ITM102: Auditing Process of IT Application Systems to Achieve Security: กระบวนการตรวจสอบระบบแอปพลิเคชันเทคโนโลยีสารสนเทศเพื่อให้เกิดความมั่นคงปลอดภัย

หลักการและเหตุผล:

ปัจจุบันโลกได้ก้าวสู่ยุคเศรษฐกิจดิจิทัล เทคโนโลยีสารสนเทศและดิจิทัลสมัยใหม่ได้เข้ามามีบทบาทต่อการขับเคลื่อนธุรกิจให้กับหลายองค์กร เห็นได้จากการรีบเร่งพัฒนาแอปพลิเคชันด้านเทคโนโลยีสารสนเทศต่างๆให้เป็นระบบอัตโนมัติกันมากขึ้น แต่เนื่องด้วยเทคโนโลยีสมัยใหม่ได้มีความซับซ้อนและยุ่งยากต่อการพัฒนา ซึ่งนักพัฒนาระบบส่วนใหญ่ยังขาดความรู้ความชำนาญ และประกอบกับต้องเร่งรีบพัฒนา ระบบงานจึงมีข้อผิดพลาดและช่องโหว่เกิดขึ้น ส่งผลให้องค์กรต้องเผชิญกับสภาวะเสี่ยงต่อการถูกคุกคามในรูปแบบต่างๆ ทั้งจากภายในและภายนอกองค์กร เช่น การกระทำทุจริต การเข้าถึงแอปพลิเคชันโดยไม่ได้รับอนุญาต การล่วงรู้ความลับ การแก้ไขเปลี่ยนแปลงข้อมูลเพื่อแสวงหาผลประโยชน์ให้กับตนเอง และความเสี่ยงจากการถูกคุกคามทางไซเบอร์ จนก่อให้เกิดความเสียหายติดตามมาอย่างมากมาย

ความเสี่ยงดังกล่าวมักจะมาจากสาเหตุหลายประการด้วยกัน เช่น ผู้พัฒนาระบบขาดความพร้อมด้านความรู้ความเข้าใจและความเชี่ยวชาญในเทคโนโลยีที่นำมาใช้เป็นเครื่องมือพัฒนาระบบ ผู้พัฒนาระบบมักขาดประสบการณ์ขาดความเข้าใจในกระบวนการทางธุรกิจ (Business Process) ขององค์กร และด้วยสภาวะการแข็งขันที่แต่ละองค์กรต่างต้องแย่งชิงความเป็นผู้นำ จึงต่างต้องเร่งรีบพัฒนาและปรับปรุงระบบเทคโนโลยีสารสนเทศของตนเองให้แล้วเสร็จโดยเร็ว จากการพัฒนาอย่างเร่งรีบ ได้ก่อให้เกิดปัญหาขึ้นในกระบวนการพัฒนาระบบ เช่น ปัญหาการรวบรวมความต้องการของผู้ใช้งาน (User Requirements) ที่ไม่ถูกต้องครบถ้วนตามความต้องการที่แท้จริงของผู้ใช้งาน รวมถึงระบบควบคุมต่างๆ ที่ควรจะมีก็มักจะถูกละเลยไม่เห็นความสำคัญ และหากองค์กรใดมีกระบวนการทางธุรกิจที่สลับซับซ้อนมีระเบียบวิธีปฏิบัติหลากหลายขั้นตอน ก็ยิ่งทำให้ปัญหาเหล่านี้เกิดขึ้นได้ง่ายยิ่งขึ้น และจะส่งผลให้การออกแบบแอปพลิเคชันเกิดความผิดพลาด และเมื่อแอปพลิเคชันถูกพัฒนาแล้วเสร็จและนำไปติดตั้งใช้งาน ปัญหาที่ตามมาจะเป็นสิ่งที่น่าเป็นห่วงและน่ากังวลเป็นอย่างมาก ก็คือปัญหาความผิดพลาดและช่องโหว่ต่างๆที่จะเกิดขึ้นกับแอปพลิเคชัน อันเป็นผลมาจากการขาดการติดตาม ตรวจสอบและควบคุมดูแลเอาใจใส่ในระหว่างดำเนินการพัฒนาระบบ จนทำให้องค์กรต้องเผชิญกับสภาวะเสี่ยงต่อการถูกคุกคาม ทั้งปัญหาการถูกคุกคามจากภายในองค์กรเอง และการถูกคุกคามความมั่นคงปลอดภัยทางไซเบอร์ จนก่อให้เกิดความเสียหายจากการละเมิดเข้าล่วงรู้ข้อมูลลับ การละเมิดเพื่อแก้ไข หรือทำลายข้อมูล การกระทำทุจริต การละเมิดสิทธิส่วนบุคคล จนทำให้องค์กรถูกฟ้องร้องดำเนินคดีได้รับความเสียหาย

