

## ITM102: IT Application Audit Process: กระบวนการตรวจสอบแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ

### หลักการและเหตุผล:

ปัจจุบันโลกได้ก้าวสู่ยุคเศรษฐกิจดิจิทัล เทคโนโลยีสารสนเทศและดิจิทัลสมัยใหม่ได้เข้ามามีบทบาทต่อการขับเคลื่อนธุรกิจให้กับหลายองค์กร เห็นได้จากการริเริ่มพัฒนาแอปพลิเคชันด้านเทคโนโลยีสารสนเทศต่างๆ ให้เป็นระบบอัตโนมัติกันมากขึ้น แต่เนื่องด้วยเทคโนโลยีสมัยใหม่ได้มีความซับซ้อนและยุ่งยากต่อการพัฒนา ซึ่งนักพัฒนาระบบส่วนใหญ่ยังขาดความรู้ความชำนาญ และประกอบกับต้องเร่งรีบพัฒนา ระบบงานจึงมีข้อผิดพลาดและช่องโหว่เกิดขึ้น ส่งผลให้องค์กรต้องเผชิญกับสถานะเสี่ยงต่อการถูกคุกคามในรูปแบบต่างๆ ทั้งจากภายในและภายนอกองค์กร เช่น การกระทำทุจริต การเข้าถึงแอปพลิเคชันโดยไม่ได้รับอนุญาต การล่วงรู้ความลับ การแก้ไขเปลี่ยนแปลงข้อมูลเพื่อแสวงหาผลประโยชน์ให้กับตนเอง และความเสี่ยงจากการถูกคุกคามทางไซเบอร์ จนก่อให้เกิดความเสียหายติดตามมาอย่างมากมาย

ความเสี่ยงดังกล่าวมักจะมีมาจากสาเหตุหลายประการด้วยกัน เช่น ผู้พัฒนาระบบขาดความพร้อมด้านความรู้ ความเข้าใจและความเชี่ยวชาญในเทคโนโลยีที่นำมาใช้เป็นเครื่องมือพัฒนาระบบ ผู้พัฒนาระบบมักขาดประสบการณ์ ขาดความเข้าใจในกระบวนการทางธุรกิจ (Business Process) ขององค์กร และด้วยสถานะการแข่งขันของแต่ละองค์กรต่างต้องแย่งชิงความเป็นผู้นำ จึงต่างต้องเร่งรีบพัฒนาและปรับปรุงระบบเทคโนโลยีสารสนเทศของตนเองให้แล้วเสร็จโดยเร็ว จากการพัฒนาอย่างเร่งรีบ ได้ก่อให้เกิดปัญหาขึ้นในกระบวนการพัฒนาระบบ เช่น ปัญหาการรวบรวมความต้องการของผู้ใช้งาน (User Requirements) ที่ไม่ถูกต้องครบถ้วนตามความต้องการที่แท้จริงของผู้ใช้งาน รวมถึงระบบควบคุมต่างๆ ที่ควรจะมีก็มักจะถูกละเลย และหากองค์กรใดมีกระบวนการทางธุรกิจที่ซับซ้อนซับซ้อนมีระเบียบวิธีปฏิบัติหลายขั้นตอน ก็ยิ่งทำให้ปัญหาเหล่านี้เกิดขึ้นได้ง่ายยิ่งขึ้น และจะส่งผลให้การออกแบบแอปพลิเคชันเกิดความผิดพลาด และเมื่อแอปพลิเคชันถูกพัฒนาแล้วเสร็จและนำไปติดตั้งใช้งาน ปัญหาที่ตามมาจะเป็นสิ่งที่น่าเป็นห่วงและน่ากังวลเป็นอย่างมาก ก็คือปัญหาความผิดพลาดและช่องโหว่ต่างๆ ที่จะเกิดขึ้นกับแอปพลิเคชัน อันเป็นผลมาจากการขาดการติดตามตรวจสอบและควบคุมดูแลเอาใจใส่ในระหว่างดำเนินการพัฒนาระบบ จนทำให้องค์กรต้องเผชิญกับสถานะเสี่ยงต่อการถูกคุกคาม ทั้งปัญหาการถูกคุกคามจากภายในองค์กรเอง และการถูกคุกคามความมั่นคงปลอดภัยทางไซเบอร์ จนก่อให้เกิดความเสียหายจากการละเมิดข้อมูลลับ การละเมิดเพื่อแก้ไข หรือทำลายข้อมูล การกระทำทุจริต การละเมิดสิทธิส่วนบุคคล จนทำให้องค์กรถูกฟ้องร้องดำเนินคดีได้รับความเสียหาย

อย่างไรก็ตามหากองค์กรมีกระบวนการกำกับดูแล และการตรวจสอบที่มีประสิทธิภาพ สม่ำเสมอเพียงพอตั้งแต่เริ่มต้นกระบวนการพัฒนาแอปพลิเคชัน ไปจนกระทั่งแอปพลิเคชันนั้นถูกยกเลิกการใช้งาน ก็จะสามารถลดโอกาสที่จะเกิดความเสียหายต่อความเสียหายต่างๆ อันเป็นปัญหาและอุปสรรคต่อการดำเนินกิจการขององค์กร ผู้ตรวจสอบเทคโนโลยีสารสนเทศและผู้ตรวจสอบภายในถือได้ว่าเป็นกลไกการควบคุมที่มีความสำคัญมากต่อองค์กร เพราะเป็นผู้มีหน้าที่ให้ข้อเสนอแนะ ให้คำแนะนำแนวทางการควบคุมทางกระบวนการธุรกิจ และการควบคุมด้านเทคโนโลยีสารสนเทศ และเป็นผู้มีหน้าที่ในการประเมินผลการควบคุมต่างๆ ในระบบงานว่ามีประสิทธิภาพประสิทธิผลเพียงพอตามวัตถุประสงค์ที่ได้กำหนดไว้หรือไม่ ซึ่งหากองค์กรมั่นใจว่าผู้มีส่วนเกี่ยวข้องที่ตรวจสอบแอปพลิเคชันขององค์กรได้มีความรู้ 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

