

Stemplus

ITM086: IT Security Risk Management

(การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ)

หลักการและเหตุผล:

ระบบเทคโนโลยีสารสนเทศและดิจิทัลเป็นเทคโนโลยีที่มีส่วนสำคัญต่อการขับเคลื่อนกระบวนเศรษฐกิจโดยรวม ก่อให้เกิดประโยชน์มากมายแก่ทุกภาคส่วนของระบบเศรษฐกิจในทุกวันนี้ แต่ด้วยความก้าวหน้าของเทคโนโลยีในปัจจุบันยังทำให้การใช้งานมีความสลับซับซ้อนมากยิ่งขึ้น ส่งผลให้ผู้ใช้งานส่วนใหญ่ขาดความเข้าใจและตระหนักถึงความเสี่ยงต่อการเกิดความไม่มั่นคงปลอดภัยขึ้น และจะต้องมีการกำกับดูแล บริหารจัดการระบบอย่างไรจึงจะมีความเหมาะสมและมั่นคงปลอดภัย จะเห็นได้ว่าปัจจุบันจะปรากฏรูปแบบความเสี่ยงใหม่ๆ ที่แตกต่างไปจากเดิมเพื่อคุกคามหวังผลประโยชน์จากสารสนเทศขององค์กรหรือสร้างความเสียหายให้เกิดขึ้นกับองค์กร

ดังนั้นจึงเป็นสิ่งจำเป็นและท้าทายผู้บริหารองค์กรว่าจะสามารถรับมือกับเหตุการณ์ที่ไม่พึงประสงค์เพื่อปกป้องรักษาสารสนเทศขององค์กรซึ่งจัดเป็นสินทรัพย์ที่มีมูลค่าและมีความสำคัญต่อการดำเนินภารกิจขององค์กร เช่นเดียวกับสินทรัพย์อื่นๆ เพื่อให้ภารกิจขององค์กรประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้ได้อย่างไร และสิ่งสำคัญหลังจากที่องค์กรได้ดำเนินการตามมาตรการบริหารจัดการความเสี่ยงเป็นที่เรียบร้อยแล้ว องค์กรจะมั่นใจได้อย่างไรว่าความเสี่ยงต่างๆ ได้คงสภาพอยู่ในระดับที่ถูกควบคุมได้จริง และหากปรากฏความเสี่ยงใหม่ๆ ขึ้น องค์กรจะสามารถรับรู้และตอบสนองต่อความเสี่ยงเหล่านั้นได้รวดเร็วเพียงใด และหากองค์กรปล่อยปละละเลยต่อความเสี่ยงเหล่านั้น หรือขาดการบริหารจัดการความเสี่ยงอย่างต่อเนื่อง ก็อาจจะทำให้องค์กรต้องเผชิญกับความเสียหายต่างๆ ที่ติดตามมาจนเกิดเป็นปัญหาอุปสรรคต่อการดำเนินกิจการขององค์กร

อย่างไรก็ตามเพื่อให้องค์กรสามารถดำเนินกิจการให้บรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้ องค์กรควรตระหนักถึงการนำหลักการบริหารจัดการเชิงรุกด้วยการกำกับดูแลการบริหารจัดการความเสี่ยง เพื่อให้เกิดความมั่นใจต่อการดำเนินกิจการต่างๆ ขององค์กรที่ต้องอาศัยเทคโนโลยีสารสนเทศจะสามารถสำเร็จลุล่วงไปได้ด้วยดี การบริหารจัดการความเสี่ยงเป็นการดำเนินการเพื่อรองรับโอกาสการเกิดเหตุการณ์ความเสียหายที่อาจจะเกิดขึ้นในอนาคตอย่างมีหลักการ มีเหตุมีผลและมีวิธีควบคุมความเสี่ยงเพื่อลดโอกาสการเกิดเหตุหรือป้องกันความเสียหายเอาไว้ล่วงหน้า และหากยังมีโอกาสเกิดความเสียหายขึ้น ความเสียหายที่ได้รับก็จะน้อยกว่าการที่ไม่มีการกำกับดูแลด้านการบริหารจัดการความเสี่ยง จึงเป็นการช่วยให้การประกอบกิจการขององค์กรสามารถประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้ได้

หลักสูตรนี้เป็นการอบรมเชิงปฏิบัติการ และศึกษาจากกรณีศึกษาจากประสบการณ์การกำกับดูแลด้านการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศทั้งภาครัฐและเอกชน ที่ผู้เข้ารับการอบรมจะได้รับการฝึกปฏิบัติเชิงเสมือนจริง เพื่อให้ผู้เข้ารับการอบรมได้เกิดความรู้ความเข้าใจในแนวทางปฏิบัติของแต่ละกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและสามารถนำไปปฏิบัติได้จริง

วัตถุประสงค์:

- เพื่อให้มีความรู้ ความเข้าใจ และตระหนักถึงความสำคัญของการกำกับดูแลด้านการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- เพื่อให้มีความรู้ ความเข้าใจในการนำกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศมาใช้อย่างมีประสิทธิภาพและสอดคล้องกับความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร
- เพื่อให้มีความรู้ ความเข้าใจในแนวทางการควบคุมการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- เพื่อให้มีความรู้ ความเข้าใจในบทบาทหน้าที่และความรับผิดชอบต่อการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

หลักสูตรนี้เหมาะสำหรับ:

- ผู้บริหารหน่วยงานเทคโนโลยีสารสนเทศ
- คณะกรรมการบริหารจัดการ และกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Steering Committee)
- คณะกรรมการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ผู้ที่มีบทบาทหน้าที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- ผู้ที่มีบทบาทหน้าที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ผู้ที่ปฏิบัติงานในหน่วยงานเทคโนโลยีสารสนเทศ
- ผู้สนใจทั่วไป

