

**ITM113: Audit and Control Risk for IT Outsourcing (การตรวจสอบและควบคุมความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ)**

**หลักการและเหตุผล:**

จากการเปลี่ยนผ่านสู่ยุคเศรษฐกิจดิจิทัล ทำให้วิวัฒนาการด้านเทคโนโลยีดิจิทัลถูกพัฒนาขึ้นอย่างต่อเนื่องและรวดเร็ว จนเป็นที่ยอมรับว่าเทคโนโลยีดิจิทัลเป็นเทคโนโลยีที่มีอิทธิพลอย่างมากต่อการใช้ชีวิตของผู้คนในยุคปัจจุบัน จนส่งผลให้เกิดการเปลี่ยนแปลงในหลากหลายมิติ สามารถพลิกโฉมรูปแบบการค้า การลงทุน และการดำเนินชีวิต ดังนั้นทุกภาคส่วนต่างเล็งเห็นถึงประโยชน์จากการนำความสามารถของเทคโนโลยีดิจิทัลมาเป็นปัจจัยสำคัญต่อการพัฒนาองค์กร หลายองค์กรจึงต่างทุ่มเทการลงทุนพัฒนาระบบแอปพลิเคชันต่างๆขององค์กรให้เป็นระบบอัตโนมัติด้วยเทคโนโลยีดิจิทัล เพื่อช่วยเพิ่มสมรรถนะด้านการปฏิบัติงานของบุคลากร และเพิ่มศักยภาพในการดำเนินกิจการให้มากยิ่งขึ้น จะเห็นได้ว่าปัจจุบันได้เกิดนวัตกรรมทางเทคโนโลยีใหม่ๆขึ้นอย่างมากมาย ดังเช่น หลายๆ องค์กรได้นำเอาเทคโนโลยี AI (Artificial Intelligence) มาพัฒนาเป็นระบบอัจฉริยะที่สามารถแสดงผลลัพธ์ที่มีความแน่นอน แม่นยำ เทียบตรงสูง ที่ความสามารถของมนุษย์เองก็ยากที่จะทัดเทียมได้ และยังสามารถนำเอาเทคโนโลยี AI มาประมวลผลร่วมกับข้อมูลขนาดใหญ่ (Big Data) เพื่อทำนาย วิเคราะห์ข้อมูลเชิงลึก (Data Analytic) ได้อย่างถูกต้องแม่นยำ และยังเกิดนวัตกรรมใหม่ๆขึ้นอีกมากมายในหลายๆอุตสาหกรรม

