## ITM116: Database System Security Audit
## (การตรวจสอบความปลอดภัยของระบบฐานข้อมูล)

**หลักการและเหตุผล:**

ในยุคเศรษฐกิจดิจิทัล (Digital Economic) วิวัฒนาการของเทคโนโลยีดิจิทัลเข้ามามีบทบาทอย่างมากมายในทุกมิติ ทุกองค์กรทั่วโลกต่างตื่นตัวและรับมือกับความเปลี่ยนแปลงจากเทคโนโลยีสมัยใหม่ในครั้งนี้ แม้กระทั่งทางสภาเศรษฐกิจโลก (World Economic Forum) ได้คาดการณ์เอาไว้ว่า จากการเปลี่ยนแปลงเทคโนโลยีดิจิทัลในครั้งนี้จะพลิกโฉมรูปแบบการดำเนินธุรกิจในทุกภาคส่วนทั้งภาคการผลิต การบริการ รูปแบบการดำเนินงานของภาครัฐ และที่สำคัญคือรูปแบบการใช้ชีวิตของมนุษย์ให้แตกต่างไปจากเดิมอย่างสิ้นเชิง เทคโนโลยีดิจิทัลสามารถต่อยอดสร้างนวัตกรรมเพื่อก่อประโยชน์ให้กับองค์กรได้อย่างมากมาย หลายๆองค์กรจึงต่างมุ่งมั่นปรับปรุงและปรับเปลี่ยนเทคโนโลยีของตน ไปสู่เทคโนโลยีดิจิทัลเพื่อตอบสนองต่อความต้องการของผู้บริโภคที่แปรเปลี่ยนไป และเพื่อลดต้นทุนทางธุรกิจให้ต่ำลงจนสามารถยืนหยัดแข่งขันอยู่ได้

หนึ่งในเป้าหมายหลักที่ทุกองค์กรต่างมุ่งมั่นนำเทคโนโลยีดิจิทัลมาใช้พัฒนาและปรับปรุงการบริหารจัดการให้มีประสิทธิภาพ ประสิทธิผลในการดำเนินธุรกิจเพิ่มมากขึ้น ก็คือระบบฐานข้อมูลขององค์กร เพราะเป็นที่ทราบกันดีว่าปัจจุบันเป็นยุคแห่งข้อมูลข่าวสาร โดยเฉพาะข้อมูลข่าวสารออนไลน์ หากผู้ใดสามารถครอบครองข้อมูลและนำเสนอข้อมูลที่ครอบคลุมได้ทุกมิติทั้งในแนวกว้างและลึกได้มากกว่ากันก็ย่อมเป็นผู้ได้เปรียบทางธุรกิจ แต่ด้วยสภาวะที่องค์กรต่างแข็งขันแย่งชิงความเป็นผู้นำ จึงต่างต้องเร่งรีบพัฒนาและปรับปรุงระบบฐานข้อมูลของตนเอง และประกอบกับความประสงค์ขององค์กรที่ต้องการฐานข้อมูลที่มีความหลากหลายครอบคลุมในทุกมิติ ซึ่งจะต้องอาศัยเทคโนโลยีการวิเคราะห์ข้อมูลขั้นสูงที่มีความสลับซับซ้อน และหากผู้พัฒนาและปรับปรุงระบบฐานข้อมูลขาดความรู้ความชำนาญที่ดีพอก็จะทำให้เกิดข้อผิดพลาดขึ้นกับระบบฐานข้อมูล และจะกลายเป็นช่องโหว่ให้เกิดความไม่มั่นคงปลอดภัยกับระบบฐานข้อมูลขององค์กร ทำให้องค์กรต้องเผชิญกับสภาวะเสี่ยงต่อการถูกคุกคาม ทั้งปัญหาการถูกคุกคามความปลอดภัยจากภายในองค์กร และปัญหาการถูกคุกคามทางไซเบอร์ ก่อให้เกิดความเสียหายจากการละเมิดเพื่อให้ล่วงรู้ข้อมูลลับ ละเมิดเพื่อแก้ไขและทำลายข้อมูล การกระทำทุจริต องค์กรถูกฟ้องร้องและภัยคุกคามอื่นๆ ติดตามมาอย่างมากมาย สภาวะเสี่ยงเหล่านี้ล้วนเกิดจากขาดระบบการรักษาความมั่นคงปลอดภัยกับระบบฐานข้อมูลที่ดีพอ