อย่างไรก็ตามหากองค์กรมีกระบวนการกำกับดูแล และการตรวจสอบที่มีประสิทธิภาพ สม่ำเสมอเพียงพอตั้งแต่เริ่มต้นกระบวนการพัฒนาแอปพลิเคชัน ไปจนกระทั่งแอปพลิเคชันนั้นถูกยกเลิกการใช้งาน ก็จะสามารถลดโอกาสที่จะเกิดความเสี่ยงต่อความเสียหายต่างๆ อันเป็นปัญหาและอุปสรรคต่อการดำเนินกิจการขององค์กร ผู้ตรวจสอบเทคโนโลยีสารสนเทศและผู้ตรวจสอบภายในถือได้ว่าเป็นกลไกการควบคุมที่มีความสำคัญมากต่อองค์กร เพราเป็นผู้มีหน้าที่ให้ข้อเสนอแนะ ให้คำแนะนำแนวทางการควบคุมทางกระบวนการธุรกิจ และการควบคุมด้านเทคโนโลยีสารสนเทศ และเป็นผู้มีหน้าที่ในการประเมินผลการควบคุมต่างๆในระบบงานว่ามีประสิทธิภาพประสิทธิผลเพียงพอตามวัตถุประสงค์ที่ได้กำหนดไว้หรือไม่ ซึ่งหากองค์กรมั่นใจว่าผู้มีบทบาทหน้าที่ตรวจสอบแอปพลิเคชันขององค์กรได้มีความรู้ ความเข้าใจในกระบวนการตรวจสอบแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ และมีความรู้ ความเข้าใจตระหนักถึงความเสี่ยงและการควบคุมแอปพลิเคชันด้านเทคโนโลยีสารสนเทศเป็นอย่างดีแล้วก็สามารถสร้างความเชื่อมั่นได้ว่าแอปพลิเคชันด้านเทคโนโลยีสารสนเทศขององค์กร จะมีคุณภาพ มีความถูกต้อง ปลอดภัยและมีความน่าเชื่อถือ

หลักสูตรนี้เป็นการอบรมเชิงปฏิบัติการ และศึกษาจากกรณีศึกษา จากประสบการณ์การกำกับดูแล และการตรวจสอบแอปพลิเคชันด้านเทคโนโลยีสารสนเทศทั้งองค์กรภาครัฐและเอกชน ที่ผู้เข้ารับการอบรมจะได้รับการฝึกปฏิบัติการ เพื่อให้ผู้เข้ารับการอบรมได้เกิดความรู้ ความเข้าใจในแนวทางปฏิบัติของแต่ละกระบวนการการตรวจสอบและควบคุมความเสี่ยงจากการใช้แอปพลิเคชันด้านเทคโนโลยีสารสนเทศ และสามารถนำไปปฏิบัติได้จริง

วัตถุประสงค์:

