Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต
73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400
โทรศัพท์ 0 2644 8150 โทรสาร 0 2644 8110
www.career4future.com

Monitoring and Auditing of Information Technology System Administration Operations Based on ISO/IEC 27001:2023
การติดตามและตรวจสอบการปฏิบัติงานด้านการดูแลระบบเทคโนโลยีสารสนเทศตามมาตรฐานสากล ISO/IEC 27001:2023

ITM132

ฉบับแก้ไข วันที่ 17 ธันวาคม 2568

หลักการและเหตุผล:

ระบบเศรษฐกิจและสังคมในโลกปัจจุบันได้ก้าวสู่ศตวรรษที่ 21 ทำให้เกิดการเปลี่ยนแปลงหลากหลายประการอย่างมีนัยสำคัญ โดยเฉพาะทางด้านเทคโนโลยี เห็นได้จากเทคโนโลยีดิจิทัล ได้มีบทบาทสำคัญอย่างมากต่อการปฏิรูปโครงสร้างเศรษฐกิจของประเทศครั้งใหญ่ เพื่อพัฒนาขับเคลื่อนเศรษฐกิจของประเทศไทยไปสู่ระบบเศรษฐกิจดิจิทัล โดยภาครัฐเองได้ตระหนักถึงความจำเป็นเร่งด่วนในการใช้เทคโนโลยีดิจิทัลมาเป็นเครื่องมือสำคัญในการกระตุ้นเศรษฐกิจของประเทศโดยผลักดันให้ภาคธุรกิจไทยสามารถใช้เทคโนโลยีดิจิทัลในการลดต้นทุนการผลิตสินค้า และบริการ เพิ่มประสิทธิภาพในการดำเนินธุรกิจ ตลอดจนพัฒนาไปสู่การแข่งขันเชิงธุรกิจรูปแบบใหม่ในระยะยาว เพื่อขับเคลื่อนการปฏิรูปประเทศไทยไปสู่ความมั่นคง มั่งคั่ง และยั่งยืน

ด้วยความเจริญก้าวหน้าของเทคโนโลยีดิจิทัลสมัยใหม่ที่แตกต่างและมีความสลับซับซ้อนมากขึ้นกว่าเดิมเป็นอย่างมาก ประกอบกับการเปลี่ยนแปลงที่เกิดขึ้นอย่างรวดเร็วเกินคาดหมาย ทำให้หลายองค์กรที่มีความจำเป็นต้องรีบเร่งนำเทคโนโลยีสมัยใหม่มาใช้งานขาดการเตรียมความพร้อมที่ดีและเพียงพอต่อการปรับเปลี่ยนสู่องค์กรดิจิทัล โดยเฉพาะความพร้อมด้านทักษะ ความรู้ ความเข้าใจของบุคลากร และด้านกระบวนการทางธุรกิจ ด้านกระบวนการดำเนินงานต่างๆ ที่เกี่ยวข้องกับการปฏิบัติงานด้วยระบบเทคโนโลยีสารสนเทศเพื่อให้สามารถรองรับการปฏิบัติงาน ที่ถูกต้อง ปลอดภัย และสอดคล้องกับเทคโนโลยีที่นำมาใช้ใหม่ ทำให้องค์กรต้องเผชิญกับสภาวะเสี่ยงต่อการถูกคุกคาม ทั้งปัญหาการถูกคุกคามความปลอดภัยจากภายในองค์กรเอง และการถูกคุกคามทางไซเบอร์ จนก่อให้เกิดความเสียหายจากการละเมิดเพื่อล่วงรู้ข้อมูลที่เป็นความลับ ละเมิดเพื่อแก้ไข และทำลายข้อมูล การกระทำทุจริต และภัยคุกคามอื่นๆ ติดตามมาอย่างมากมาย ทำให้องค์กรต้องรับความเสียหายทั้งในรูปของการเงิน การถูกฟ้องร้องดำเนินคดี การเสื่อมเสียชื่อเสียง และความน่าเชื่อถือ โดยผู้คุกคามมักจะอาศัยช่องโหว่ จุดอ่อน หรือข้อบกพร่องในรูปแบบต่างๆ จากการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและดิจิทัลขององค์กร หรือจากจุดเชื่อมต่อเข้าสู่ระบบเครือข่ายภายในขององค์กรทั้งจากภายในและภายนอกองค์กร ซึ่งเกิดจากการขาดความพร้อมและข้อบกพร่องในการกำกับดูแล การติดตามและตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ และมีความปลอดภัยเพียงพอ จึงนับเป็นปัญหาสำคัญที่ท้าทายองค์กรว่าจะสามารถรับมือกับเหตุการณ์ที่ไม่พึงประสงค์ เพื่อปกป้องรักษาสารสนเทศอันเป็นสินทรัพย์ที่มีมูลค่า และมีความสำคัญต่อการดำเนินภารกิจขององค์กรให้รอดพ้นจากการถูกคุกคามในรูปแบบต่างๆ ได้อย่างไร