ความเสี่ยงที่เกิดขึ้นจากความไม่มั่นคงปลอดภัยของระบบฐานข้อมูลมักจะมาจากสาเหตุหลายประการด้วยกัน เช่น เกิดจากการพัฒนาและปรับปรุงระบบฐานข้อมูลที่ต้องรีบเร่งให้แล้วเสร็จในระยะเวลาที่จำกัด เกิดจากความล้มเหลวในกระบวนการพัฒนาและปรับปรุงระบบฐานข้อมูลที่องค์กรไม่สามารถควบคุมโครงการได้เองตั้งแต่ต้น เกิดจากองค์กรมีการเปลี่ยนแปลงวัตถุประสงค์และความต้องการของระบบบ่อยเกินไป เกิดจากการมีเจตนาออกแบบและพัฒนาระบบให้เกิดช่องโหว่เพื่อให้สามารถกระทำการทุจริตได้ในภายหลัง เกิดจากการไม่ได้รับการสนับสนุนและมีส่วนร่วมจากผู้ที่เกี่ยวข้อง บุคลากรขาดความรู้ความเข้าใจและทักษะต่อเทคโนโลยีที่นำมาใช้งาน เป็นต้น

อย่างไรก็ตามหากองค์กรมีกระบวนการติดตามตรวจสอบและมีมาตรการควบคุมรักษาความมั่นคงปลอดภัยที่มีประสิทธิภาพประสิทธิผลเพียงพอตั้งแต่เริ่มต้นจัดทำระบบฐานข้อมูลก็จะสามารถป้องกันโอกาสที่จะเกิดความเสียหายที่จะเป็นปัญหาและอุปสรรคต่อการดำเนินภารกิจขององค์กรได้ ดังนั้นผู้ที่เกี่ยวข้องกับการจัดทำและดูแลระบบฐานข้อมูล ผู้ตรวจสอบภายใน ผู้ตรวจสอบเทคโนโลยีสารสนเทศ และผู้ที่มีส่วนใช้งานระบบฐานข้อมูลถือว่าเป็นกลไกควบคุมที่มีความสำคัญมากต่อการรักษาความมั่นคงปลอดภัยระบบฐานข้อมูลองค์กร ซึ่งเป็นผู้มีหน้าที่ต้องคอยให้คำแนะนำด้านการควบคุมความมั่นคงปลอดภัยระบบฐานข้อมูล และมีหน้าที่ในการประเมิน แสดงความคิดเห็นว่าระบบการควบคุมที่ถูกนำมาใช้นั้น มีประสิทธิภาพประสิทธิผลเพียงพอ สามารถปฏิบัติตาม และได้ผลตามวัตถุประสงค์ที่กำหนดไว้หรือไม่ เพื่อสร้างความมั่นใจในความถูกต้องเชื่อถือได้ของสารสนเทศ ทั้งนี้ผู้ที่เกี่ยวข้องกับระบบฐานข้อมูลขององค์กรจะต้องมีความรู้ ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบฐานข้อมูล โดยเฉพาะอย่างยิ่งผู้ที่มีหน้าที่ตรวจสอบระบบฐานข้อมูลขององค์กร ต้องมีความรู้ความเข้าใจถึงความเสี่ยงของระบบฐานข้อมูล วิธีการควบคุมให้ระบบฐานข้อมูลมีความปลอดภัย และกระบวนการติดตามตรวจสอบระบบฐานข้อมูลเป็นอย่างดี

**วัตถุประสงค์ :**

- เพื่อให้มีความรู้ ความเข้าใจการรักษาความมั่นคงปลอดภัยระบบฐานข้อมูล
- เพื่อให้มีความรู้ ความเข้าใจมาตรการการคุ้มครองข้อมูลส่วนบุคคล
- เพื่อให้มีความรู้ ความเข้าใจการออกแบบพัฒนาระบบฐานข้อมูลให้มีความมั่นคงปลอดภัย
- เพื่อให้มีความรู้ ความเข้าใจในการประเมินความเสี่ยงของระบบฐานข้อมูล
- เพื่อให้มีความรู้ ความเข้าใจในความจำเป็นของการตรวจสอบความปลอดภัยของระบบฐานข้อมูล
- เพื่อให้มีความรู้ ความเข้าใจในกระบวนการตรวจสอบความปลอดภัยของระบบฐานข้อมูล
- เพื่อให้มีความรู้ ความเข้าใจในการวางแผนตรวจสอบความปลอดภัยของระบบฐานข้อมูล
- เพื่อให้มีความรู้ ความเข้าใจในการควบคุมระบบฐานข้อมูลให้มีความมั่นคงปลอดภัย
- เพื่อให้มีความรู้ ความเข้าใจในการติดตามและประเมินผลการควบคุมความปลอดภัยระบบฐานข้อมูล