- เพื่อให้มีความรู้ ความเข้าใจและตระหนักถึงความเสี่ยงที่เกิดกับแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ
- เพื่อให้มีความรู้ ความเข้าใจในการนำกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศมาใช้อย่างมีประสิทธิภาพและสอดคล้องกับความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร
- เพื่อให้มีความรู้ ความเข้าใจในแนวทาง และวิธีปฏิบัติในการกำกับดูแลความมั่นคงปลอดภัยกับแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ ให้เกิดประสิทธิภาพกับองค์กร
- เพื่อให้มีความรู้ ความเข้าใจในการนำกระบวนการตรวจสอบแอปพลิเคชันด้านเทคโนโลยีสารสนเทศมาใช้อย่างมีประสิทธิภาพ

หลักสูตรนี้เหมาะสำหรับ:

- ผู้บริหารหน่วยงานเทคโนโลยีสารสนเทศ
- คณะกรรมการบริหารจัดการ และกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Steering Committee)
- คณะกรรมการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ผู้ที่มีบทบาทหน้าที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ผู้ที่มีบทบาทหน้าที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- คณะกรรมการกำกับดูแลการตรวจสอบด้านเทคโนโลยีสารสนเทศ
- ผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ
- ผู้บริหารโครงการด้านเทคโนโลยีสารสนเทศ
- ผู้ประสานงานโครงการด้านเทคโนโลยีสารสนเทศ
- ผู้ทำหน้าที่พัฒนาแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ
- นักวิเคราะห์ระบบงาน
- ผู้ตรวจสอบภายใน
- ผู้สนใจทั่วไป

เนื้อหาหลักสูตร:

- ภัยคุกคามต่อความปลอดภัยของแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ (IT Application Security Threats)
- ความเสี่ยงที่เกิดขึ้นกับแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ (IT Application Risk)
- หลักการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- การรักษาความมั่นคงปลอดภัยกับแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ ตามมาตรฐานสากลด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ISO/IEC 27001
- แนวทางการประเมินความเสี่ยง (Risk Assessment) กับแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ
- ความรู้ทั่วไปเกี่ยวกับการควบคุมตรวจสอบแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ
- ความจำเป็นของการควบคุมตรวจสอบแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ
- กระบวนการปฏิบัติงานควบคุมตรวจสอบแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ
    - การวางแผนการปฏิบัติงานการควบคุมตรวจสอบแอปพลิเคชัน
    - การปฏิบัติงานตรวจสอบแอปพลิเคชัน
    - การรายงานผลการปฏิบัติงานการควบคุมตรวจสอบแอปพลิเคชัน
    - การติดตามและประเมินผลการนำข้อเสนอแนะในรายงานผลการปฏิบัติงานไปสู่การปฏิบัติ
- แนวทางการควบคุมตรวจสอบเทคโนโลยีสารสนเทศทั่วไป (IT General Control) ที่เกี่ยวข้องกับแอปพลิเคชัน
- แนวทางการควบคุมตรวจสอบแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ (IT Application Control)
    - แนวทางการควบคุมตรวจสอบขั้นตอนการพัฒนาแอปพลิเคชันตามกระบวนการ SDLC
    - แนวทางการควบคุมตรวจสอบการนำเข้าข้อมูล
    - แนวทางการควบคุมตรวจสอบการประมวลผล
    - แนวทางการควบคุมตรวจสอบข้อมูลผลลัพธ์
    - แนวทางการควบคุมตรวจสอบจากการใช้ร่องรอยการตรวจสอบ
    - แนวทางการประเมินผลการตรวจสอบควบคุมระบบงาน
- แนวทางการควบคุมตรวจสอบแอปพลิเคชัน ตามมาตรฐานสากลด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ISO/IEC 27001
    - แนวทางการตรวจสอบการบริหารจัดการการเปลี่ยนแปลง (Change Management) ที่เกี่ยวข้องกับแอปพลิเคชัน
    - แนวทางการตรวจสอบการบริหารจัดการการตั้งค่าระบบ (System Configuration Management) ที่เกี่ยวข้องกับแอปพลิเคชัน
    - แนวทางการตรวจสอบการบริหารจัดการขีดความสามารถของระบบ (Capacity Management) ที่เกี่ยวข้องกับแอปพลิเคชัน
    - แนวทางการตรวจสอบการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging) ที่เกิดขึ้นจากการปฏิบัติงานกับแอปพลิเคชัน
    - แนวทางการตรวจสอบการดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring) ที่เกี่ยวข้องกับแอปพลิเคชัน
    - แนวทางการตรวจสอบการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Management and Penetration Testing) ที่เกี่ยวข้องกับแอปพลิเคชัน
    - แนวทางการตรวจสอบการสำรองข้อมูล (Data Backup) ที่เกี่ยวข้องกับแอปพลิเคชัน