แต่การนำเทคโนโลยีดิจิทัลซึ่งเป็นเทคโนโลยีสมัยใหม่ที่มีความหลากหลายและมีความซับซ้อนเข้ามาติดตั้งใช้งานหรือนำมาพัฒนาเป็นระบบแอปพลิเคชันเพื่อใช้งานในองค์กรก็ไม่ใช่เรื่องง่าย เพราะจะต้องอาศัยบุคลากรที่มีความพร้อมด้านความรู้ ความเข้าใจและความเชี่ยวชาญด้านเทคโนโลยีดิจิทัลนั้นๆเป็นอย่างดี รวมถึงการอาศัยเครื่องมืออุปกรณ์ประกอบต่างๆ ซึ่งส่วนใหญ่มีราคาสูง นั้นหมายความว่าหากองค์กรประสงค์ที่จะนำเทคโนโลยีสมัยใหม่มาใช้งานหรือนำมาพัฒนาเป็นระบบแอปพลิเคชันต่างๆขึ้นใช้งานเองภายในองค์กร ก็จะทำให้องค์กรต้องประสบกับปัญหาด้านความพร้อมของบุคลากรที่จะมาทำหน้าที่พัฒนาระบบ รวมถึงองค์กรต้องอาศัยงบประมาณและระยะเวลาที่ใช้ในการพัฒนาเป็นอันมาก ซึ่งเป็นความเสี่ยงที่อาจจะทำให้การพัฒนาและการติดตั้งใช้งานระบบเทคโนโลยีดิจิทัลสมัยใหม่ไม่อาจประสบความสำเร็จได้ตามวัตถุประสงค์ที่องค์กรคาดหวังไว้ ดังนั้นเพื่อเป็นการลดโอกาสที่จะเกิดความเสียหายจากความเสี่ยงดังกล่าว และจะเป็นการลดต้นทุนจากการนำเทคโนโลยีดิจิทัลเข้ามาใช้งานในองค์กร และสามารถทำให้การบริหารกิจการขององค์กรสามารถประสบความสำเร็จตามวัตถุประสงค์ที่องค์กรได้คาดหวังไว้ องค์กรจึงต้องอาศัยการใช้บริการจากผู้ให้บริการภายนอก (Outsourcing) ที่ได้จัดสรรระบบเทคโนโลยีต่างๆเอาไว้พร้อมแล้วเพื่อรองรับการให้บริการตามความต้องการของลูกค้า ยกตัวอย่างเช่น การใช้บริการจากผู้ให้บริการภายนอกที่ให้บริการระบบคลาวด์ (Cloud Service Provider) การใช้บริการจากผู้ให้บริการภายนอกที่ให้บริการชำระเงินทางอิเล็กทรอนิกส์ (Payment Gateway) หรือการใช้บริการจากผู้ให้บริการภายนอกที่ให้บริการด้านระบบงานประมวลผล (Processing System) เป็นต้น หรือองค์กรจะใช้วิธีการว่าจ้างผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ที่มีความรู้ ความเชี่ยวชาญ และประสบการณ์ด้านการพัฒนาระบบแอปพลิเคชันด้วยเทคโนโลยีสารสนเทศสมัยใหม่มาเป็นผู้ดำเนินการพัฒนาระบบแอปพลิเคชันให้ตามที่ต้องการ แต่ด้วยข้อจำกัดของผู้ให้บริการภายนอกที่ไม่ใช่บุคลากรภายในขององค์กรจึงมักขาดประสบการณ์ ขาดความเข้าใจในกระบวนการทางธุรกิจ (Business Process) ขององค์กร และด้วยสถานะการแข่งขันที่แต่ละองค์กรต่างต้องแย่งชิงความเป็นผู้นำ จึงต่างต้องเร่งรีบพัฒนาและปรับปรุงระบบเทคโนโลยีสารสนเทศของตนเองให้แล้วเสร็จโดยเร็ว จากการพัฒนาอย่างเร่งรีบ ได้ก่อให้เกิดปัญหาขึ้นในกระบวนการพัฒนาระบบ เช่น ปัญหาการรวบรวมความต้องการของผู้ใช้งาน (User Requirements) ที่ไม่ถูกต้องครบถ้วนตามความต้องการที่แท้จริงของผู้ใช้งาน รวมถึงระบบควบคุมต่างๆที่ควรจะมีก็มักจะถูกละเลย และหากองค์กรใดมีกระบวนการทางธุรกิจที่ซับซ้อนซับซ้อนมีระเบียบวิธีปฏิบัติหลายขั้นตอน ก็ยิ่งทำให้ปัญหาเหล่านี้เกิดขึ้นได้ง่ายยิ่งขึ้น และจะส่งผลให้การออกแบบระบบแอปพลิเคชันเกิดความผิดพลาด และเมื่อระบบแอปพลิเคชันถูกพัฒนาเสร็จและนำไปติดตั้งใช้งาน ปัญหาที่ตามมาจะเป็นสิ่งที่น่าเป็นห่วงและน่ากังวลเป็นอย่างมาก ก็คือปัญหาความผิดพลาดและช่องโหว่ต่างๆที่จะเกิดขึ้นกับระบบแอปพลิเคชัน อันเป็นผลมาจากการขาดการติดตาม ตรวจสอบและควบคุมดูแลเอาใจใส่ในระหว่างที่ผู้ให้บริการภายนอกดำเนินการพัฒนาระบบ จนทำให้องค์กรต้องเผชิญกับสถานะเสี่ยงต่อการถูกคุกคาม ทั้งปัญหาการถูกคุกคามจากภายในองค์กร และการถูกคุกคามความมั่นคงปลอดภัยทางไซเบอร์ ก่อให้เกิดความเสียหายจากการละเมิดข้อมูล การละเมิดเพื่อแก้ไข หรือทำลายข้อมูล การกระทำทุจริต การละเมิดสิทธิส่วนบุคคล จนทำให้องค์กรถูกฟ้องร้องดำเนินคดีได้รับความเสียหาย