เนื้อหาหลักสูตร:

- ความรู้ทั่วไปเกี่ยวกับความเสี่ยง
- องค์ประกอบของความเสี่ยง
- แนวคิดเพื่อการวิเคราะห์หาสาเหตุ ที่มา และปัจจัยของความเสี่ยง
- หลักการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security Principles)
- ความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
 - ความเสี่ยงจากการเปลี่ยนแปลงทางสภาพแวดล้อมทางธุรกิจและเทคโนโลยี (Agility Risk)
 - ความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Risk)
 - ความเสี่ยงจากการปฏิบัติการทางด้านเทคโนโลยีสารสนเทศขององค์กร (IT Operation Risk)
 - ความเสี่ยงจากการบริหารจัดการโครงการเทคโนโลยีสารสนเทศ (IT Project Management Risk)
- มาตรฐานสากลด้านการบริหารจัดการความเสี่ยง (Risk Management Standard)
- แนวทางการจัดทำโครงสร้างในการกำกับดูแลการดำเนินงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- แนวทางการจัดตั้งคณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- แนวทางการกำหนดบทบาทหน้าที่ในการกำกับดูแลการดำเนินงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA)
- การกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ
 - นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)
 - นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Policy)
- การกำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT Risk Appetite)
- กระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Process)
 - การประเมินความเสี่ยง (Risk Assessment)
 - การระบุความเสี่ยง (Risk Identification)
 - การวิเคราะห์ความเสี่ยง (Risk Analysis)
 - การประเมินค่าความเสี่ยง (Risk Evaluation)
 - การจัดการความเสี่ยง (Risk Treatment)
 - การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)
 - การรายงานความเสี่ยง (Risk Reporting)
- แนวทางจัดทำแผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- แนวทางควบคุมจัดการความเสี่ยงด้วยการบริหารจัดการบุคลากร (Personnel Management)
- แนวทางควบคุมจัดการความเสี่ยงด้วยการส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Awareness)
- แนวทางควบคุมจัดการความเสี่ยงด้วยการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)
- แนวทางควบคุมจัดการความเสี่ยงด้วยการรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)
- แนวทางควบคุมจัดการความเสี่ยงด้วยการควบคุมการเข้าถึง (Access Control) ระบบเทคโนโลยีสารสนเทศ
- แนวทางควบคุมจัดการความเสี่ยงด้วยการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security) ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ
- แนวทางควบคุมจัดการความเสี่ยงด้วยการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Network Security)
- แนวทางควบคุมจัดการความเสี่ยงด้วยการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)
- แนวทางควบคุมจัดการความเสี่ยงด้วยการบริหารจัดการกระบวนการจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ (System Acquisition and Development)
- แนวทางควบคุมจัดการความเสี่ยงด้วยการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident and Problem Management)
- แนวทางควบคุมจัดการความเสี่ยงด้วยการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (Information Technology Contingency Plan)
- แนวทางควบคุมจัดการความเสี่ยงด้วยการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management)
- แนวทางการสื่อสารประชาสัมพันธ์ข้อมูลข่าวสารความเสี่ยงด้านเทคโนโลยีสารสนเทศให้บุคลากรทั่วทั้งองค์กรได้รับทราบ
- Workshops

Career for the Future Academy: CFA

วิทยากร :



อาจารย์ภิษัณปต์ อิศรตยาพิทักษ์

- วิทยากรรับเชิญประจำสถาบันพัฒนาบุคลากรแห่งอนาคต

จำนวนชั่วโมงในการฝึกอบรม: 3 วัน (18 ชั่วโมง)

ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.

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

ค่าลงทะเบียนอบรม:

ราคา Onsite	ราคา Online
10,500 บาท	9,600 บาท

* ราคาค่าลงทะเบียนอบรม **ไม่รวมภาษีมูลค่าเพิ่ม**

* สถาบันฯ เป็นหน่วยงานราชการ จึงไม่อยู่ในเกณฑ์ที่ต้องถูกหักภาษี ณ ที่จ่าย

* ค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมทางวิชาชีพของบริษัทหรือห้างหุ้นส่วนนิติบุคคล สามารถนำไปลดหย่อนภาษีได้ 200%

* สถาบันฯ ได้มีการปรับรูปแบบการอบรมทุกหลักสูตรให้พร้อมบริการ ทั้ง แบบ Onsite (Classroom) และ แบบ Online

* ขอสงวนสิทธิ์ในการเปลี่ยนแปลงกำหนดการ และปรับรูปแบบการอบรมตามความเหมาะสม

* **เฉพาะหลักสูตรนี้** => ผู้ประกอบการที่ส่งบุคลากรเข้ารับการฝึกอบรมในหลักสูตรที่ผ่านการรับรองตามมาตรฐาน Thailand Plus Package สามารถ **"ลดหย่อนภาษีเงินได้ 250%"** ของค่าใช้จ่ายในการฝึกอบรมลูกจ้าง ดูรายละเอียดเพิ่มเติมได้ที่ www.stemplus.or.th

* ในการอบรม Online & Onsite สถาบันฯ ขอสงวนสิทธิ์ ไม่บันทึกภาพวิดีโอ หรือบันทึกเสียง ตลอดระยะเวลาการอบรม เนื่องจากเป็นลิขสิทธิ์ร่วมระหว่างวิทยากรกับสถาบันฯ และเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

รูปแบบการเรียนรู้ Online

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

วิธีการสำรองที่นั่ง:

ติดต่อสำรองที่นั่งล่วงหน้า ในวัน-เวลาราชการ

โทรศัพท์: 0 2644 8150 ต่อ 81886, 81887

โทรสาร: 0 2644 8110

Website: www.career4future.com

E-mail: training@nstda.or.th