ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ
ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

พ.ศ. ๒๕๖๗

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจกำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่หรือเจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์และให้ระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่เป็นไปตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด จึงสมควรกำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้หน่วยงานใช้ในการสร้างความตระหนักรู้ การฝึกอบรม และการศึกษาสำหรับการพัฒนาความรู้ความเชี่ยวชาญของพนักงานเจ้าหน้าที่และบุคลากรที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์อันจะนำไปสู่การยกระดับความมั่นคงปลอดภัยในการป้องกันและรับมือภัยคุกคามทางไซเบอร์ในภาพรวม เพื่อให้การปฏิบัติงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๙ (๕) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในคราวการประชุมครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๓๑ กรกฎาคม ๒๕๖๗ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“หน่วยงาน” หมายความว่า หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

“บุคลากรของหน่วยงาน” หมายความว่า เจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ ไม่หมายความรวมถึงพนักงานเจ้าหน้าที่ที่รัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“การสร้างความตระหนักรู้” (Awareness) หมายความว่า กระบวนการที่มุ่งสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยมีวัตถุประสงค์ให้บุคคลที่เกี่ยวข้องรับทราบข้อกังวลที่เกี่ยวข้องและตอบสนองได้อย่างถูกต้อง

“การฝึกอบรม” (Training) หมายความว่า กระบวนการที่เสริมสร้าง ความรู้ ทักษะ สมรรถนะ และความสามารถของบุคคล หรือกลุ่มบุคคลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จำเป็นตามสายงานที่เกี่ยวข้อง

“การศึกษา” (Education) หมายความว่า กระบวนการเรียนรู้ที่ผสานระหว่างทักษะและสมรรถนะเฉพาะด้านเข้าไว้ด้วยกันเป็นองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อผลิตผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ที่มีวิสัยทัศน์และสามารถตอบสนองในเชิงรุกต่อภัยคุกคามทางไซเบอร์

“แผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม” (Cybersecurity Awareness and Training Program) หมายความว่า แผนงานหรือโครงการที่ใช้เป็นแนวทางให้หน่วยงานใช้ในการออกแบบ พัฒนา นำไปใช้ และบำรุงรักษาเพื่อสร้างความตระหนักรู้และการฝึกอบรม

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“มาตรการในการยกระดับทักษะความรู้และความเชี่ยวชาญ” หมายความว่า มาตรการที่ดำเนินการโดยสำนักงานและหน่วยงาน เพื่อยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่หรือบุคลากรของหน่วยงาน ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“แนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ” หมายความว่า แนวปฏิบัติที่สำนักงานและหน่วยงานสามารถใช้ในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่หรือบุคลากรของหน่วยงาน

ข้อ ๔ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติรักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้เลขาธิการมีอำนาจตีความและวินิจฉัยชี้ขาด แล้วรายงานให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ทั้งนี้ การตีความและคำวินิจฉัยของเลขาธิการให้เป็นที่สุด

หมวด ๑
มาตรการในการยกระดับทักษะความรู้และความเชี่ยวชาญให้แก่บุคลากรของหน่วยงาน

ส่วนที่ ๑
มาตรการของสำนักงาน

ข้อ ๕ เพื่อส่งเสริมและสนับสนุนการเรียนรู้และการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ให้สำนักงานสนับสนุนหน่วยงาน ดังต่อไปนี้

(๑) ส่งเสริมให้เกิดการพัฒนามาตรฐานและกฎเกณฑ์ เพื่อสร้างความเชื่อมั่น และอำนวยความสะดวกในการดำเนินการภายใต้การกำกับดูแลอย่างเหมาะสม เป็นธรรม และแข่งขันได้

(๒) สนับสนุนให้เกิดการเรียนรู้อิเล็กทรอนิกส์ (e-Learning) ผ่านโครงสร้างพื้นฐานโครงข่ายอินเทอร์เน็ต ให้ครอบคลุมการเข้าถึงทุกภาคส่วนอย่างมีประสิทธิภาพ

(๓) สนับสนุนให้หน่วยงานที่มีความเสี่ยงต่อภัยคุกคามทางไซเบอร์สูงมีมาตรการควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยพัฒนาทักษะความรู้และความเชี่ยวชาญของบุคลากรให้ครอบคลุมในทุกด้าน

(๔) ส่งเสริมให้เกิดการลงทุนเพื่อการพัฒนาบุคลากรและการวิจัยเชิงนโยบาย รวมถึงพัฒนานวัตกรรมเพื่อสร้างองค์ความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์

ข้อ ๖ เพื่อประโยชน์ในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรของหน่วยงาน ให้สำนักงานดำเนินการ ดังต่อไปนี้

(๑) กำกับและติดตามการดำเนินมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรของหน่วยงาน

(๒) เป็นศูนย์กลางข้อมูล ให้คำปรึกษา และถ่ายทอดองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์

(๓) สร้างหลักสูตรหรือกิจกรรมมารองรับ เพื่อเป็นหลักสูตรกลางสำหรับหน่วยงานใช้ในการยกระดับทักษะความรู้และความเชี่ยวชาญของบุคลากร และเพิ่มผลลัพธ์ตัวชี้วัดดัชนีความมั่นคงปลอดภัยไซเบอร์ในระดับนานาชาติ

(๔) สนับสนุนการจัดหาทุนสำหรับการอบรมและการสอบใบรับรองผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงาน

ข้อ ๗ ให้สำนักงานประสานงานกับสำนักงบประมาณ สำนักงานคณะกรรมการข้าราชการพลเรือน และหน่วยงานอื่นที่มีอำนาจหน้าที่ในการพิจารณาจัดสรรงบประมาณและอัตรากำลังที่เพียงพอให้แก่หน่วยงานที่เกี่ยวข้อง เพื่อสนับสนุนการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๒
มาตรการของหน่วยงาน

ข้อ ๘ เพื่อเป็นการยกระดับทักษะความรู้และความเชี่ยวชาญของบุคลากรของหน่วยงาน ให้หน่วยงานจัดให้มีมาตรการในการพัฒนาศักยภาพบุคลากรของหน่วยงานของตนในด้านทักษะของบุคลากร โดยให้มีการส่งเสริมและสนับสนุนการเรียนรู้ และการพัฒนาบุคลากรอย่างต่อเนื่อง

การดำเนินการตามมาตรการในการพัฒนาด้านทักษะของบุคลากรตามวรรคหนึ่ง ให้หน่วยงานกำหนดแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม โดยอาจดำเนินการในรูปแบบใดรูปแบบหนึ่ง ดังต่อไปนี้

(๑) แบบรวมศูนย์

(๒) แบบกระจายอำนาจบางส่วน

(๓) แบบกระจายอำนาจอย่างเต็มที่

ข้อ ๙ ให้หน่วยงานทบทวนแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม รวมถึงเอกสาร สื่อ หรือเนื้อหาที่ใช้ในการดำเนินการตามแผนงานหรือโครงการดังกล่าวให้สอดคล้องกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มากขึ้นอยู่เสมอ ทั้งนี้ ให้ทบทวนอย่างน้อยปีละหนึ่งครั้ง

หมวด ๒
มาตรการในการยกระดับทักษะความรู้และความเชี่ยวชาญให้แก่พนักงานเจ้าหน้าที่

ข้อ ๑๐ เพื่อประโยชน์ในการยกระดับทักษะความรู้และความเชี่ยวชาญของพนักงานเจ้าหน้าที่ ให้สำนักงานดำเนินการ ดังต่อไปนี้

(๑) จัดให้มีโครงการพัฒนาศักยภาพพนักงานเจ้าหน้าที่และหลักสูตร หรือโครงการสร้างความตระหนักรู้และการฝึกอบรม รวมถึงแผนงานที่เกี่ยวข้อง โดยสำนักงานต้องดำเนินการจัดประเภทของพนักงานเจ้าหน้าที่ จัดโครงการ จัดทำหลักสูตร และกำหนดแผนงานดังกล่าวให้เหมาะสมกับพนักงานเจ้าหน้าที่แต่ละประเภท ทั้งนี้ ให้เป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยการกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่

(๒) จัดให้มีการฝึกซ้อมตามแผนเผชิญเหตุการณ์ภัยคุกคามไซเบอร์ หรือฝึกซ้อมการดำเนินการตามหน้าที่ร่วมกันอย่างน้อยปีละครั้ง เพื่อให้พนักงานเจ้าหน้าที่แต่ละประเภทตระหนักถึงบทบาทและหน้าที่ของตน และการประสานงานระหว่างพนักงานเจ้าหน้าที่แต่ละประเภทเป็นไปอย่างมีประสิทธิภาพ

(๓) กำกับและติดตามการดำเนินมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่

(๔) จัดทำทะเบียนประวัติทักษะ ความรู้ ความเชี่ยวชาญของพนักงานเจ้าหน้าที่เพื่อติดตามและส่งเสริมการพัฒนาทักษะ ความรู้ ความเชี่ยวชาญ

(๕) จัดทำลำดับทักษะ ความรู้ ความเชี่ยวชาญ รวมถึงผลงานของพนักงานเจ้าหน้าที่ตลอดจนส่งเสริม ยกย่อง และเชิดชูเกียรติพนักงานเจ้าหน้าที่ที่มีพัฒนาการดีเด่น และมีการปฏิบัติงานดีเด่นเพื่อเป็นการเสริมสร้างขวัญกำลังใจในการเรียนรู้และการปฏิบัติหน้าที่

(๖) สนับสนุนการจัดหาทุนสำหรับการอบรมและการสอบใบรับรองผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่พนักงานเจ้าหน้าที่ รวมถึงการอบรมด้านกฎหมายที่เกี่ยวข้องเพื่อป้องกันการดำเนินการที่ไม่สอดคล้องกับกฎหมาย

(๗) จัดอบรมและสัมมนาเพื่อแนะนำเทคนิคใหม่ที่ผู้ไม่ประสงค์ดีใช้ในการจู่โจมรวมถึงกระบวนการหรือเทคโนโลยีใหม่ ๆ ในการป้องกันภัยคุกคามทางไซเบอร์

(๘) กำหนดให้พนักงานเจ้าหน้าที่ต้องเข้ารับการอบรมที่จัดโดยสำนักงาน เพื่อเพิ่มทักษะความสามารถอย่างน้อยปีละหนึ่งครั้ง

(๙) สนับสนุนให้พนักงานเจ้าหน้าที่มีโอกาสมาฝึกงานที่สำนักงาน (On the job training)