อย่างไรก็ตามหากองค์กรมีกระบวนการติดตาม ตรวจสอบและมีมาตรการควบคุมความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกที่เหมาะสม มีประสิทธิภาพ ประสิทธิผลเพียงพอ และทำการติดตาม ตรวจสอบการให้บริการอย่างสม่ำเสมอตั้งแต่เริ่มต้นจนกระทั่งสิ้นสุดการให้บริการ ก็จะสามารถป้องกันโอกาสการเกิดความเสียหายให้แก่องค์กรได้

หลักสูตรนี้เป็นการอบรมเชิงปฏิบัติการ และศึกษาจากกรณีศึกษา จากประสบการณ์การตรวจสอบและควบคุมความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศทั้งภาครัฐและเอกชน ที่ผู้เข้ารับการอบรมจะได้รับการฝึกปฏิบัติเชิงเสมือนจริง เพื่อให้ผู้เข้ารับการอบรมได้เกิดความรู้ความเข้าใจในแนวทางปฏิบัติของแต่ละกระบวนการการตรวจสอบและควบคุมความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ และสามารถนำไปปฏิบัติได้จริง

### วัตถุประสงค์:

- เพื่อให้มีความรู้ ความเข้าใจเกี่ยวกับความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing)
- เพื่อให้มีความรู้ ความเข้าใจในการประเมินความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing)
- เพื่อให้มีความรู้ ความเข้าใจในการควบคุมความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing)
- เพื่อให้มีความรู้ ความเข้าใจในกระบวนการตรวจสอบการให้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing)
- เพื่อให้มีความรู้ ความเข้าใจในกระบวนการติดตามและประเมินผลการควบคุมความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing)

### หลักสูตรนี้เหมาะสำหรับ:

- ผู้บริหารหน่วยงานเทคโนโลยีสารสนเทศ
- คณะกรรมการกำกับดูแลการให้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ
- คณะกรรมการบริหารจัดการ และกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Steering Committee)
- คณะกรรมการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- คณะกรรมการกำกับดูแลการตรวจสอบด้านเทคโนโลยีสารสนเทศ
- ผู้บริหารโครงการด้านเทคโนโลยีสารสนเทศ
- ผู้ประสานงานโครงการด้านเทคโนโลยีสารสนเทศ
- ผู้ทำหน้าที่พัฒนาระบบงานด้านเทคโนโลยีสารสนเทศ
- ผู้ที่มีบทบาทหน้าที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- ผู้ที่มีบทบาทหน้าที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ
- ผู้ตรวจสอบภายใน
- ผู้ที่ปฏิบัติงานในหน่วยงานเทคโนโลยีสารสนเทศ
- ผู้สนใจทั่วไป

### เนื้อหาหลักสูตร:

- ความรู้เกี่ยวกับการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing: ITO)
- ความเสี่ยงที่เกิดจากการใช้บริการจาก IT Outsourcing
- หลักการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ จากการให้บริการจาก IT Outsourcing
- ความรู้เกี่ยวกับการตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศจากการให้บริการ IT Outsourcing
- การกำหนดกรอบการตรวจสอบการให้บริการจาก IT Outsourcing (IT Outsourcing Audit Framework)
- การจัดทำโครงสร้างองค์กร และกำหนดบทบาทหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการบริหารจัดการการให้บริการจาก IT Outsourcing
- แนวทางการพัฒนาทักษะความรู้ ความเข้าใจ และเสริมสร้างความตระหนัก ให้แก่บุคลากรที่ปฏิบัติงานเกี่ยวข้องกับการให้บริการจาก IT Outsourcing
- แนวทางการกำกับดูแลการให้บริการจาก IT Outsourcing
- การกำหนดหลักเกณฑ์การกำกับดูแลการให้บริการจาก IT Outsourcing
- การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ มาตรฐานสากลด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ISO/IEC 27001 ให้ครอบคลุมการให้บริการจาก IT Outsourcing
- การติดตาม ตรวจสอบ และประเมินการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ จากการให้บริการจาก IT Outsourcing
- การจัดทำนโยบายการรักษาความปลอดภัยจากการถูกคุกคามทางไซเบอร์ ให้ครอบคลุมการให้บริการจาก IT Outsourcing
- การติดตาม ตรวจสอบ และประเมินการปฏิบัติตามนโยบายการรักษาความปลอดภัยจากการถูกคุกคามทางไซเบอร์ จากการให้บริการจาก IT Outsourcing
- การบริหารจัดการความเสี่ยงจากการให้บริการจาก IT Outsourcing
- การจัดทำนโยบายการบริหารจัดการความเสี่ยงจากการให้บริการจาก IT Outsourcing
- การติดตาม ตรวจสอบ และประเมินการปฏิบัติตามนโยบายการบริหารจัดการความเสี่ยงจากการให้บริการจาก IT Outsourcing

