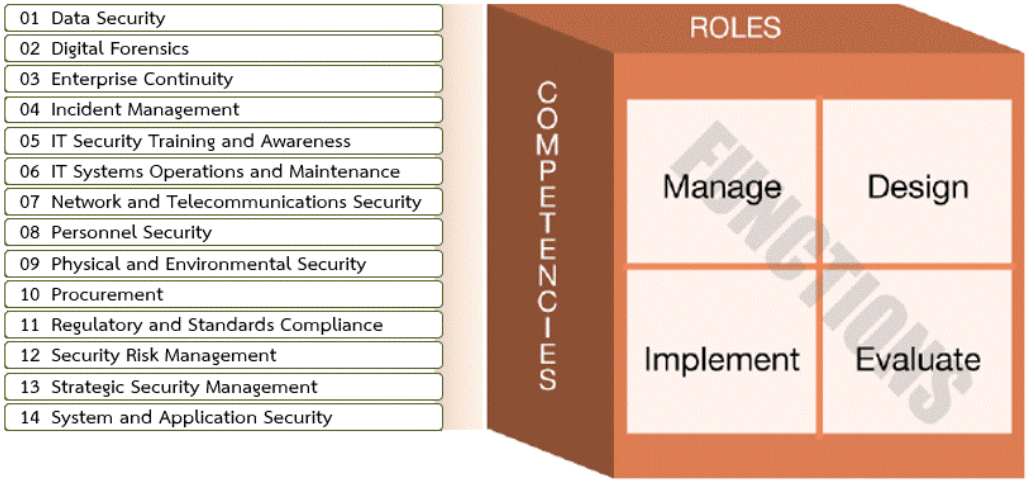
หลักสูตร “การฝึกอบรมและสอบวัดสมรรถนะเพื่อพัฒนามาตรฐานการรับรองบุคลากรด้านความมั่นคงปลอดภัยระบบสารสนเทศของประเทศไทย (iSEC)” ครั้งที่ ๕



CA01 **ความมั่นคงปลอดภัยของข้อมูล**

(Data Security)

การประยุกต์ใช้หลักการ นโยบาย และขั้นตอนการทำงานที่สำคัญ เพื่อรักษาไว้ ซึ่งความลับ ความถูกต้องครบถ้วน ความพร้อมใช้ และความเป็นส่วนตัวของข้อมูล ตามแนวทางจัดการข้อมูลทั้งในรูปแบบสื่ออิเล็กทรอนิกส์และเอกสาร

CA02 **นิติวิทยาทางดิจิตอล**

(Digital Forensics)

องค์ความรู้ด้านเทคนิคการสืบสวนและวิเคราะห์หลักฐานทางดิจิตัล ซึ่งใช้ในการรวบรวม ยืนยันและวิเคราะห์ข้อมูลอิเล็กทรอนิกส์ เพื่อสืบย้อนถึงเหตุอุบัติการณ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศ โดยมีกระบวนการในเชิงสืบสวน รวม ๔ ขั้นตอน ได้แก่ การเตรียมการ การรวบรวมหลักฐาน การวิเคราะห์หลักฐาน และการรายงานผล

CA03 **การสร้างความต่อเนื่องในการดำเนินงาน**

(Enterprise Continuity)

การประยุกต์ใช้หลักการ นโยบาย และขั้นตอนการทำงาน เพื่อให้แน่ใจได้ว่าองค์กรจะสามารถดำเนินการในส่วนงานที่สำคัญได้อย่างต่อเนื่องภายหลังจากเกิดเหตุภัยพิบัติ

CA04 **การบริหารอุบัติการณ์/การจัดการสถานการณ์ที่ไม่พึงประสงค์**

(Incident Management)

องค์ความรู้ด้านกระบวนการในการเตรียมการ การป้องกัน การตรวจจับ การจำกัดความเสียหาย การกำจัด การกู้คืน ตลอดจนการเรียนรู้บทเรียนจากเหตุการณ์ที่มีผลกระทบต่อองค์กร

CA05 **การฝึกอบรมและการสร้างความตระหนักด้านเทคโนโลยีสารสนเทศ**

(IT Security Training and Awareness)

หลักการ แนวปฏิบัติ และวิธีการในการสร้างความตระหนักด้านความมั่นคงปลอดภัยระบบสารสนเทศสำหรับพนักงาน รวมทั้งการจัดฝึกอบรมให้กับบุคลากรตามบทบาทหน้าที่งานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อเสริมสร้างความรู้ ทักษะ และขีดความสามารถที่เหมาะสมในการปฏิบัติหน้าที่งาน

CA06 **การดำเนินงานและการบำรุงรักษาระบบเทคโนโลยีสารสนเทศ**

(IT Systems Operations and Maintenance)