อย่างไรก็ตาม หากองค์กรมีบุคลากรที่มีความรู้ ความเข้าใจ ตระหนักถึงการรักษาความมั่นคงปลอดภัยของข้อมูลและเทคโนโลยีขององค์กร มีกระบวนการบริหารจัดการควบคุมความเสี่ยง มีการกำกับดูแล ติดตามและตรวจสอบที่ดีมีประสิทธิภาพ และที่สำคัญมีระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยของข้อมูล (ISMS) ที่ดีมีประสิทธิภาพตามมาตรฐาน ISO/IEC 27001:2013 โดยเฉพาะในข้อกำหนดที่ A.12 ซึ่งเป็นข้อกำหนดที่สำคัญที่จะสามารถควบคุมการดำเนินงานใดๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศขององค์กร ให้มีความมั่นคงปลอดภัย และหากผู้ปฏิบัติสามารถปฏิบัติได้ตามวัตถุประสงค์ของการควบคุมการรักษาความมั่นคงปลอดภัยกับข้อมูลตามที่องค์กรได้กำหนดไว้อย่างเคร่งครัด ก็จะทำให้มั่นใจได้ว่าองค์กรจะสามารถลดความเสี่ยงจากการถูกคุกคามหรือถูกโจมตีให้ข้อมูลหรือเทคโนโลยีขององค์กรเกิดความเสียหาย หรือหากมีการควบคุมที่ดีแล้วแต่ยังเกิดความเสียหายขึ้นอีก ขนาดของความเสียหายที่จะเกิดขึ้นก็จะเล็กน้อยอยู่ในระดับที่องค์กรยอมรับได้ และไม่ก่อให้เกิดเป็นอุปสรรคต่อการดำเนินภารกิจขององค์กร

ในหลักสูตรนี้ผู้เข้ารับการอบรมจะได้รับความรู้ ความเข้าใจถึงหลักการจัดการการรักษาความมั่นคงปลอดภัยกับข้อมูลในเชิงรุก ด้วยกระบวนการติดตาม การตรวจสอบและการประเมินระบบควบคุมการควบคุมการดำเนินงานใดๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศในปัจจุบันขององค์กร เพื่อเปรียบเทียบกับระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยกับข้อมูลตามมาตรฐาน ISO/IEC 27001:2013 ตามข้อกำหนดที่ A.12 ซึ่งจะช่วยให้องค์กรสามารถทราบได้ว่ามีช่องโหว่ จุดอ่อน ข้อบกพร่องอะไรบ้างที่ยังไม่ได้ถูกควบคุม หรือควรทำการปรับปรุงการควบคุมที่มีอยู่เดิมในปัจจุบันอย่างไรบ้าง ทั้งนี้เพื่อให้สามารถควบคุมการรักษาความมั่นคงปลอดภัยกับระบบสารสนเทศขององค์กรได้อย่างมีประสิทธิผล และเกิดความยั่งยืน จากกรณีศึกษาที่ผ่านการปฏิบัติงานจริงเพื่อให้ผู้เข้ารับการอบรมได้เกิดความรู้ความเข้าใจมากยิ่งขึ้นและสามารถนำไปปฏิบัติได้จริง

วัตถุประสงค์:

- เพื่อให้มีความรู้ ความเข้าใจและตระหนักถึงการรักษาความมั่นคงปลอดภัยด้านการดำเนินงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศขององค์กร
- เพื่อให้มีความรู้ ความเข้าใจเกี่ยวกับระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ
- เพื่อให้มีความรู้ ความเข้าใจในการควบคุมการดำเนินงานใดๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ให้มีความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001:2013 ตามข้อกำหนดที่ A.12
- เพื่อให้มีความรู้ ความเข้าใจในกระบวนการติดตาม และตรวจสอบ เพื่อประเมินผลการควบคุมการรักษาความมั่นคงปลอดภัยต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศหลังจากนำไปใช้งาน

- เพื่อให้มีความรู้ ความเข้าใจในกระบวนการปรับปรุงการควบคุมการรักษาความมั่นคงปลอดภัยกับระบบสารสนเทศขององค์กรให้เกิดประสิทธิภาพมากยิ่งขึ้น

- เพื่อให้มีความรู้ ความเข้าใจถึงแนวทางการทบทวนและปรับปรุงกระบวนการบริหารจัดการการสื่อสารให้มีประสิทธิภาพมากยิ่งขึ้น