(๑๐) สนับสนุนให้พนักงานเจ้าหน้าที่แลกเปลี่ยนความรู้และประสบการณ์ทางด้านความมั่นคงปลอดภัยไซเบอร์ ผ่านการจัดกิจกรรมการทำงานร่วมกับผู้เชี่ยวชาญเฉพาะทาง และกิจกรรมการเรียนรู้นอกสถานที่ (Outing)

(๑๑) ส่งเสริมและสนับสนุนการแลกเปลี่ยนองค์ความรู้ที่เกี่ยวข้องระหว่างหน่วยงาน

(๑๒) จัดทำจดหมายข่าว เว็บบอร์ด หรือการสื่อสารในรูปแบบอื่นใด เพื่อแบ่งปันข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ระหว่างพนักงานเจ้าหน้าที่

หมวด ๓

แนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ
ให้แก่พนักงานเจ้าหน้าที่และบุคลากรของหน่วยงาน

ข้อ ๑๑ การดำเนินการตามมาตรการในข้อ ๕ และข้อ ๑๐ (๑) ให้เป็นไปตามแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดท้ายประกาศนี้

ข้อ ๑๒ ให้สำนักงานพิจารณาปรับปรุงแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่พนักงานเจ้าหน้าที่หรือบุคลากรของหน่วยงานอย่างน้อยหนึ่งครั้งทุกสามปี และแจ้งให้หัวหน้าหน่วยงานทราบถึงแนวทางดังกล่าว

ประกาศ ณ วันที่ ๓ กันยายน พ.ศ. ๒๕๖๗
ภูมิธรรม เวชยชัย
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

แนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ
ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

บทนำ

เพื่อให้เป็นไปตามมาตรา ๙ (๕) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ จึงสมควรกำหนดแนวทางการยกระดับทักษะความรู้และความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่พนักงานเจ้าหน้าที่หรือบุคลากรของหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ขอบเขตการใช้

หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวทางการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. ขอบเขตการพัฒนา

แนวทางการพัฒนาพนักงานเจ้าหน้าที่หรือบุคลากรของหน่วยงานได้กำหนดการดำเนินการไว้ ๒ เรื่อง ดังนี้

๑.๑ ทักษะของบุคลากร (Skillsets) เพื่อกำหนดแนวทางการพัฒนาพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือบุคลากรอื่นที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ให้มีกรอบความคิดและทักษะที่จำเป็นเหมาะสมในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมให้มีการเรียนรู้และทำงานร่วมกัน หรือร่วมกันเป็นเครือข่ายแลกเปลี่ยนองค์ความรู้ และสนับสนุนบุคลากรพัฒนาร่วมกัน ผ่านการปฏิบัติงานในโครงการต่าง ๆ เพื่อสร้างผลลัพธ์ที่เป็นประโยชน์ต่อหน่วยงานอย่างมีประสิทธิภาพ โดยการประเมินและวางแผนการพัฒนาอย่างต่อเนื่อง

๑.๒ ระบบนิเวศในการทำงาน (Ecosystem) ที่ส่งเสริมและสนับสนุนการเรียนรู้และการพัฒนาบุคลากรอย่างต่อเนื่อง เพื่อส่งเสริมให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล มีสภาพแวดล้อมและระบบการทำงานที่เอื้อต่อการเรียนรู้และการพัฒนากรอบความคิดและกรอบทักษะ สำหรับการทำงานด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง และแสดงพฤติกรรมที่คาดหวังออกมาได้อย่างมีประสิทธิผล

๒. การพัฒนาทักษะของบุคลากร (Skillsets)

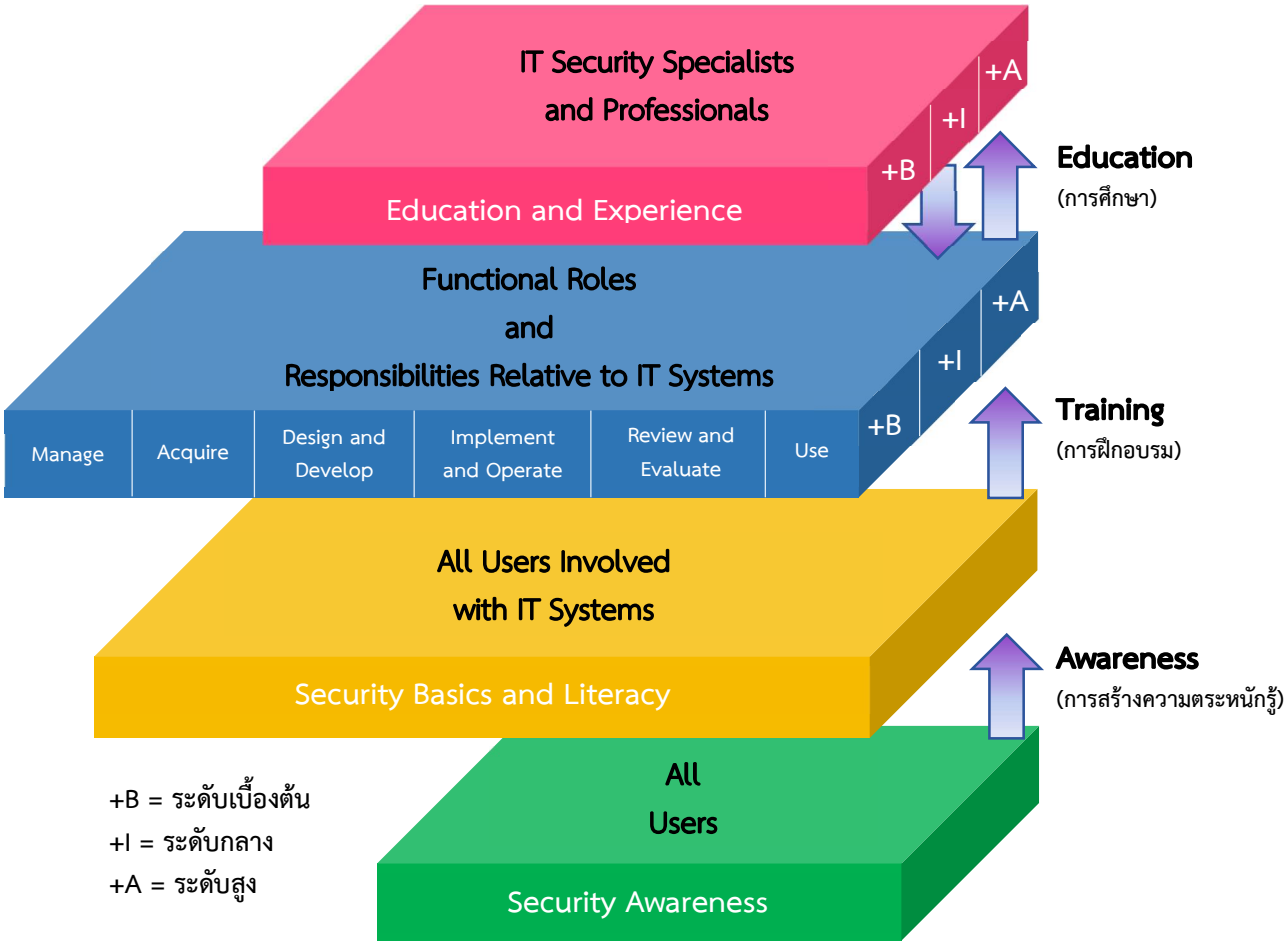
เพื่อให้เป็นไปตามแนวทางการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานซึ่งเป็นที่ยอมรับเป็นการทั่วไปว่าเชื่อถือได้ แนวทางการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ มีการดำเนินการเพื่อส่งเสริมการเรียนรู้ ดังนี้

๒.๑ การสร้างความตระหนักรู้ (Awareness)

๒.๒ การฝึกอบรม (Training)

๒.๓ การศึกษา (Education)

การเรียนรู้ทั้ง ๓ ประการข้างต้น นำมากำหนดความต่อเนื่องของการพัฒนาทักษะของบุคลากรในการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ โดยเริ่มจากการสร้างความตระหนักรู้ สร้างการฝึกอบรมและพัฒนาไปสู่การศึกษา จะได้ดังภาพความต่อเนื่องของการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ด้านล่าง



ภาพความต่อเนื่องของการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์

นอกจากนี้ การดำเนินงานดังกล่าว มีการเปรียบเทียบเพื่อให้เกิดความเข้าใจที่ชัดเจน ดังตารางกรอบการเปรียบเทียบการสร้างความตระหนักรู้ การฝึกอบรม และการศึกษา

ตารางกรอบการเปรียบเทียบการสร้างความตระหนักรู้ การฝึกอบรม และการศึกษา

กรอบการเปรียบเทียบ (Comparative Framework)			
	การสร้างความตระหนักรู้	**การอบรม**	**การศึกษา**
เพื่อ	ให้รู้ว่าคืออะไร	ให้รู้ว่าทำอย่างไร	ให้รู้ว่าทำไมต้องทำ
ระดับ	ข้อมูล	ความรู้	ข้อมูลเชิงลึก
จุดประสงค์การเรียนรู้	สร้างการรับรู้และความจำ	สร้างทักษะ	สร้างความเข้าใจ
ตัวอย่างวิธีสอน	<u>เนื้อหาและสื่อการเรียนรู้</u> - วีดิทัศน์ - จดหมายข่าว/บทความ - โปสเตอร์/สื่อสิ่งพิมพ์	<u>คำแนะนำการปฏิบัติ</u> - การสอนและการสาธิต - ศึกษาจากกรณีศึกษา - ลงมือปฏิบัติจริง	<u>การสอนเชิงทฤษฎี</u> - การสัมมนาและอภิปราย - การอ่านและการศึกษา - การวิจัย
วิธีการวัดผลการเรียนรู้	การเรียนรู้แบบแยกแยะ - คำถามตัวเลือกถูกผิด - คำถามแบบหลายตัวเลือก	<u>การเรียนรู้แบบประยุกต์</u> - การแก้ปัญหา - การวิเคราะห์สถานการณ์เพื่อแก้ปัญหา	<u>การเรียนรู้แบบตีความ</u> - สัมภาษณ์ - เขียนเรียงความ

กรอบการเปรียบเทียบ (Comparative Framework)			
	การสร้างความตระหนักรู้	**การอบรม**	**การศึกษา**
ระยะเวลา	ระยะเวลาสั้น (๓ - ๖ ชั่วโมง)	ระยะเวลาปานกลาง (๓ - ๕ วัน)	ระยะเวลานาน (๑ - ๒ สัปดาห์)

หมายเหตุ : แผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์มีความแตกต่างกันได้ โดยขึ้นอยู่กับจำนวนบุคลากร เงินทุน และการสนับสนุนขั้นพื้นฐาน