**หลักสูตรนี้เหมาะสำหรับ:**

- ผู้บริหารหรือผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
- ผู้บริหารหรือผู้จัดการด้านความมั่นคงปลอดภัยสารสนเทศ
- ผู้จัดการระบบฐานข้อมูล
- ผู้ออกแบบระบบฐานข้อมูล
- ผู้ที่เกี่ยวข้องกับการพัฒนาระบบงานด้านเทคโนโลยีสารสนเทศ
- ผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ
- ผู้ตรวจสอบภายใน
- ผู้ที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

**เนื้อหาการอบรม:**

- ความรู้เกี่ยวกับระบบฐานข้อมูล
- ภัยคุกคามต่อระบบฐานข้อมูล
- แนวทางการรับมือกับภัยคุกคาม
- การป้องกันระบบฐานข้อมูลให้มั่นคงปลอดภัยอย่างมีประสิทธิภาพ
- การกำหนดมาตรการรักษาความมั่นคงปลอดภัยของระบบฐานข้อมูลในข้อกำหนดขอบเขตของงาน (TOR)
- ความรู้เกี่ยวกับการตรวจสอบความมั่นคงปลอดภัยของระบบฐานข้อมูล
- การกำหนดกรอบการตรวจสอบระบบฐานข้อมูล (Database Audit Framework)
- การตรวจสอบและติดตามการออกแบบระบบฐานข้อมูลให้มีความปลอดภัย
- การกำหนดมาตรฐาน การจัดการข้อมูลและบริหารความมั่นคงปลอดภัยของข้อมูล
- แนวนโยบาย แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบฐานข้อมูล
- การประเมินความเสี่ยงจากความไม่มั่นคงปลอดภัยของระบบฐานข้อมูล
- การกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy and Protection)
- การตรวจสอบการควบคุมการตั้งค่าความมั่นคงปลอดภัยของระบบฐานข้อมูล
- การตรวจสอบการควบคุมสิทธิ์และหน้าที่ในการเข้าถึงระบบฐานข้อมูล
- การตรวจสอบการเข้าถึงฐานข้อมูล (Data Access Auditing)
- การตรวจสอบกิจกรรมการใช้ฐานข้อมูล (Data Activity Monitoring: DAM)
- การตรวจสอบความมั่นคงปลอดภัยของสภาพแวดล้อมที่ติดตั้งระบบฐานข้อมูล
- การตรวจสอบการควบคุมการเปลี่ยนแปลงระบบฐานข้อมูล
- การตรวจสอบประสิทธิภาพของระบบฐานข้อมูล (Database System Performance Monitoring)
- การตรวจสอบการเข้ารหัสข้อมูล (Encryption Data)
- การตรวจสอบการบันทึก Audit Log
- การตรวจสอบและวิเคราะห์ Database Log
- การตรวจสอบการควบคุมความมั่นคงปลอดภัยของฐานข้อมูลด้วยวิว (View)
- การตรวจสอบการจัดการทรานแซคชัน (Transaction Management)
- การตรวจสอบความมั่นคงปลอดภัยระบบฐานข้อมูลด้วยคำสั่ง Structured Query Language: SQL
- การตรวจสอบ SQL Transactions
- การตรวจสอบการสำรองฐานข้อมูล (Database Backup)
- การตรวจสอบการกู้คืนฐานข้อมูล (Database Recovery)
- การตรวจสอบมาตรการสร้างความพร้อมใช้งานและความต่อเนื่องให้กับระบบฐานข้อมูล (Availability and Continuity for the Database System)
- การวิเคราะห์และประเมินความเพียงพอของการควบคุมความมั่นคงปลอดภัยระบบฐานข้อมูล

**วิทยากร : อาจารย์ภิธันปต์ ถิรสัตยาพิทักษ์**

- 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 | 8,750 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 เพื่อลดการทำกิจกรรมที่มีการรวมตัวกันที่อาจจะเกิดความเสี่ยงต่อการติดเชื้อได้ สถาบันฯ จะมีการปรับรูปแบบการอบรมเป็น "อบรมออนไลน์"

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

**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