หลักสูตรนี้เหมาะสำหรับ:
- ผู้บริหารหรือผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
- ผู้บริหารหรือผู้จัดการฝ่ายความมั่นคงปลอดภัยสารสนเทศ
- ผู้ที่ทำหน้าที่รักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- ผู้ที่ทำหน้าที่บริหารจัดการความเสี่ยงด้านสารสนเทศ
- ผู้ปฏิบัติหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ
- ผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ
- ผู้ตรวจสอบภายใน
- ผู้สนใจทั่วไป

ความรู้พื้นฐาน:
- การรักษาความมั่นคงปลอดภัยด้านสารสนเทศเบื้องต้น

เนื้อหาหลักสูตร:
1. ระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. เป้าหมายการรักษาความมั่นคงปลอดภัยสารสนเทศ
3. โครงสร้างมาตรฐาน ISO/IEC 27001:2013
4. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)
5. การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security) ขององค์กร
6. กระบวนการติดตามตรวจสอบความมั่นคงปลอดภัยสำหรับการดำเนินงาน (A.12 Operations Security)

➢ **ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (A.12.1 Operational Procedures and Responsibilities)**
- ❑ ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (A.12.1.1 Documented Operating Procedures)
  - แนวทางการจัดทำขั้นตอนปฏิบัติงาน ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ให้มีความมั่นคงปลอดภัย
  - การติดตามตรวจสอบการจัดทำขั้นตอนปฏิบัติงาน ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ
- ❑ การบริหารจัดการการเปลี่ยนแปลง (A.12.1.2 Change Management)
  - แนวทางการจัดทำขั้นตอนปฏิบัติงาน การบริหารจัดการการเปลี่ยนแปลงที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศให้มีความมั่นคง ปลอดภัย
  - การติดตามตรวจสอบการจัดทำขั้นตอนปฏิบัติงานการบริหารจัดการการเปลี่ยนแปลงที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ
- ❑ การบริหารจัดการขีดความสามารถของระบบ (A.12.1.3 Capacity Management)
  - แนวทางการจัดทำขั้นตอน หรือแผนการบริหารจัดการทรัพยากร
  - การติดตามตรวจสอบการบริหารจัดการขีดความสามารถของระบบ
- ❑ การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการ ออกจากกัน (A.12.1.4 Separation of Development, Testing and Operational Environments)
  - แนวทางการแยกสภาพแวดล้อมสำหรับการพัฒนา ทดสอบ และการให้บริการออกจากกัน
  - การติดตามตรวจสอบการจัดทำแนวทางการแยกสภาพแวดล้อมสำหรับการพัฒนา ทดสอบ และการให้บริการออกจากกัน

➢ **การป้องกันโปรแกรมไม่ประสงค์ดี (A.12.2 Protection from Malware)**
- ❑ มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (A.12.2.1 Control Against Malware)
  - แนวทางการจัดทำมาตรการในการป้องกัน จัดการโปรแกรมไม่ประสงค์ดี และการสร้างความตระหนักในการป้องกัน จัดการโปรแกรมไม่ประสงค์ดี
  - การติดตามตรวจสอบ การจัดทำและการปฏิบัติตามมาตรการในการป้องกัน จัดการโปรแกรมไม่ประสงค์ดี และการสร้างความตระหนักในการป้องกัน จัดการโปรแกรมไม่ประสงค์ดี

- **การสำรองข้อมูล (A.12.3 Backup)**
  - การสำรองข้อมูล (A.12.3.1 Information Backup)
    - แนวทางการจัดทำขั้นตอนการสำรองข้อมูล และการทดสอบการกู้คืนข้อมูลที่สำรอง
    - การติดตามตรวจสอบ การจัดทำและการปฏิบัติตามขั้นตอนการสำรองข้อมูล และการทดสอบการกู้คืนข้อมูลที่สำรอง

- **การบันทึกข้อมูลล็อกและการเฝ้าระวัง (A.12.4 Logging and Monitoring)**
  - การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (A.12.4.1 Event Logging)
    - การติดตามตรวจสอบ การปฏิบัติการบันทึกข้อมูลล็อกในอุปกรณ์ที่มีความสำคัญ
  - การป้องกันข้อมูลล็อก (A.12.4.2 Protection of Log Information)
    - การติดตามตรวจสอบ มาตรการป้องกันข้อมูลล็อกในอุปกรณ์ที่มีความสำคัญ
  - ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (A.12.4.3 Administrator and Operator Logs)
    - การติดตามตรวจสอบ การบันทึกกิจกรรมการดำเนินงานกับข้อมูลล็อกของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ
  - การตั้งนาฬิกาให้ถูกต้อง (A.12.4.4 Clock Synchronization)
    - การติดตามตรวจสอบ ความถูกต้องเที่ยงตรงของนาฬิกาภายในอุปกรณ์ที่มีความสำคัญ