๓. บุคคลที่เกี่ยวข้องกับการพัฒนาทักษะของพนักงานเจ้าหน้าที่หรือบุคลากรของหน่วยงาน

เพื่อให้หน่วยงานมั่นใจได้ว่า การจัดทำและดำเนินการตามแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ หน่วยงานต้องเข้าใจบทบาทและความรับผิดชอบของตำแหน่งสำคัญ ๆ ดังต่อไปนี้

๓.๑ หัวหน้าหน่วยงาน (Agency Head)

หัวหน้าหน่วยงานมีความสำคัญอย่างสูงต่อความสำเร็จในการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรของหน่วยงาน ซึ่งรวมถึงการดำเนินแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ที่มีองค์ประกอบที่แข็งแกร่งด้วย ดังนั้น หัวหน้าหน่วยงานควรดำเนินการ ดังนี้

(๑) แต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) หัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Program Manager) และหัวหน้าส่วนงาน (Manager)

(๒) มอบหมายความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ให้บุคลากรที่เกี่ยวข้อง

(๓) กำหนดนโยบายสำหรับการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

(๔) กำกับและติดตามการดำเนินการตามแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ทั่วทั้งหน่วยงาน เพื่อให้แผนงานหรือโครงการได้รับการสนับสนุนทรัพยากรและงบประมาณเป็นอย่างดี และมีประสิทธิภาพ

(๕) วิเคราะห์ผลการประเมินสมรรถนะของบุคลากรและจัดให้มีบุคลากรที่ผ่านการฝึกอบรมอย่างเพียงพอ สำหรับการปกป้องทรัพยากรด้านสารสนเทศ

๓.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงเป็นตำแหน่งที่ทำหน้าที่จัดการการสร้างความตระหนักรู้และการฝึกอบรม และดูแลบุคลากรซึ่งมีความสำคัญต่อการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ควรทำงานร่วมกับหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์และหัวหน้าส่วนงาน เพื่อประโยชน์ในการดำเนินการ ดังนี้

(๑) จัดทำแผนและกำหนดกลยุทธ์โดยรวมสำหรับแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์

(๒) ประชาสัมพันธ์นโยบาย แนวคิดและกลยุทธ์ของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ ของหัวหน้าหน่วยงาน เจ้าของระบบ เจ้าของข้อมูลและบุคลากรอื่นของหน่วยงาน รวมถึงประเมินความเข้าใจนโยบาย แนวคิดและกลยุทธ์ดังกล่าว เพื่อปรับปรุงแนวทางประชาสัมพันธ์

(๓) รับทราบและประเมินความก้าวหน้าของการดำเนินแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ และเสนอรายงานความก้าวหน้าของแผนงานหรือโครงการต่อหัวหน้าหน่วยงาน

(๔) กำหนดแหล่งเงินทุนและดำเนินการให้มีการสนับสนุนงบประมาณสำหรับแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานอย่างเพียงพอ

(๕) ตรวจสอบว่าบุคลากรของหน่วยงานที่มีหน้าที่รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญได้รับการฝึกอบรมที่เพียงพอต่อความรับผิดชอบ

(๖) ประเมินและจัดให้มีการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์อย่างเพียงพอต่อการปฏิบัติงานที่อยู่ในความรับผิดชอบของผู้ใช้แต่ละคน

(๗) ดำเนินการให้มีกลไกการติดตาม และกลไกการรายงานผลที่มีประสิทธิภาพ

๓.๓ หัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Program Manager)

หัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ (หน่วยงานอาจแต่งตั้งบุคคลที่ดำรงตำแหน่งผู้บริหารระดับสูงที่มีหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer: CISO) ในกรณีที่หน่วยงานมีเจ้าหน้าที่ในตำแหน่งนี้ หรืออาจแต่งตั้งบุคคลผู้ดำรงตำแหน่งผู้บริหารหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) เพื่อทำหน้าที่เป็นหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์) มีหน้าที่รับผิดชอบระดับยุทธวิธีสำหรับแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม ในบทบาทนี้ หัวหน้าแผนงานหรือโครงการควรดำเนินการ ดังนี้

(๑) กำหนดกลวิธีและสร้างข้อกำหนดด้านการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์

(๒) ขับเคลื่อนการดำเนินการจัดทำเอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้และการฝึกอบรม ที่พัฒนาขึ้นนั้นเหมาะสมและเป็นปัจจุบันต่อกลุ่มเป้าหมาย

(๓) กำกับและติดตามการเข้าถึงและการใช้เอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้และการฝึกอบรม ของกลุ่มเป้าหมายอย่างมีประสิทธิภาพ

(๔) กำหนดวิธีการสำหรับการรับข้อเสนอแนะเกี่ยวกับเอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้และการฝึกอบรมและวิธีการนำเสนอจากผู้ใช้งานและหัวหน้าส่วนงาน

(๕) ขับเคลื่อนการดำเนินการทบทวนเอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้และการฝึกอบรม เป็นระยะ ๆ เพื่อปรับปรุง เมื่อจำเป็นหรือมีการเปลี่ยนแปลงทางเทคโนโลยี

(๖) สนับสนุนการดำเนินการของผู้บริหารเทคโนโลยีสารสนเทศระดับสูงในการสร้างกลยุทธ์การติดตาม และการรายงานผลการดำเนินการ

๓.๔ หัวหน้าส่วนงาน (Manager)

หัวหน้าส่วนงานที่มีหน้าที่รับผิดชอบในด้านการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่บุคลากรของส่วนงาน ดังนี้

(๑) ทำงานร่วมกับผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์

(๒) สนับสนุนบุคลากรของหน่วยงานที่เกี่ยวข้องในการดำเนินการตามแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ ในบทบาทของเจ้าของระบบสารสนเทศหรือเจ้าของสารสนเทศ

(๓) พิจารณาจัดทำแผนพัฒนาส่วนบุคคล (Individual Development Plan: IDP) สำหรับผู้ใช้งานในบทบาทที่มีความรับผิดชอบสูงด้านความมั่นคงปลอดภัยไซเบอร์

(๔) ส่งเสริมการพัฒนาวิชาชีพและการออกใบรับรองของเจ้าหน้าที่แผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ เจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์เต็มเวลาหรือเจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์นอกเวลา และอื่น ๆ ที่มีหน้าที่สำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์

(๕) กำกับและติดตามการฝึกอบรมของผู้ใช้งานระบบทั้งหมด (ทั้งนี้อาจรวมถึงหน่วยงานภายนอกที่ทำหน้าที่ดูแลระบบ) ทั้งระบบสนับสนุนทั่วไปและระบบงานหลัก ได้รับการฝึกอบรมเกี่ยวกับวิธีการปฏิบัติตามความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์อย่างเหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบ

(๖) กำกับและติดตามความเข้าใจข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของแต่ละระบบสารสนเทศที่ผู้ใช้งาน (ทั้งนี้อาจรวมถึงหน่วยงานภายนอกที่ทำหน้าที่ดูแลระบบ) ต้องใช้งาน

(๗) ประเมินการทำงานของผู้ใช้งานระบบ เพื่อลดข้อผิดพลาดและการละเว้นของผู้ใช้งานเนื่องจากขาดความตระหนักรู้หรือการฝึกอบรม

๓.๕ ผู้ใช้งาน (Users)

ผู้ใช้งานมีส่วนสำคัญต่อการลดข้อผิดพลาดที่เกิดขึ้นอย่างไม่ตั้งใจ และลดช่องโหว่ของเทคโนโลยีสารสนเทศ ทั้งนี้ ผู้ใช้งานประกอบไปด้วย พนักงาน ผู้ที่มาติดต่อ นักวิจัยทั้งภายในและภายนอก ผู้มาเยี่ยมชม บุคคลอื่นในหน่วยงาน (เช่น ฝ่ายบุคคล ฝ่ายฝึกอบรม ฝ่ายประชาสัมพันธ์/สื่อสารองค์กร) และผู้ทำงานร่วมกันหรือผู้ร่วมงานอื่น ๆ ที่ต้องการใช้ระบบสารสนเทศ โดยผู้ใช้งานต้องดำเนินการ ดังนี้

(๑) ทำความเข้าใจและปฏิบัติตามนโยบายและขั้นตอนการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

(๒) ได้รับการฝึกอบรมอย่างเหมาะสมในเรื่องระเบียบปฏิบัติสำหรับระบบสารสนเทศที่ผู้ใช้มีสิทธิ์เข้าถึงได้

(๓) ประเมินตนเองและเสนอความต้องการด้านการฝึกอบรมต่อหัวหน้าส่วนงานและให้ความร่วมมือกับการสร้างความตระหนักรู้และการฝึกอบรม

(๔) ปรับปรุง (Update Patch) ซอฟต์แวร์และแอปพลิเคชันอย่างสม่ำเสมอ

(๕) ตระหนักถึงการดำเนินการปกป้องข้อมูลของหน่วยงานให้มีประสิทธิผลมากขึ้น การดำเนินการเหล่านี้รวมถึงการใช้รหัสผ่านที่เหมาะสม การสำรองข้อมูล การป้องกันไวรัสที่เหมาะสม การรายงานเหตุการณ์ที่น่าสงสัยหรือการละเมิดนโยบายความมั่นคงปลอดภัยไซเบอร์ การปฏิบัติตามกฎที่กำหนดขึ้นเพื่อหลีกเลี่ยงการโจมตีทางวิศวกรรมสังคม (Social Engineering) และกฎเพื่อยับยั้งการแพร่กระจายของสแปมหรือไวรัสและเวิร์ม

ทั้งนี้ หน่วยงานอาจพัฒนาหรือยกระดับความรู้ความเชี่ยวชาญของบุคลากร ให้มีทักษะและความรู้ความสามารถ ดังตัวอย่างใน *ผนวก ก ตัวอย่างทักษะและความรู้ของบุคลากร* ท้ายแนวทางนี้ โดยการดำเนินการดังกล่าวต้องคำนึงถึงกฎหมายและหลักเกณฑ์ ระบบและเทคโนโลยีที่สำคัญสำหรับดำเนินการทางธุรกิจ และภาพรวมภัยคุกคามทางไซเบอร์ (Threat landscape) รวมถึงกระบวนการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับภารกิจหรือการให้บริการเฉพาะด้านของตนด้วย