- แนวทางการตรวจสอบการบริหารจัดการเหตุการณ์ผิดปกติ (Incident Management) ที่เกิดจากการใช้งานแอปพลิเคชัน
- แนวทางการตรวจสอบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) ที่เกี่ยวข้องกับแอปพลิเคชัน

- The Open Web Application Security Project (OWASP)
- แนวทางการตรวจสอบ และติดตามการปฏิบัติตามมาตรการการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ในการใช้งานแอปพลิเคชัน

วิทยากร :

อาจารย์ภิธันปดิ์ ถิรสัตยาพิทักษ์
- วิทยากรรับเชิญประจำสถาบันพัฒนาบุคลากรแห่งอนาคต

จำนวนชั่วโมงในการฝึกอบรม: 3 วัน (18 ชั่วโมง)
ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.
กำหนดการอบรม: ตามตารางปฏิทินอบรมประจำปี https://www.career4future.com/trainingprogram

ค่าลงทะเบียนอบรม:

ราคา Onsite	ราคา Online
9,500 บาท	8,600 บาท

* ราคาค่าลงทะเบียนอบรม ไม่รวมภาษีมูลค่าเพิ่ม
* สถาบันฯ เป็นหน่วยงานราชการ จึงไม่อยู่ในเกณฑ์ที่ต้องถูกหักภาษี ณ ที่จ่าย
* ค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมทางวิชาชีพของบริษัทหรือห้างหุ้นส่วนนิติบุคคล สามารถนำไปลดหย่อนภาษีได้ 200%
* สถาบันฯ ได้มีการปรับรูปแบบการอบรมทุกหลักสูตรให้พร้อมบริการ ทั้ง แบบ Onsite (Classroom) และ แบบ Online
* ขอสงวนสิทธิ์ในการเปลี่ยนแปลงกำหนดการ และปรับรูปแบบการอบรมตามความเหมาะสม
* ในการอบรม Online & Onsite สถาบันฯ ขอสงวนสิทธิ์ ไม่บันทึกภาพวีดิโอ หรือบันทึกเสียง ตลอดระยะเวลาการอบรม เนื่องจากเป็นลิขสิทธิ์ร่วมระหว่างวิทยากรกับสถาบันฯ และเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

<u>รูปแบบการเรียน Online</u>

1. โดยใช้วิธีการสอนแบบฟังบรรยาย และ ดู Presentation ผ่านโปรแกรม Zoom (https://zoom.us/join) มีกรณีศึกษา (Case Study) และ ฝึกปฏิบัติ (Workshops)
2. จัดตั้งไลน์กลุ่มเพื่อใช้ในการสื่อสารร่วมกันระหว่างวิทยากร ผู้เข้าอบรม และเจ้าหน้าที่ของสถาบันฯ
3. ส่งไฟล์เอกสารให้ก่อนการอบรม
4. จัดส่งวุฒิบัตรภายหลังจบการอบรม

สถานที่ฝึกอบรม (กรณี Onsite)

สถาบันพัฒนาบุคลากรแห่งอนาคต
เลขที่ 73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (NSTDA) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400

วิธีการการสำรองที่นั่ง:

ติดต่อสำรองที่นั่งล่วงหน้า ในวัน-เวลาราชการ
โทรศัพท์: 0 2644 8150 ต่อ 81886, 81887
โทรสาร: 0 2644 8110
Website: www.career4future.com
E-mail: training@nstda.or.th