การประยุกต์ใช้หลักการ นโยบาย และขั้นตอนการทำงาน ได้อย่างต่อเนื่อง เพื่อบำรุงรักษา เฝ้าระวัง ควบคุม และ ป้องกันโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและสารสนเทศ ที่ใช้ในองค์กร สำหรับบุคลากรในการปฏิบัติหน้าที่งาน โดยเกี่ยวข้องกับการเก็บรวบรวมข้อมูล วิเคราะห์และรายงาน รวมทั้งการปฏิบัติงานในการจัดการ ความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อให้สอดคล้องกับนโยบายขององค์กร

CA07 **ความมั่นคงปลอดภัยด้านเครือข่ายและโทรคมนาคม**

(Network and Telecommunications Security)

การประยุกต์ใช้หลักการ นโยบาย และขั้นตอนการทำงาน เพื่อรักษาความมั่นคงปลอดภัยของระบบเครือข่าย และบริการโทรคมนาคม รวมทั้งการบำรุงรักษาอุปกรณ์ฮาร์ดแวร์ที่เกี่ยวข้อง

CA08 **ความมั่นคงปลอดภัยด้านบุคลากร**

(Personnel Security)

วิธีการและมาตรการควบคุมที่ใช้ในการสรรหาและคัดเลือกสำหรับทรัพยากรบุคคลขององค์กร ทั้งพนักงานและผู้ให้บริการภายนอก ทั้งนี้ เพื่อส่งเสริมด้านความมั่นคงปลอดภัย โดยครอบคลุมถึงมาตรการควบคุมสำหรับบุคลากร เพื่อใช้ในการป้องกันและตรวจสอบการทำงานของพนักงานที่อาจจะเกิดการละเมิดความมั่นคงปลอดภัยขององค์กร อาทิ การขโมย โจรกรรม การทุจริต การใช้ข้อมูลในทางที่ผิด และ การไม่ปฏิบัติตามข้อกำหนดต่าง ๆ รวมทั้งมาตรการที่เกี่ยวข้อง ได้แก่ การออกแบบโครงสร้างตามหน้าที่งานหรือในระดับองค์กร เช่น การแบ่งแยกหน้าที่ และหมุนเวียนหน้าที่งาน และ การจัดชั้นสารสนเทศ เป็นต้น

CA09 **ความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม**

(Physical and Environmental Security)

วิธีการและมาตรการควบคุมที่ใช้ในการป้องกันทางกายภาพ จากภัยคุกคามทางธรรมชาติหรือจากฝีมือของมนุษย์ สำหรับระบบสาธารณูปโภคพื้นฐานและอาคารขององค์กร รวมถึงสถานที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ

CA10 **การจัดซื้อจัดจ้างและบริหารงานสัญญา**

(Procurement)

การประยุกต์ใช้หลักการ นโยบาย และขั้นตอนการทำงานที่สำคัญ สำหรับการวางแผน การดำเนินการ และการประเมินการจัดซื้อผลิตภัณฑ์และบริการทางด้านระบบสารสนเทศ

CA11 **การปฏิบัติตามกฎระเบียบและมาตรฐาน**

(Regulatory and Standards Compliance)

การประยุกต์ใช้หลักการ นโยบาย และขั้นตอนการทำงาน ที่ช่วยให้องค์กรตอบสนองในการปฏิบัติตามกฎหมาย กฎระเบียบ ข้อบังคับ มาตรฐาน และนโยบายต่าง ๆ บรรลุตามเป้าหมายและข้อกำหนดด้านความมั่นคงปลอดภัยระบบสารสนเทศ

CA12 **การบริหารความเสี่ยงด้านความมั่นคงปลอดภัย**

(Security Risk Management)

การจัดให้มีนโยบาย กระบวนการ ขั้นตอนการทำงาน และเทคโนโลยีที่ใช้ในการระบุปัจจัยเสี่ยงและประเมินความเสี่ยงขององค์กรที่มีต่อทรัพย์สินสารสนเทศ บุคลากร ระบบสาธารณูปโภค และอุปกรณ์ รวมทั้ง การบริหารจัดการกลยุทธ์เพื่อลดความเสี่ยงให้บรรลุด้านความมั่นคงปลอดภัยระบบสารสนเทศและงบประมาณค่าใช้จ่ายที่เหมาะสม

CA13 **การบริหารความมั่นคงปลอดภัยเชิงกลยุทธ์**

(Strategic Security Management)

หลักการ แนวปฏิบัติ และวิธีการ ที่เกี่ยวข้องในการตัดสินใจเชิงบริหารที่มีผลต่อผลดำเนินงานขององค์กรในระยะยาว

CA14 **ความมั่นคงปลอดภัยของระบบและโปรแกรมประยุกต์**

(System and Application Security)

หลักการ นโยบาย และขั้นตอนการทำงาน ที่เกี่ยวข้องในการบูรณาการด้านความมั่นคงปลอดภัยระบบสารสนเทศในขั้นตอนการพัฒนาระบบเทคโนโลยีสารสนเทศหรือระบบงาน ก่อนที่จะนำไปใช้งานและการบำรุงรักษาระบบ เพื่อให้แน่ใจได้ว่ามีการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับซอฟต์แวร์อย่างเหมาะสม