## Career for the Future Academy: CFA

- ผู้ที่มีบทบาทหน้าที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ผู้ที่มีบทบาทหน้าที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- คณะกรรมการกำกับดูแลการตรวจสอบด้านเทคโนโลยีสารสนเทศ
- ผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ
- ผู้บริหารโครงการด้านเทคโนโลยีสารสนเทศ
- ผู้ประสานงานโครงการด้านเทคโนโลยีสารสนเทศ
- ผู้ทำหน้าที่พัฒนาแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ
- นักวิเคราะห์ระบบงาน
- ผู้ตรวจสอบภายใน
- ผู้สนใจทั่วไป

### เนื้อหาหลักสูตร:

- ภัยคุกคามต่อความปลอดภัยของแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ (IT Application Security Threats)
- ความเสี่ยงจากการใช้งานแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ (IT Application Risk)
- หลักการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศกับแอปพลิเคชัน ตามมาตรฐานสากลด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ISO/IEC 27001
- แนวทางการประเมินความเสี่ยง (Risk Assessment) กับแอปพลิเคชันเทคโนโลยีสารสนเทศ
- การควบคุมเทคโนโลยีสารสนเทศทั่วไป (IT General Control) ที่เกี่ยวข้องกับการแอปพลิเคชัน
- การควบคุมแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ (IT Application Control)
  - การควบคุมการนำเข้าข้อมูล
  - การควบคุมการประมวลผล
  - การควบคุมข้อมูลผลลัพธ์
  - การควบคุมโดยใช้ระบบร่องรอยการตรวจสอบ
  - การตรวจสอบและประเมินผลการควบคุมระบบงาน
- The Open Web Application Security Project (OWASP)
- การทดสอบความปลอดภัยกับเว็บแอปพลิเคชัน
- ความรู้ทั่วไปเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ
- ความจำเป็นของการตรวจสอบแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ
- กระบวนการปฏิบัติงานตรวจสอบแอปพลิเคชันด้าน
  - การวางแผนการปฏิบัติงานตรวจสอบแอปพลิเคชัน
  - การปฏิบัติงานตรวจสอบแอปพลิเคชัน
  - การรายงานผลการปฏิบัติงานตรวจสอบแอปพลิเคชัน
  - การติดตามและประเมินผลการนำข้อเสนอแนะในรายงานผลการปฏิบัติงานไปสู่การปฏิบัติ
- แนวทางการตรวจสอบการควบคุมแอปพลิเคชันเทคโนโลยีสารสนเทศ (Auditing IT Application Control)
- แนวทางการตรวจสอบแอปพลิเคชัน ตามมาตรฐานสากลด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ISO/IEC 27001
- แนวทางการตรวจสอบแอปพลิเคชัน ตามแนวนโยบายการรักษาความปลอดภัยจากการคุกคามทางไซเบอร์
- แนวทางการตรวจสอบการพัฒนาแอปพลิเคชันตามกระบวนการ SDLC
- แนวทางการตรวจสอบการบริหารจัดการความเสี่ยง (Risk Management) ด้านแอปพลิเคชันเทคโนโลยีสารสนเทศ
- แนวทางการตรวจสอบการบริหารจัดการการเปลี่ยนแปลง (Change Management) ด้านแอปพลิเคชันเทคโนโลยีสารสนเทศ
- แนวทางการตรวจสอบการบริหารจัดการการตั้งค่าระบบ (System Configuration Management) ด้านแอปพลิเคชันเทคโนโลยีสารสนเทศ
- แนวทางการตรวจสอบการบริหารจัดการขีดความสามารถของระบบ (Capacity Management) ด้านแอปพลิเคชันเทคโนโลยีสารสนเทศ
- แนวทางการตรวจสอบการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging) ที่เกิดขึ้นจากการปฏิบัติงานกับแอปพลิเคชันด้านเทคโนโลยีสารสนเทศ
- แนวทางการตรวจสอบการดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring) ด้านแอปพลิเคชันเทคโนโลยีสารสนเทศ
- แนวทางการตรวจสอบการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Management and Penetration Testing) ด้านแอปพลิเคชันเทคโนโลยีสารสนเทศ
- แนวทางการตรวจสอบการสำรองข้อมูล (Data Backup) ด้านแอปพลิเคชันเทคโนโลยีสารสนเทศ

## Career for the Future Academy: CFA

- แนวทางการตรวจสอบการบริหารจัดการเหตุการณ์ผิดปกติ (Incident Management) ที่เกิดจากการใช้งานแอปพลิเคชันเทคโนโลยีสารสนเทศ
- แนวทางการตรวจสอบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) ที่เกี่ยวข้องกับแอปพลิเคชันเทคโนโลยีสารสนเทศ
- แนวทางการตรวจสอบ และติดตามการปฏิบัติตามมาตรการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ในการใช้งานแอปพลิเคชันเทคโนโลยีสารสนเทศ

### วิทยากร:



อาจารย์ธีรรัตน์ ธีรสัตยาพิทักษ์

- วิทยากรรับเชิญประจำสถาบันพัฒนาบุคลากรแห่งอนาคต

จำนวนชั่วโมงในการฝึกอบรม: 3 วัน (18 ชั่วโมง)

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

ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.

### ค่าลงทะเบียนอบรม:

ราคาปกติ	ราคาออนไลน์
8,500 บาท	7,500 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

## Career for the Future Academy: CFA

---

### 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)