๔. ขั้นตอนการพัฒนาทักษะของพนักงานเจ้าหน้าที่หรือบุคลากรของหน่วยงาน

ในการสร้างความตระหนักรู้ การฝึกอบรม และการศึกษา เมื่อมีการกำหนดบทบาทและความรับผิดชอบแล้วนั้น ต้องทำความเข้าใจเกี่ยวกับขั้นตอนการสร้างความตระหนักรู้ การฝึกอบรมและการศึกษา โดยการดำเนินการการสร้างความตระหนักรู้ การฝึกอบรม และการศึกษา ประกอบด้วย ๔ ขั้นตอน ดังนี้

๔.๑ การออกแบบแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม (Awareness and Training Program Design)

๔.๒ การพัฒนาเอกสาร/สื่อ เนื้อหาสำหรับแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม (Awareness and Training Material Development)

๔.๓ การดำเนินการแผนงานหรือโครงการ (Program Implementation)

๔.๔ หลังดำเนินการแผนงานหรือโครงการ (Post-Implementation)

โดยในแต่ละขั้นตอน มีรายละเอียดการดำเนินงาน ดังต่อไปนี้

ขั้นตอนที่ ๑ การออกแบบแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม

ในขั้นตอนนี้จะมีการประเมินความต้องการทั่วทั้งหน่วยงาน มีการพัฒนาและอนุมัติกลยุทธ์การฝึกอบรม เอกสารการวางแผนเชิงกลยุทธ์นี้จะระบุงานการดำเนินการที่จะดำเนินการเพื่อสนับสนุนเป้าหมายการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานที่จัดตั้งขึ้น โดยมีขั้นตอนย่อย ดังนี้

๑.๑ การกำหนดโครงสร้างของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม

การกำหนดโครงสร้างของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม สามารถออกแบบ พัฒนาและนำไปใช้ได้หลายรูปแบบ ตามมาตรฐานที่ยอมรับโดยทั่วไป มีการอธิบายแนวทางหรือแบบจำลองไว้ ๓ รูปแบบ คือ

(๑) รูปแบบการจัดการแผนงานหรือโครงการแบบรวมศูนย์ (นโยบาย กลยุทธ์ งบประมาณ แผนการฝึกอบรม และการดำเนินการ อำนาจหน้าที่ทั้งหมดอยู่ที่หน่วยงานส่วนกลาง) เหมาะสมกับหน่วยงานที่มีขนาดเล็ก หรือหน่วยงานที่มีรูปแบบการบริหารแบบบนลงล่าง (Top to Down) ในแบบรูปแบบนี้หน่วยงานส่วนกลางจะสื่อสารและแนะนำหน่วยงานย่อย ในประเด็น (๑.๑) นโยบายและคำสั่งของส่วนกลางเกี่ยวกับการสร้างความตระหนักรู้และการฝึกอบรมเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (๑.๒) กลยุทธ์ เอกสาร/สื่อเนื้อหาความมั่นคงปลอดภัยไซเบอร์ และ (๑.๓) วิธีการนำแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมไปใช้ หน่วยงานส่วนกลางอาจขอความคิดเห็นจากหน่วยงานย่อยเกี่ยวกับประสิทธิภาพของเอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้ วิธีการสื่อสาร หรือการฝึกอบรมด้วยตนเอง ข้อเสนอแนะนี้จะช่วยให้หน่วยงานส่วนกลางสามารถปรับปรุง เอกสาร/สื่อ เนื้อหาตามความจำเป็น เพื่อปรับปรุงแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม รายละเอียดเพิ่มเติมดังภาพรูปแบบการจัดการแบบรวมศูนย์ ด้านล่าง

ภาพรูปแบบการจัดการแบบรวมศูนย์

(๒) รูปแบบการจัดการแผนงานหรือโครงการแบบกระจายอำนาจบางส่วน (นโยบายและกลยุทธ์แบบรวมศูนย์ที่ส่วนกลาง งบประมาณ แผนการฝึกอบรม และการดำเนินการ จะเป็นแบบกระจายตามหน่วยงานย่อย) เหมาะกับหน่วยงานที่ค่อนข้างใหญ่ มีโครงสร้างที่ค่อนข้างกระจายอำนาจและมีหน้าที่รับผิดชอบที่ชัดเจน หน่วยงานมีหน่วยงานย่อยที่มีความหลากหลาย ในรูปแบบนี้ หน่วยงานส่วนกลางจะสื่อสารนโยบายการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ กลยุทธ์การดำเนินแผนงานหรือโครงการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และการจัดสรรงบประมาณโดยรวมสำหรับแต่ละหน่วยงานย่อย หน่วยงานส่วนกลางยังดำเนินการประเมินความต้องการของหน่วยงานย่อย เนื่องจากการประเมินนี้จะเป็นแนวทางในการกำหนดกลยุทธ์สำหรับแผนงานหรือโครงการสร้างความตระหนักรู้ หน่วยงานส่วนกลางอาจให้คำแนะนำแก่หน่วยงานย่อยในการจัดทำแผนการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ อย่างไรก็ตาม การจัดการงบประมาณและการนำไปใช้เป็นความรับผิดชอบของหน่วยงานย่อย

ในบทบาทการกำกับดูแล หน่วยงานกลางอาจร้องขอข้อมูลจากหน่วยงานย่อยในรายการต่าง ๆ เป็นประจำ เช่น สถานะของการพัฒนาโปรแกรมการสร้างความตระหนักรู้และการฝึกอบรม ความคืบหน้าในการดำเนินการและการพัฒนาเอกสาร/สื่อ เนื้อหา และงบประมาณ เมื่อแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมถูกนำมาใช้แล้ว หน่วยงานกลางอาจขอข้อมูลจำนวนผู้เข้าร่วมในการฝึกอบรมการสร้างความตระหนักรู้จำนวนคนที่ผ่านการฝึกอบรมในหัวข้อเฉพาะ และจำนวนผู้ที่ยังไม่ได้เข้าร่วมในกิจกรรมการสร้างความตระหนักรู้ข้อมูลเหล่านี้สามารถช่วยหน่วยงานในการกำหนดระดับการปฏิบัติตามและประสิทธิผลของการนำแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมของหน่วยงานย่อย รายละเอียดเพิ่มเติมดังภาพรูปแบบการจัดการแผนงานหรือโครงการแบบกระจายอำนาจบางส่วน ด้านล่าง

ภาพรูปแบบการจัดการแผนงานหรือโครงการแบบกระจายอำนาจบางส่วน

(๓) รูปแบบการจัดการแผนงานหรือโครงการแบบกระจายอำนาจอย่างเต็มที่ (นโยบายแบบรวมศูนย์ที่ส่วนกลางแต่กลยุทธ์ งบประมาณ แผนการฝึกอบรม และการดำเนินการเป็นรูปแบบกระจาย หน่วยงานย่อยสามารถออกแบบและดำเนินการเองได้) เหมาะกับหน่วยงานที่ค่อนข้างใหญ่ มีการกระจายอำนาจมาก มีหน่วยงานย่อยแบบกึ่งอิสระ มีภารกิจแยกจากหน่วยงานหลัก ในรูปแบบนี้ หน่วยงานส่วนกลางจะสื่อสารนโยบายการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมของหน่วยงาน

และความคาดหวังเกี่ยวกับการดำเนินการและการจัดการโปรแกรม ในรูปแบบนี้ หน่วยงานย่อยมีหน้าที่รับผิดชอบในการจัดทำงบประมาณ สร้าง ดำเนินการ และจัดการแผนงานหรือโครงการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ คำสั่งและความคาดหวังต่อหน่วยงานย่อยจะกำหนดโดยหน่วยงานส่วนกลาง นอกจากนี้ การประเมินความต้องการจะดำเนินการโดยแต่ละหน่วยงานย่อย เนื่องจากหน่วยงานย่อยจะใช้ผลการประเมินมากำหนดกลยุทธ์ที่ดีที่สุดสำหรับแผนงานหรือโครงการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ หน่วยงานย่อยจึงพัฒนาแผนการสร้างความตระหนักรู้และการฝึกอบรม วิธีการสื่อสารที่เหมาะสมที่สุดสำหรับความต้องการของตน หน่วยงานกลางอาจร้องขอสถานะของค่าใช้จ่ายแผนงานหรือโครงการสร้างความตระหนักรู้ ผลการประเมินความต้องการการดำเนินการแผนงานหรือโครงการ และผลการฝึกอบรมที่ดำเนินการจนถึงปัจจุบัน รายละเอียดเพิ่มเติมดังภาพรูปแบบการจัดการแผนงานหรือโครงการแบบกระจายอำนาจอย่างเต็มที่ ด้านล่าง

ภาพรูปแบบการจัดการแผนงานหรือโครงการแบบกระจายอำนาจอย่างเต็มที่

ทั้งนี้การเลือกใช้งานในแต่ละรูปแบบนั้นขึ้นอยู่กับ ๑) ขนาดและการกระจายทางภูมิศาสตร์ของหน่วยงาน ๒) การกำหนดบทบาทและความรับผิดชอบของหน่วยงาน และ ๓) การจัดสรรงบประมาณและอำนาจการบริหาร

๑.๒ การดำเนินการ การประเมินตามความต้องการ

การประเมินความต้องการเป็นกระบวนการที่สามารถใช้เพื่อกำหนดการสร้างความตระหนักรู้และการฝึกอบรมของหน่วยงาน โดยผลลัพธ์ของการประเมินความต้องการสามารถให้เหตุผลเพื่อโน้มน้าวให้ฝ่ายบริหารจัดสรรทรัพยากรที่เพียงพอเพื่อตอบสนองความต้องการกำหนดการสร้างความตระหนักรู้และการฝึกอบรม

ในการดำเนินการประเมินความต้องการ สิ่งสำคัญคือ บุคลากรของหน่วยงานโดยหลักต้องมีส่วนร่วม บุคคลต่อไปนี้ควรมีบทบาทการกำหนดความต้องการฝึกอบรมเพิ่มเติม

(๑) ฝ่ายบริหาร (Executive Management) (หัวหน้าหน่วยงาน ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผู้บริหารหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ) จำเป็นต้องเข้าใจการสั่งการและกฎหมายที่เป็นพื้นฐานสำหรับแผนงานหรือโครงการรักษาความมั่นคงปลอดภัย นอกจากนี้ยังต้องเข้าใจบทบาทและความเป็นผู้นำเพื่อสร้างความมั่นใจให้กับบุคลากรในหน่วยงานของตนเอง