- กระบวนการติดตาม ตรวจสอบ และประเมินความเสี่ยงจากการใช้บริการจาก IT Outsourcing
- การกำหนดหลักเกณฑ์การให้บริการจาก IT Outsourcing
- การกำหนดระเบียบวิธีปฏิบัติและหลักเกณฑ์ในการพิจารณาคัดเลือก IT Outsourcing
- การติดตาม ตรวจสอบ และประเมินการปฏิบัติตามระเบียบวิธีปฏิบัติและหลักเกณฑ์ในการพิจารณาคัดเลือก IT Outsourcing
- การจัดทำสัญญาการให้บริการจาก IT Outsourcing หรือการจัดทำข้อตกลงการให้บริการ (Service Level Agreement: SLA)
- การติดตาม ตรวจสอบ และประเมินการจัดทำสัญญาการให้บริการจาก IT Outsourcing หรือการจัดทำข้อตกลงการให้บริการ (Service Level Agreement: SLA)
- การประเมินความเสี่ยงจากการเชื่อมต่อหรือการเข้าถึงข้อมูลขององค์กรจาก IT Outsourcing
- มาตรการการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการเชื่อมต่อหรือการเข้าถึงข้อมูลจาก IT Outsourcing
- แนวทางการควบคุมการเชื่อมต่อหรือการเข้าถึงข้อมูลขององค์กรจาก IT Outsourcing
- การจัดทำสัญญาหรือข้อตกลงการเชื่อมต่อหรือการเข้าถึงข้อมูลขององค์กรจาก IT Outsourcing
- การติดตาม ตรวจสอบ และประเมินการปฏิบัติตามสัญญาหรือข้อตกลงการเชื่อมต่อหรือการเข้าถึงข้อมูลขององค์กรจาก IT Outsourcing
- กระบวนการและแนวทางบริหารจัดการการเปลี่ยนแปลง (Change Management) ในการใช้บริการจาก IT Outsourcing
- กระบวนการและแนวทางการบริหารจัดการการตั้งค่าระบบ (System Configuration Management) ในการใช้บริการจาก IT Outsourcing
- กระบวนการและแนวทางการบริหารจัดการขีดความสามารถของระบบ (Capacity Management) ในการใช้บริการจาก IT Outsourcing
- การติดตาม ตรวจสอบการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging) ของ IT Outsourcing
- การติดตาม ตรวจสอบการดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring) ของ IT Outsourcing
- การติดตาม ตรวจสอบการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Management and Penetration Testing) ของ IT Outsourcing
- แนวทางการกำหนดมาตรฐานและวิธีปฏิบัติในการสำรองข้อมูล (Data Backup) ให้กับ IT Outsourcing
- แนวทางการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT Incident Management) ที่เกิดจากการใช้บริการจาก IT Outsourcing
- แนวทางการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) จากการใช้บริการจาก IT Outsourcing
- การกำหนดมาตรการการคุ้มครองผู้ใช้บริการขององค์กร (Consumer Protection) ในการใช้บริการจากผู้ให้บริการภายนอก IT Outsourcing
- การตรวจสอบ และติดตามการปฏิบัติตามมาตรการการคุ้มครองผู้ใช้บริการขององค์กร (Consumer Protection) ในการใช้บริการจากผู้ให้บริการภายนอก IT Outsourcing
- แนวทางการบริหารจัดการการติดต่อสื่อสาร (Communication Management) กับผู้ให้บริการ IT Outsourcing
- การติดตาม ตรวจสอบ และประเมินการบริหารจัดการการติดต่อสื่อสาร (Communication Management) กับผู้ให้บริการ IT Outsourcing
- แนวปฏิบัติในการติดตามผลการให้บริการของ IT Outsourcing
- แนวทางการประเมินผลการให้บริการของ IT Outsourcing
- แนวทางการประเมินความเสี่ยงจากการใช้บริการ IT Outsourcing ด้านประสิทธิภาพการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และการปฏิบัติตามกฎหมายของ IT Outsourcing
- แนวทางการกำหนดมาตรฐาน ระเบียบวิธีปฏิบัติว่าด้วยการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง
- แนวทางการวางแผนเพื่อเตรียมการนำเอาบริการที่ใช้กับ IT Outsourcing กลับมาดำเนินการเอง