- **การควบคุมการติดตั้งซอฟต์แวร์ (A.12.5 Control of Operational Software)**
  - การติดตั้งซอฟต์แวร์บนระบบให้บริการ (A.12.5.1 Installation of Software on Operational Systems)
    - แนวทางการกำหนดมาตรฐานซอฟต์แวร์ภายในองค์กร
    - การติดตามตรวจสอบ การปฏิบัติตามมาตรฐานซอฟต์แวร์

- **การบริหารจัดการช่องโหว่ทางเทคนิค (A.12.6 Technical Vulnerability Management)**
  - การบริหารจัดการช่องโหว่ทางเทคนิค (A.12.6.1 Management of Technical Vulnerabilities)
    - การประเมินความเสี่ยงของช่องโหว่ และจุดอ่อน ต่างๆ ของระบบ
    - การติดตามตรวจสอบ การปฏิบัติตามแนวทางการบริหารจัดการช่องโหว่
  - การจำกัดการติดตั้งซอฟต์แวร์ (A.12.6.2 Restrictions on Software Installation)
    - การกำกับดูแล ติดตามตรวจสอบ การติดตั้งซอฟต์แวร์ภายในองค์กร

- **สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (A.12.7 Information Systems Audit Considerations)**
  - มาตรการการตรวจประเมินระบบ (A.12.7.1 Information System Audit Controls)
    - การติดตามตรวจสอบ การปฏิบัติตามมาตรการการตรวจประเมินระบบ

7. กระบวนการปรับปรุงการควบคุมการรักษาความมั่นคงปลอดภัยกับระบบสารสนเทศขององค์กรให้เกิดประสิทธิภาพมากยิ่งขึ้น

ค่าลงทะเบียนอบรม:	9,500 บาท (ไม่รวมภาษีมูลค่าเพิ่ม)
จำนวนชั่วโมงในการฝึกอบรม:	3 วัน (18 ชั่วโมง)
ช่วงเวลาฝึกอบรม:	9.00 - 16.00 น.
กำหนดการอบรม:	ตามตารางปฏิทินอบรมประจำปี https://www.career4future.com/trainingprogram

วิทยากร:

อาจารย์ภิธันปต์ ถิรสัตยาพิทักษ์

- วิทยากรรับเชิญ ประจำสถาบันพัฒนาบุคลากรแห่งอนาคต
- ที่ปรึกษาระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศภาครัฐและเอกชน

หมายเหตุ

- สถาบันฯ มีการจัดเตรียมเครื่องคอมพิวเตอร์ (ในหลักสูตรที่ต้องใช้โปรแกรมคอมพิวเตอร์) เอกสารการอบรม อาหารว่าง และอาหารกลางวัน ให้กับผู้เข้าอบรม
- สถานที่อบรม ห้องอบรม ณ สถาบันพัฒนาบุคลากรแห่งอนาคต อาคาร สวทช. ชั้น 6 ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400
- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ ที่ไม่ใช่ธุรกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
- สถาบันฯ เป็นหน่วยงานราชการ ได้รับการยกเว้นไม่ต้องหักภาษี ณ ที่จ่าย 3%
- ผู้เข้าร่วมอบรมจากหน่วยงานราชการสามารถเบิกค่าลงทะเบียนจากต้นสังกัดได้ ตามระเบียบกระทรวงการคลัง และไม่ถือเป็นวันลาเมื่อได้รับการอนุมัติจากผู้บังคับบัญชา
- ค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมทางวิชาชีพของบริษัทหรือห้างหุ้นส่วนนิติบุคคล สามารถนำไปลดหย่อนภาษีได้ 200%
- สถาบันฯ ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร รูปแบบการอบรม ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- สถาบันฯ ขอสงวนสิทธิ์ ไม่บันทึกภาพ วิดิโอ หรือบันทึกเสียง ตลอดระยะเวลาการอบรม เนื่องจากเป็นลิขสิทธิ์ร่วมระหว่างวิทยากรกับสถาบันฯ และเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
- ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ติดต่อสอบถามรายละเอียด

สถาบันพัฒนาบุคลากรแห่งอนาคต (Career for the Future Academy)
73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400
โทรศัพท์ 0 2644 8150 ต่อ 81886-7
โทรสาร 0 2644 8150
E-mail: training@nstda.or.th
www.career4future.com