(๒) บุคลากรด้านการรักษาความมั่นคงปลอดภัย (Security Personnel) (ผู้จัดการแผนงานหรือโครงการรักษาความมั่นคงปลอดภัย (Security Program Manager) เจ้าหน้าที่รักษาความมั่นคงปลอดภัย (Security Officer) หรือ เจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Staff)) ทำหน้าที่เป็นที่ปรึกษาผู้เชี่ยวชาญสำหรับหน่วยงาน ดังนั้น จึงต้องมีความรู้เกี่ยวกับนโยบายความมั่นคงปลอดภัยและแนวทางปฏิบัติที่ดีซึ่งได้รับการยอมรับเป็นอย่างดี

(๓) เจ้าของระบบสารสนเทศ (Information System Owners) เจ้าของระบบต้องมีความเข้าใจอย่างกว้างขวางเกี่ยวกับนโยบายความมั่นคงปลอดภัย และความเข้าใจในระดับสูงเกี่ยวกับการควบคุมความมั่นคงปลอดภัยและข้อกำหนดที่ใช้กับระบบที่ตนจัดการ

(๔) ผู้ดูแลระบบและบุคลากรของหน่วยงานฝ่ายสนับสนุนด้านเทคโนโลยีสารสนเทศ (System Administrators and IT Support Personnel) ได้รับความไว้วางใจจากผู้มีอำนาจระดับสูงในการดำเนินการสนับสนุนที่มีความสำคัญต่อแผนงานหรือโครงการความมั่นคงปลอดภัยที่ประสบความสำเร็จ บุคคลเหล่านี้ต้องการความรู้ด้านเทคนิคในระดับที่สูงด้านความมั่นคงปลอดภัย และแนวทางปฏิบัติเพื่อการนำไปใช้งาน

(๕) ผู้จัดการฝ่ายปฏิบัติการและผู้ใช้ระบบ (Operational Managers and System Users) บุคคลเหล่านี้ต้องการความรู้ระดับสูงด้านการตระหนักรู้และการฝึกอบรม เกี่ยวกับการควบคุมความมั่นคงปลอดภัยและพฤติกรรมระบบที่ใช้ในการดำเนินธุรกิจ

แนวทางสำหรับการจัดเก็บความต้องการด้านการสร้างความตระหนักรู้และการฝึกอบรมของหน่วยงาน

- การสัมภาษณ์กับทุกกลุ่มเป้าหมายที่เกี่ยวข้องและบุคคลที่หน่วยงานกำหนด
- การสำรวจหน่วยงาน
- การทบทวนและประเมินทรัพยากรที่มีอยู่ เช่น เอกสาร/สื่อ เนื้อหาที่ใช้ในการสร้างความตระหนักรู้และการฝึกอบรมที่มีอยู่ ณ ปัจจุบัน ตารางการฝึกอบรม และรายการของผู้เข้าร่วมแผนงานหรือโครงการ
- การวิเคราะห์ที่เกี่ยวข้องกับการสร้างความตระหนักรู้และการฝึกอบรม เช่น จำนวนร้อยละ (เปอร์เซ็นต์) ของพนักงานที่ผ่านพื้นฐานของการสร้างความตระหนักรู้และการฝึกอบรม จำนวนร้อยละ (เปอร์เซ็นต์) ของพนักงานที่ได้รับการฝึกอบรมตามหน้าที่เฉพาะ
- การทบทวนแผนการรักษาความมั่นคงปลอดภัยสำหรับระบบสนับสนุนทั่วไปและแอปพลิเคชันหลัก เพื่อกำหนดการเป็นเจ้าของระบบและแอปพลิเคชัน และการรักษาความมั่นคงปลอดภัย
- ตรวจสอบระบบคงคลังและฐานข้อมูลรหัสผู้ใช้งานแอปพลิเคชันเพื่อกำหนดว่าใครมีสิทธิ์เข้าถึงได้
- ทบทวนข้อค้นพบหรือคำแนะนำจากหน่วยงานกำกับดูแล หรือการตรวจสอบแผนงานหรือโครงการเกี่ยวกับข้องกับแผนงานหรือโครงการความมั่นคงปลอดภัยไซเบอร์
- การสนทนาและสัมภาษณ์ผู้บริหาร เจ้าของระบบสนับสนุนทั่วไปและแอปพลิเคชันหลักและพนักงานในหน่วยงานอื่น ๆ ที่ทำงานเกี่ยวข้องกับเทคโนโลยีสารสนเทศ

ทั้งนี้ ตัวอย่างคำถามและรายการตรวจสอบความต้องการของบุคลากรในหน่วยงานเพื่อการสร้างความตระหนักรู้และการฝึกอบรม อยู่ใน*ผนวก ข ตัวอย่างการวัดผลการสร้างความตระหนักรู้และการฝึกอบรม* ท้ายแนวทางนี้

๑.๓ การวางแผนและการพัฒนาแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม

การประเมินความต้องการที่เสร็จสมบูรณ์จะช่วยให้หน่วยงานสามารถพัฒนากลยุทธ์สำหรับการพัฒนาการนำไปใช้ และการบำรุงรักษาแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ แผนงานจะเป็นเอกสารการทำงานที่มีองค์ประกอบหลากหลายประกอบกันเป็นกลยุทธ์ โดยแผนควรพิจารณาเกี่ยวกับองค์ประกอบต่อไปนี้

- นโยบายระดับชาติและระดับท้องถิ่นที่มีความต้องการสร้างความตระหนักรู้และการฝึกอบรมให้สำเร็จ
- ขอบเขตของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม
- บทบาทและความรับผิดชอบของเจ้าหน้าที่ของหน่วยงานที่ทำหน้าที่ออกแบบพัฒนานำไปใช้ และการบำรุงรักษาเอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้ และผู้รับผิดชอบในการตรวจสอบความถูกต้องของการเข้าร่วมของพนักงานหรือการดูเอกสาร/สื่อ เนื้อหาที่เกี่ยวข้อง
- เป้าหมายที่ต้องทำให้สำเร็จในแต่ละด้านของแผนงานหรือโครงการ เช่น การสร้างความตระหนักรู้ การฝึกอบรม การศึกษา การพัฒนาวิชาชีพ (การรับรอง)
- กลุ่มเป้าหมายของแผนงานหรือโครงการแต่ละด้าน
- หลักสูตรหรือเอกสารที่จำเป็น (ถ้ามี) สำหรับกลุ่มเป้าหมายแต่ละกลุ่ม
- จุดประสงค์การเรียนรู้ของแผนงานหรือโครงการแต่ละด้าน
  - หัวข้อที่จะนำเสนอในแต่ละช่วงกิจกรรมหรือหลักสูตร
  - วิธีการปรับใช้สำหรับความคาดหวังของแผนงานหรือโครงการแต่ละด้าน
- เอกสาร ข้อเสนอแนะและหลักฐานการเรียนรู้ของแผนงานหรือโครงการแต่ละด้าน
- การประเมินและการปรับปรุงเนื้อหาสำหรับแผนงานหรือโครงการแต่ละด้านและความถี่ที่เข้าถึงเอกสาร/สื่อของกลุ่มเป้าหมายแต่ละราย

ทั้งนี้ จากองค์ประกอบด้านบน สามารถนำมาเขียนโครงร่างแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมได้ดังตัวอย่างใน*ผนวก ค ตัวอย่างโครงร่างแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม*

๑.๔ การลำดับความสำคัญ

เมื่อแผนและกลยุทธ์การสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยได้รับการสรุปแล้วจะต้องมีการกำหนดตารางการดำเนินการ หากเกิดความจำเป็นบางอย่างในขั้นตอนนี้ เช่น ข้อจำกัดด้านงบประมาณและความพร้อมใช้งานของทรัพยากร การเลือกว่าจะกำหนดตารางการดำเนินการอย่างไรและลำดับแบบใดเป็นสิ่งสำคัญที่ต้องตัดสินใจ ดังนั้น ปัจจัยสำคัญที่ควรพิจารณา มีดังนี้

- **ความพร้อมใช้งานของเอกสาร/สื่อ เนื้อหาหรือทรัพยากร (Availability of Material/ Resources)** หากเอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้และการฝึกอบรมและทรัพยากรที่จำเป็น พร้อมใช้งาน การเริ่มกำหนดแผนงานเป็นกิจกรรมที่ควรทำก่อน อย่างไรก็ตาม หากต้องมีการพัฒนาเนื้อหาหลักสูตรหรือผู้สอน ต้องมีการระบุและกำหนดเวลา ข้อกำหนดเหล่านี้ควรนำมาพิจารณาในการกำหนดลำดับความสำคัญ

• **บทบาทและผลกระทบต่อหน่วยงาน (Role and Organization Impact)**
เป็นเรื่องปกติที่หน่วยงานจะให้ความสำคัญกับบทบาทและความเสี่ยง การสร้างความตระหนักรู้ให้กับคนทั้งหน่วยงานมีความสำคัญระดับสูง เนื่องจากจำเป็นต้องให้พนักงานเข้าใจถึงกฎของแนวทางปฏิบัติที่ดีด้านความมั่นคงปลอดภัยไซเบอร์ นอกจากนี้ ตำแหน่งในหน่วยงานที่ได้รับความไว้วางใจสูงหรือมีผลกระทบสูง เช่น ผู้จัดการแผนงานหรือโครงการความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Program Manager) เจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Officers) ผู้ดูแลระบบ (System Administrators) และผู้ดูแลระบบความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Administrators) ตำแหน่งเหล่านี้จะถูกพิจารณาเป็นกลุ่มที่มีผลกระทบสูง การตรวจสอบให้แน่ใจว่ากลุ่มคนเหล่านี้ได้รับการจัดลำดับความสำคัญ ในระดับสูงในกลยุทธ์การดำเนินการ ตำแหน่งประเภทนี้มักจะสอดคล้องกับประเภทของการเข้าถึงระบบและความเป็นเจ้าของระบบ

• **สถานะของการปฏิบัติในปัจจุบัน (State of Current Compliance)**
เป็นการมองหาจุดบกพร่องที่สำคัญในแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม เช่น การวิเคราะห์จุดบกพร่อง (Gap Analysis) และการกำหนดเป้าหมายไปที่จุดบกพร่องนั้น ในช่วงแรกของการดำเนินแผนงานหรือโครงการ

• **แผนงานหรือโครงการที่สำคัญที่เกี่ยวข้อง (Critical Project Dependencies)**
หากมีแผนงานหรือโครงการที่เกี่ยวข้องกับส่วนของการฝึกอบรมด้านความมั่นคงปลอดภัย เพื่อเตรียมข้อกำหนดที่จำเป็นสำหรับระบบที่เกี่ยวข้อง เช่น ระบบปฏิบัติการ อุปกรณ์ป้องกันการบุกรุกเครือข่าย เครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN) การกำหนดการฝึกอบรมจำเป็นต้องตรวจสอบให้แน่ใจว่าการฝึกอบรมที่เกิดขึ้นนั้นอยู่ภายใต้กรอบเวลาที่กำหนดซึ่งจำเป็นต่อการจัดการส่วนที่เกี่ยวข้องเหล่านี้

