบัติงานตรวจสอบด้านเทคโนโลยีสารสนเทศ
- ISO 27001:2013 กับการบริหารความเสี่ยงเทคโนโลยีสารสนเทศ
- แนวทางการตรวจประเมินตามมาตรฐาน ISO/IEC 19011:2011 และประสบการณ์การตรวจสอบ ด้านเทคโนโลยีสารสนเทศ
- Integrated Audit in Practice

ระยะเวลาหลักสูตร

ระหว่างวันที่ 17 - 21 มีนาคม 2568
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 5 วัน)

สถานที่อบรม



โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

ศึกษารายละเอียดเพิ่มเติมได้ที่ <https://www.career4future.com/ita>

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891, 81898 E-mail: npd@nstda.or.th