## Career for the Future Academy: CFA

### วิทยากร:



อาจารย์ภิษัณปดี ธีรสัตยาพิทักษ์

- วิทยากรรับเชิญประจำสถาบันพัฒนาบุคลากรแห่งอนาคต

จำนวนชั่วโมงในการฝึกอบรม: 3 วัน (18 ชั่วโมง)

กำหนดการอบรม: ตามตารางปฏิทินอบรมประจำปี <https://www.career4future.com/trainingprogram>

ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.

### ค่าลงทะเบียนอบรม:

ราคาปกติ	ราคาออนไลน์
9,500 บาท	8,000 บาท

\*\* ราคารวมภาษีมูลค่าเพิ่มแล้ว

\*\* สถาบันฯ เป็นหน่วยงานราชการ จึงไม่อยู่ในเกณฑ์ที่ต้องถูกหักภาษี ณ ที่จ่าย

### สถานที่ฝึกอบรม:

สถาบันพัฒนาบุคลากรแห่งอนาคต

เลขที่ 73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (NSTDA) ชั้น 6

ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400

หมายเหตุ: ในช่วงสถานการณ์การแพร่ระบาดของโรคติดเชื้อไวรัส COVID 19 เพื่อลดการทำกิจกรรมที่มีการรวมตัวกันที่อาจก่อให้เกิดความเสี่ยงต่อการติดเชื้อได้ สถาบันฯ จะมีการปรับรูปแบบการอบรมเป็น "อบรมออนไลน์"

### รูปแบบการเรียนออนไลน์

1. โดยใช้วิธีการสอนแบบฟังบรรยาย และ ดู Presentation ผ่านโปรแกรม Zoom (<https://zoom.us/join>) เพื่อประสิทธิภาพในการเรียน ควรใช้ Internet ที่มีความเสถียร (ไม่แนะนำให้ใช้ Internet ผ่านมือถือ)
2. ลงโปรแกรม Anydesk หรือ Teamviewer ที่เครื่องคอมพิวเตอร์ของท่าน (สำหรับหลักสูตรฝึกปฏิบัติที่ผู้เข้าอบรมจะต้องใช้วิธีการ Remote เพื่อมาใช้เครื่องคอมพิวเตอร์ของสถาบันฯ หรือ กรณีที่วิทยากรต้อง Remote ไปที่เครื่องผู้อบรม และ Share File ที่ใช้ในการอบรม)
3. สำหรับหลักสูตรฝึกปฏิบัติ ขอแนะนำผู้เข้าอบรมเตรียมหน้าจอ 2 หน้าจอ เพื่อแยกการใช้งาน คือ หน้าจอสำหรับ Zoom พร้อมหน้าจอสำหรับปฏิบัติหรือ remote ซึ่งอาจจะเป็นหน้าจอคอมพิวเตอร์ทั้ง 2 เครื่อง หรือ หน้าจอคอมพิวเตอร์ฯ เพื่อใช้ในการ remote และ หน้าจอโทรศัพท์มือถือ/แท็บเล็ต เพื่อใช้กับ zoom
4. จัดตั้งไลน์กลุ่มเพื่อใช้ในการสื่อสารร่วมกันระหว่างวิทยากร ผู้เข้าอบรม และเจ้าหน้าที่ของสถาบันฯ
5. ส่งไฟล์เอกสารให้ก่อนการอบรม
6. จัดส่งวุฒิบัตรภายหลังจบการอบรม

### วิธีการสำรองที่นั่ง:

ติดต่อสำรองที่นั่งล่วงหน้า ในวัน-เวลาราชการ

โทรศัพท์: 0 2644 8150 ต่อ 81886, 81887

โทรสาร: 0 2644 8110

Website: [www.career4future.com](http://www.career4future.com)

E-mail: [training@nstda.or.th](mailto:training@nstda.or.th)