๑.๕ การกำหนดตัวชี้วัดพื้นฐาน

การกำหนดตัวชี้วัดพื้นฐาน คือ การตัดสินใจเกี่ยวกับความซับซ้อนของเอกสาร/สื่อเนื้อหาที่จะใช้ในการพัฒนาการสร้างความตระหนักรู้และฝึกอบรมด้านความมั่นคงปลอดภัย ซึ่งขึ้นอยู่กับความเหมาะสมและบทบาทของบุคคลที่จะพัฒนา โดยเอกสาร/สื่อ เนื้อหาที่จะใช้ในการพัฒนามีหลักเกณฑ์สำคัญในการพิจารณา ๒ ประการ ดังนี้

(๑) ตำแหน่งภายในหน่วยงาน ของกลุ่มเป้าหมายที่เข้าร่วม

(๒) ทักษะ ความรู้ด้านความมั่นคงปลอดภัยที่จำเป็นสำหรับตำแหน่งนั้น

ต้องมีการกำหนดความซับซ้อนของเอกสาร/สื่อ เนื้อหาก่อนที่จะเริ่มการพัฒนาและมีการกำหนดตัวชี้วัดพื้นฐานให้กับการเรียนรู้ทั้งสามประเภท คือ การสร้างความตระหนักรู้ การฝึกอบรม และการศึกษา

การกำหนดตัวชี้วัดพื้นฐานสำหรับการเรียนรู้นั้น ควรเน้นที่ข้อกำหนดพฤติกรรมที่คาดหวังสำหรับการใช้ระบบสารสนเทศ ซึ่งข้อกำหนดนี้ควรมาจากนโยบายของหน่วยงานการนำไปใช้กับทุกคนในหน่วยงาน ดังนั้นควรอธิบายให้ชัดเจนเพียงพอเพื่อไม่ให้เกิดความสับสนหรือเข้าใจผิดเมื่อแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมของหน่วยงานเกิดขึ้น และผู้ใช้งานส่วนใหญ่ได้เริ่มเข้าถึงเอกสาร/สื่อ เนื้อหา

การกำหนดตัวชี้วัดพื้นฐาน มีหลายวิธีในการดำเนินการ ตัวอย่างเช่น การพัฒนาหลักสูตรพื้นฐานและการสร้างความตระหนักรู้ โดยในเอกสาร NIST Special Publication 800-16 บทที่ ๓ มีคำแนะนำวิธีการการกำหนดตัวชี้วัดพื้นฐาน และในส่วนที่ ๖ มีการให้ข้อเสนอแนะเพิ่มเติมในการยกระดับการกำหนดตัวชี้วัดพื้นฐาน

๑.๖ เตรียมเงินทุนสำหรับแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม

เมื่อกลยุทธ์การสร้างความตระหนักรู้และการฝึกอบรมได้รับการยอมรับและมีการกำหนดลำดับความสำคัญแล้ว การกำหนดด้านเงินทุนจะต้องเพิ่มเข้าไปในแผนด้วย ต้องมีการกำหนดเกี่ยวกับขอบเขตของการสนับสนุนเงินทุนที่จะจัดสรรตามรูปแบบการดำเนินการ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ของหน่วยงานต้องมีการสื่อสารที่ชัดเจนเกี่ยวกับความคาดหวังในการปฏิบัติ แนวทางที่ใช้ในการกำหนดแหล่งเงินทุน จะพิจารณาตามงบประมาณที่มีอยู่หรือที่คาดการณ์ไว้และลำดับความสำคัญของหน่วยงานอื่น ๆ แผนงานการสร้างความตระหนักรู้และการฝึกอบรมต้องพิจารณาตามข้อกำหนดขั้นต่ำที่ต้องปฏิบัติตามและข้อกำหนดเหล่านั้นต้องได้รับการสนับสนุนจากมุมมองด้านงบประมาณหรือตามสัญญา ข้อกำหนดการฝึกอบรมตามสัญญาควรระบุในเอกสารที่มีผลผูกพัน เช่น บันทึกความเข้าใจ (MOU) วิธีการที่ใช้ในการแสดงความต้องการเงินทุนอาจรวมถึง

- ร้อยละ (เปอร์เซ็นต์) ของงบประมาณการฝึกอบรมโดยรวม
- การจัดสรรต่อผู้ใช้ตามบทบาท เช่น การฝึกอบรมเจ้าหน้าที่รักษาความมั่นคงปลอดภัยหลักและผู้ดูแลระบบ จะมีค่าใช้จ่ายสูงกว่าการฝึกอบรมด้านความมั่นคงปลอดภัยทั่วไปสำหรับผู้ที่อยู่ในหน่วยงานที่ไม่ได้ทำหน้าที่เฉพาะด้านความมั่นคงปลอดภัย
- ร้อยละ (เปอร์เซ็นต์) ของงบประมาณด้านเทคโนโลยีสารสนเทศโดยรวม หรือ
- การจัดสรรเงินทุนอย่างชัดเจนตามองค์ประกอบตามค่าใช้จ่ายการใช้งานโดยรวม

ปัญหาในการดำเนินการการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัย อาจเกิดขึ้นเมื่อการตระหนักด้านความมั่นคงปลอดภัยและความคิดริเริ่มแผนงานหรือโครงการใหม่ในการฝึกอบรมถูกมองว่ามีลำดับความสำคัญต่ำกว่าความคิดริเริ่มงานใหม่อื่น ๆ ของหน่วยงาน ดังนั้น จึงเป็นความรับผิดชอบของผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ในการประเมินลำดับความสำคัญและพัฒนากลยุทธ์เพื่อจัดการกับการขาดแคลนเงินทุน ที่อาจส่งผลกระทบต่อความสามารถของหน่วยงานในการปฏิบัติตามข้อกำหนดการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยที่มีอยู่ ซึ่งอาจหมายถึงการปรับการรับรู้และกลยุทธ์การสร้างความตระหนักรู้และการฝึกอบรมให้สอดคล้องกับงบประมาณที่มีอยู่ การจัดหาเงินทุนเพิ่มเติม หรือการจัดสรรทรัพยากรที่มีอยู่ในปัจจุบันใหม่ อาจหมายความว่าแผนการดำเนินการอาจถูกแบ่งเป็นระยะ (Phase) ในช่วงเวลาที่กำหนดจากเงินทุนที่มีอยู่

ขั้นตอนที่ ๒ การพัฒนาเอกสาร/สื่อ เนื้อหาสำหรับแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม

เมื่อแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมได้รับการออกแบบแล้วนั้น การพัฒนาเอกสาร/สื่อ เนื้อหาเพื่อสนับสนุน ควรมีการคำนึงถึง

(๑) ต้องการเสริมพฤติกรรมอะไร (การรับรู้) และ

(๒) ทักษะหรือกลุ่มทักษะใด ที่ต้องการให้ผู้รับการอบรมได้เรียนรู้ หรือนำไปใช้ (การฝึกอบรม)

การพัฒนาเอกสาร/สื่อ เนื้อหาทั้งสองกรณี ควรเน้นเนื้อหาเฉพาะของผู้ใช้งาน ควรรวมเข้ากับงานของตน หากผู้ใช้งานรู้สึกได้ว่าเนื้อหานั้นถูกพัฒนาขึ้นมาเพื่อพวกเขาโดยเฉพาะ จะทำให้ผู้ใช้งานเห็นว่า “เขามาทำการฝึกอบรมเพราะอะไร และทำไมพวกเขาถึงต้องมา” ทำให้แผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมมีประสิทธิภาพ นอกจากนี้การฝึกอบรมยังเป็นส่วนหนึ่งของการดำเนินงานประจำปีอีกด้วย อย่างไรก็ตาม เอกสาร/สื่อ เนื้อหาจำเป็นต้องมีความน่าสนใจและเป็นปัจจุบัน

ขั้นตอนนี้เน้นที่ทรัพยากรการฝึกอบรมที่มีอยู่ เช่น แหล่งข้อมูล ขอบเขต เนื้อหา และการพัฒนาเอกสาร/สื่อ เนื้อหาในการฝึกอบรม รวมถึงการขอความช่วยเหลือจากผู้รับจ้างภายนอกหากจำเป็น โดยมีขั้นตอนย่อย ดังนี้

๒.๑ การพัฒนาเอกสาร/สื่อ เนื้อหาของการสร้างความตระหนักรู้

คำถามที่ต้องตอบเมื่อเริ่มพัฒนาเอกสาร/สื่อ เนื้อหาสำหรับแผนงานหรือโครงการหรือการรณรงค์ การสร้างความตระหนักรู้ทั่วทั้งหน่วยงาน คือ “เราต้องการให้บุคลากรทุกคนในหน่วยงานตระหนักถึงอะไรเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” แผนการสร้างความตระหนักรู้และการฝึกอบรมควรประกอบด้วยหัวข้อต่าง ๆ ดังนี้ คำแนะนำทางอีเมล เว็บไซต์ข่าวรายวันด้านความมั่นคงปลอดภัยไซเบอร์ออนไลน์ และวารสารต่าง ๆ เป็นแหล่งแนวคิดและเอกสาร/สื่อ เนื้อหาที่ดี นอกจากนี้อาจจะเพิ่มเติมหัวข้อ นโยบายของหน่วยงาน การทบทวนแผนงานหรือโครงการ การตรวจสอบภายใน การทบทวนแผนงานหรือโครงการควบคุมภายในการประเมินตนเอง และการตรวจสอบเฉพาะจุดได้อีกด้วย

๒.๒ การพัฒนาเอกสาร/สื่อ เนื้อหาของการฝึกอบรม

คำถามที่ต้องตอบเมื่อเริ่มพัฒนาเอกสาร/สื่อ เนื้อหาสำหรับหลักสูตรการฝึกอบรมเฉพาะ คือ “ทักษะหรือกลุ่มทักษะใด ที่ต้องการให้ผู้รับการอบรมได้เรียนรู้” แผนการสร้างความตระหนักรู้และการฝึกอบรม ควรระบุผู้ใช้งานหรือกลุ่มของผู้ใช้งาน ที่ควรได้รับการฝึกอบรมปรับให้เหมาะกับความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ซึ่งวิธีการในการสร้างหลักสูตรการฝึกอบรมสำหรับกลุ่มของผู้ใช้งาน ใน NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role-Based and Performance-Based Model มีวิธีการแนะนำในการหาความต้องการและหัวข้อในการสร้างความตระหนักรู้ ไว้ดังตัวอย่าง IT Security Training Matrix – System Administrator ซึ่งเป็นการกำหนดเนื้อหา/หลักสูตรในการฝึกอบรมเฉพาะด้านสำหรับตำแหน่งงานผู้ดูและระบบ (System Administrator)

ตัวอย่าง IT Security Training Matrix — System Administrator

Training Areas	Functional Specialties						
	A Manage	B Acquire	C Design and Develop	D Implement and Operate	E Review and Evaluate	F Use	G Other
1. Laws and Regulations				1D			
2. Security Program							
2.1 Planning							
2.2 Management				2.2D			
3. System Life Cycle Security							
3.1 Initiation							
3.2 Development				3.2D			
3.3 Test and Evaluation				3.3D			
3.4 Implementation			3.4C	3.4D			

Training Areas	Functional Specialties						
	A Manage	B Acquire	C Design and Develop	D Implement and Operate	E Review and Evaluate	F Use	G Other
3.5 Operations	3.5A		3.5C	3.5D			
3.6 Termination				3.6D			
4. Other							

โดยตารางตัวอย่างนี้ แบ่งลักษณะงานของผู้ดูแลระบบออกเป็น ๖ กลุ่ม ซึ่งอิงกับปัจจัยพื้นฐานเนื้อหาในการฝึกอบรมหรือขอบเขตการฝึกอบรม โดยมีรายละเอียดดังนี้

(๑) ผู้จัดการ หมายความว่า บุคคลที่ทำหน้าที่ในการจัดการงาน หรือลักษณะงานด้านเทคโนโลยีสารสนเทศในหน่วยงาน

(๒) ผู้จัดหา หมายความว่า บุคคลที่มีส่วนร่วมในการซื้อผลิตภัณฑ์หรือบริการด้านเทคโนโลยีสารสนเทศ เช่น ทำหน้าที่ในคณะกรรมการคัดเลือกแหล่งที่มาเพื่อประเมินข้อเสนอของผู้จำหน่ายสำหรับระบบสารสนเทศ

(๓) ผู้ออกแบบและพัฒนา หมายความว่า บุคคลที่เป็นผู้ออกแบบและพัฒนาระบบสารสนเทศ หรือโปรแกรมประยุกต์

(๔) ผู้ดำเนินการ หมายความว่า บุคคลที่ดำเนินการ (ดูแล) ระบบสารสนเทศ เช่น เครื่องแม่ข่ายให้บริการเว็บไซต์ เครื่องแม่ข่ายให้บริการจดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายระยะใกล้ (LAN) ระบบเครือข่ายระยะไกล (WAN) เครื่องแม่ข่ายอื่นในระบบ

(๕) ผู้ตรวจสอบและประเมิน หมายความว่า บุคคลที่ทำหน้าที่ตรวจสอบและประเมินการดำเนินงานด้านเทคโนโลยีสารสนเทศ ซึ่งการดำเนินการตรวจสอบและประเมินนี้ เป็นส่วนหนึ่งของโปรแกรมการควบคุมภายในของหน่วยงาน การตรวจสอบภายใน หรือโปรแกรมการตรวจสอบภายนอก

(๖) ผู้ใช้งาน หมายความว่า บุคคลที่เข้าถึงทรัพยากรด้านเทคโนโลยีสารสนเทศหรือใช้เทคโนโลยีสารสนเทศในการทำงาน

แหล่งที่มาของเอกสาร/สื่อ เนื้อหาของการฝึกอบรม

การพิจารณาแหล่งที่มาของเอกสาร/สื่อ และเนื้อหาการฝึกอบรมเพื่อสร้างหลักสูตร คือ การตัดสินใจว่าจะพัฒนาเอกสาร/สื่อ และเนื้อหาภายในหน่วยงานหรือจ้างเหมา หากหน่วยงานมีความเชี่ยวชาญภายในหน่วยงานและสามารถจัดสรรทรัพยากรที่จำเป็นเพื่อพัฒนาเอกสาร/สื่อ เนื้อหาการสอนและหลักสูตรการฝึกอบรมได้ ก็สามารถใช้ NIST Special Publication 800-16 เป็นแนวทางในการกำหนดแหล่งที่มาได้ ตัวอย่างคำถามสำคัญ เพื่อใช้ในการตัดสินใจจะพัฒนาเอกสาร/สื่อ เนื้อหาภายในหน่วยงานหรือจ้างเหมา เช่น

- เรามีทรัพยากรภายในหน่วยงานเพื่อทำงานนี้หรือไม่ รวมถึงคนที่มีทักษะที่เหมาะสมและมีคนเพียงพอที่จะทำงาน
- การพัฒนาเอกสาร/สื่อ และเนื้อหาภายในหน่วยงานคุ้มค่ากว่าเมื่อเทียบกับการจ้างเหมาจากภายนอกหรือไม่
- มีกลไกการจัดหาเงินทุน (งบประมาณ) หรือไม่

• เรามีบุคลากรที่สามารถทำหน้าที่เป็นตัวแทนเจ้าหน้าที่ด้านเทคนิคการทำสัญญา (COTR) และติดตามกิจกรรมของผู้รับจ้างเหมาได้อย่างมีประสิทธิภาพหรือไม่

• หน่วยงานมีทรัพยากรที่จำเป็น เช่น เงินทุนและพนักงานที่มีความเชี่ยวชาญที่จำเป็นเพื่อบำรุงรักษาเอกสาร/สื่อ เนื้อหาหรือไม่ หากได้รับการพัฒนาโดยผู้รับจ้างเหมา

• ความละเอียดอ่อนของเนื้อหาหลักสูตร ห้ามไม่ให้มีผู้รับจ้างเหมาหรือไม่

• การใช้ผู้เชี่ยวชาญภายนอก (Outsource) ช่วยให้สามารถจัดตารางการฝึกอบรมที่สำคัญได้หรือไม่

หากหน่วยงานตัดสินใจว่า จ้างบุคคลภายนอกให้พัฒนาหลักสูตรการฝึกอบรม มีผู้ให้บริการหลายรายที่เสนอหลักสูตร “หลักสูตรเฉพาะ” ที่เหมาะสำหรับผู้ใช้งานเฉพาะกลุ่ม หรือสามารถพัฒนาหลักสูตรสำหรับผู้ใช้งานเฉพาะกลุ่มได้ ก่อนที่จะเลือกผู้ให้บริการรายใดรายหนึ่งนั้น หน่วยงานควรมีความเข้าใจอย่างถ่องแท้เกี่ยวกับความต้องการในการฝึกอบรมของผู้ใช้งาน และสามารถระบุได้ว่าหลักสูตรของผู้ให้บริการนั้นตรงตามความคาดหวังของผู้ใช้งานหรือไม่

ขั้นตอนที่ ๓ การดำเนินการแผนงานหรือโครงการ

ขั้นตอนนี้ระบุถึงการสื่อสารที่มีประสิทธิภาพและการเปิดตัวของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม นอกจากนี้ยังระบุทางเลือกสำหรับการเผยแพร่สื่อสารเอกสาร/สื่อ เนื้อหาในการสร้างความตระหนักรู้และการฝึกอบรม ตัวอย่างเช่น ทางเว็บไซต์ การเรียนรู้ทางไกล วิดีโอ การฝึกอบรมในสถานที่ตั้ง การดำเนินการแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์นั้น ต้องมีการดำเนินการดังต่อไปนี้ ก่อนนำไปใช้

• ดำเนินการประเมินความต้องการ

• มีการกำหนดกลยุทธ์เรียบร้อยแล้ว

• มีการกำหนดแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมสำหรับการดำเนินการตามกลยุทธ์เสร็จสมบูรณ์แล้ว

• พัฒนาเอกสาร/สื่อ เนื้อหาแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมแล้ว การดำเนินการแผนงานหรือโครงการ โดยมีขั้นตอนย่อย ดังนี้

๓.๑ การสื่อสารแผนงานหรือโครงการ

การดำเนินการของแผนงานหรือโครงการ ต้องทำการสื่อสารไปยังทุกส่วนของหน่วยงานเพื่อให้ได้รับการสนับสนุนสำหรับการดำเนินการ และการจัดการทรัพยากรที่จำเป็นต้องใช้งาน โดยต้องคำนึงถึงความคาดหวังของหน่วยงานในการจัดการ และการสนับสนุนของพนักงาน ซึ่งผลของความคาดหวังของแผนงานหรือโครงการจะมีประโยชน์ต่อหน่วยงาน โดยจะมีการกำหนดเงินทุนที่จะใช้ในแผนงานหรือโครงการ ตัวอย่างเช่น หัวหน้าหน่วยงานต้องรู้ว่าจะต้องใช้งบประมาณโดยรวมในการดำเนินการแผนงานหรือโครงการสร้างความตระหนักรู้จากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรืองบประมาณในแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ จำเป็นอย่างยิ่งที่ผู้เกี่ยวข้องในการดำเนินแผนงานหรือโครงการ ต้องเข้าใจบทบาทและความรับผิดชอบของตน นอกจากนี้ ต้องมีการสื่อสารกำหนดการและความคาดหวังเมื่อดำเนินการแล้วเสร็จ

การสื่อสารแผนควรจะมีการกำหนดให้สอดคล้องกับรูปแบบการดำเนินการตามที่อธิบายไว้ในขั้นตอนที่ ๑

๓.๒ การถ่ายทอดเอกสาร/สื่อ เนื้อหาของแผนงานหรือโครงการสร้างความตระหนักรู้

การถ่ายทอดเอกสาร/สื่อ เนื้อหาของแผนงานหรือโครงการสร้างความตระหนักรู้เป็นการสร้างการรับรู้ในเรื่องความมั่นคงปลอดภัยไซเบอร์ไปยังทั่วทั้งหน่วยงาน สามารถทำได้หลายวิธีการ

และขึ้นอยู่กับความพร้อมของทรัพยากรและความซับซ้อนของเนื้อหา ตัวอย่างเช่น โปสเตอร์ ภาพพักหน้าจอ แผ่นพับ จดหมายอิเล็กทรอนิกส์ รวมถึงเว็บไซต์ สื่อวิดีโอ การจัดอบรม ณ สถานที่ตั้ง หรือการจัดอบรมออนไลน์ การสัมมนาในหัวข้อที่สนใจ (Brown Bag Seminar)

ตัวอย่างของเทคนิคที่ใช้ในการถ่ายทอด มีหลายรูปแบบ ตัวอย่างเช่น

• เทคนิคที่ใช้เพื่อเผยแพร่หรือสื่อสารข้อความเดียว ได้แก่ โปสเตอร์ รายการเข้าถึง ภาพพักหน้าจอและป้ายเตือน ข้อความอีเมลของหน่วยงาน สัมมนาในหัวข้อที่สนใจ และแผนงานหรือโครงการให้รางวัล

• เทคนิคที่สามารถรวมข้อความจำนวนมากได้ง่ายขึ้น ได้แก่ รายการที่ควรทำและไม่ควรทำจดหมายข่าว วิดีโอ เว็บไซต์ การประชุมทางไกล การสอนด้วยตนเอง การสัมมนาในหัวข้อที่สนใจ

• เทคนิคที่ใช้งบประมาณต่ำในการนำไปปฏิบัติ ได้แก่ ข้อความบนโปสเตอร์ รายการเข้าถึง รายการที่ควรทำและไม่ควรทำ รายการตรวจสอบ ภาพพักหน้าจอและป้ายเตือน การสอนด้วยตนเอง การสัมมนาในหัวข้อที่สนใจ

• เทคนิคที่อาจต้องใช้ทรัพยากรมากขึ้น ได้แก่ จดหมายข่าว วิดีโอ เว็บไซต์ การประชุมทางไกล

ทั้งนี้ นอกเหนือจากการทำให้เอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้น่าสนใจและเป็นปัจจุบันแล้ว การทำซ้ำข้อความการสร้างความตระหนักรู้ และใช้วิธีต่าง ๆ ในการนำเสนอข้อความนั้น สามารถเพิ่มความจำในบทเรียนหรือประเด็นปัญหาของผู้ใช้งานในการสร้างความตระหนักรู้ได้อย่างมาก ตัวอย่างเช่น การอภิปรายโดยผู้สอนเกี่ยวกับการหลีกเลี่ยงการตกเป็นเหยื่อของการโจมตีแบบวิศวกรรมสังคม สามารถเสริมด้วยโปสเตอร์ ข้อความอีเมลเป็นระยะ

๓.๓ การถ่ายทอดเอกสาร/สื่อ เนื้อหาของแผนงานหรือโครงการฝึกอบรม

การถ่ายทอดเอกสาร/สื่อ เนื้อหาของแผนงานหรือโครงการฝึกอบรม กระบวนการที่เสริมสร้างความรู้ ทักษะ สมรรถนะและความสามารถของบุคคล หรือกลุ่มบุคคลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จำเป็นตามสายงานที่เกี่ยวข้อง เทคนิคในการถ่ายทอดเอกสาร/สื่อ เนื้อหาการฝึกอบรมอย่างมีประสิทธิภาพควรใช้ประโยชน์จากเทคโนโลยีที่สนับสนุนคุณลักษณะต่อไปนี้

• ใช้งานง่าย (Ease of Use) เช่น เข้าถึงง่าย ปรับปรุง/บำรุงรักษาง่าย

• การปรับขนาดได้ (Scalability) เช่น ใช้ได้กับจำนวนผู้ใช้งานที่หลากหลายและหลากหลายสถานที่

• รับผิดชอบ (Accountability) เช่น มีการบันทึกและใช้สถิติเกี่ยวกับระดับความสำเร็จ

• ฐานการสนับสนุนอุตสาหกรรมที่กว้างขวาง (Broad Base of Industry Support) เช่น จำนวนผู้ขายที่มีศักยภาพเพียงพอ โอกาสที่ดีกว่าในการติดตามผลและสนับสนุนเทคนิคทั่วไป

บางอย่างที่หน่วยงานสามารถนำไปใช้ได้ ได้แก่

• การฝึกอบรมผ่านวิดีโอเชิงโต้ตอบ (Interactive Video Training)

• การฝึกอบรมบนเว็บไซต์ (Web-based Training)

• การฝึกอบรมผ่านคอมพิวเตอร์ที่ไม่ใช่เว็บไซต์ (Non-web, Computer-based Training)

• การฝึกอบรมนอกสถานที่โดยผู้สอน (Outsite, Instructor-led Training) รวมถึงการนำเสนอโดยผู้เกี่ยวข้องและการให้คำปรึกษา

ทั้งนี้ การผสมผสานเทคนิคการถ่ายทอดการฝึกอบรมต่าง ๆ ในการดำเนินการเดียวเป็นวิธีที่มีประสิทธิภาพในการถ่ายทอดเอกสาร/สื่อ เนื้อหา และดึงความสนใจของผู้ใช้งาน

ขั้นตอนที่ ๔ หลังดำเนินการแผนงานหรือโครงการ

ขั้นตอนนี้จะเป็นการให้คำแนะนำในการทำให้แผนงานหรือโครงการเป็นปัจจุบันอยู่เสมอ และการตรวจสอบประสิทธิภาพของแผนงานหรือโครงการ มีการอธิบายวิธีการรับฟังผลสะท้อนกลับที่มีประสิทธิภาพ ตัวอย่างเช่น แบบสำรวจ การรับฟังความคิดเห็นกลุ่มเป้าหมาย การเปรียบเทียบ โดยพิจารณาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการเปลี่ยนแปลงของหน่วยงาน การเปลี่ยนแปลงภารกิจและลำดับความสำคัญของหน่วยงาน ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ จำเป็นต้องรับรู้ถึงปัญหาที่อาจเกิดขึ้นและนำกลไกต่าง ๆ รวมเข้ากับกลยุทธ์ เพื่อให้แน่ใจว่าแผนงานหรือโครงการยังคงมีความเกี่ยวข้องและสอดคล้องกับวัตถุประสงค์โดยรวมของหน่วยงาน

การปรับปรุงอย่างต่อเนื่องควรเป็นหัวข้อสำคัญในการเริ่มดำเนินการสำหรับการสร้างความตระหนักรู้และการฝึกอบรม ขั้นตอนหลังการดำเนินแผนงานหรือโครงการ มีขั้นตอนย่อย ดังนี้

๔.๑ การตรวจสอบการปฏิบัติตาม

เมื่อจัดแผนงานหรือโครงการเป็นที่เรียบร้อยแล้ว จะต้องวางกระบวนการเพื่อตรวจสอบการปฏิบัติตามและประสิทธิผลของแผนงานหรือโครงการ มีระบบติดตามอัตโนมัติที่ได้รับการออกแบบเพื่อเก็บข้อมูลสำคัญเกี่ยวกับกิจกรรมของแผนงานหรือโครงการ เช่น หลักสูตร วันที่ ผู้เข้าร่วม ค่าใช้จ่าย แหล่งที่มา โดยระบบติดตามนี้ควรเก็บข้อมูลระดับหน่วยงาน เพื่อให้สามารถใช้ในการวิเคราะห์ภาพรวมและรายงานเกี่ยวกับการสร้างความตระหนักรู้ การฝึกอบรม และการริเริ่มด้านการศึกษา ข้อกำหนดสำหรับฐานข้อมูล ควรรวบรวมความต้องการของผู้ใช้งานทั้งหมด โดยทั่วไปผู้ใช้งานฐานข้อมูลดังกล่าวจะรวมถึง

- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง สามารถใช้ฐานข้อมูลเพื่อสนับสนุนการวางแผนเชิงกลยุทธ์ แจ้งหัวหน้าหน่วยงานและเจ้าหน้าที่บริหารระดับสูงอื่น ๆ เกี่ยวกับสถานภาพของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ ระบุความสามารถภายในหน่วยงานและความต้องการที่สำคัญในด้านบุคลากรด้านความมั่นคงปลอดภัย ดำเนินการวิเคราะห์แผนงานหรือโครงการ ระบุกิจกรรมทั่วทั้งหน่วยงาน ช่วยเหลือในเรื่องงบประมาณด้านการรักษาความมั่นคงปลอดภัยและงบประมาณด้านเทคโนโลยีสารสนเทศ ระบุความจำเป็นในการปรับปรุงแผนงานหรือโครงการ และประเมินการปฏิบัติตามหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Program Manager) สามารถใช้ฐานข้อมูลเพื่อสนับสนุนการวางแผนการรักษาความมั่นคงปลอดภัย รายงานสถานะต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูงฝ่ายบริหาร และเจ้าหน้าที่รักษาความมั่นปลอดภัย ระบุคำของบประมาณ แสดงให้เห็นถึงการปฏิบัติตามเป้าหมายและวัตถุประสงค์ที่หน่วยงานกำหนดขึ้น ระบุผู้ให้การฝึกอบรมและแหล่งข้อมูลการฝึกอบรมอื่น ๆ ตอบสนองต่อข้อซักถามที่เกี่ยวข้องกับความมั่นคงปลอดภัย ระบุความครอบคลุมของแผนงานในปัจจุบัน และทำการปรับเปลี่ยนเมื่อมีเหตุจำเป็นต้องดำเนินการ และละเว้นการดำเนินการ
- แผนกทรัพยากรบุคคล (Human Resource Department) สามารถใช้ฐานข้อมูลเพื่อให้แน่ใจว่ามีกลไกที่มีประสิทธิภาพสำหรับการรวบรวมข้อมูลการฝึกอบรมที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทั้งหมด ระบุค่าใช้จ่ายที่เกี่ยวข้องกับการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ ช่วยเหลือในการจัดทำคำอธิบายตำแหน่ง สนับสนุนการรายงานสถานะ ตอบคำถามเกี่ยวกับการฝึกอบรม และช่วยเหลือในพัฒนาด้านวิชาชีพ
- แผนกฝึกอบรมหน่วยงาน (Agency Training Department) สามารถใช้ฐานข้อมูล เพื่อช่วยในการพัฒนากลยุทธ์การฝึกอบรมหน่วยงานโดยรวม สร้างข้อกำหนดฐานข้อมูลการฝึกอบรมที่เชื่อมโยงโดยตรงกับด้านความมั่นคงปลอดภัย ระบุแหล่งการฝึกอบรมที่เป็นไปได้ สนับสนุนคำขอฝึกอบรม ระบุความเกี่ยวข้องและความนิยมของหลักสูตร สนับสนุนกิจกรรมการจัดทำงบประมาณและตอบข้อซักถาม

• หัวหน้างาน (Functional Manager) สามารถใช้ฐานข้อมูลเพื่อตรวจสอบความคืบหน้าในการฝึกอบรมของผู้ใช้งานและปรับแผนการฝึกอบรมตามความจำเป็น รับรายงานสถานะและตอบข้อซักถามเกี่ยวกับส่วนเสริมในการฝึกอบรมด้านความมั่นคงปลอดภัย และระบุแหล่งฝึกอบรมและค่าใช้จ่ายเพื่อช่วยเหลือเกี่ยวกับข้อเสนอและคำของบประมาณ

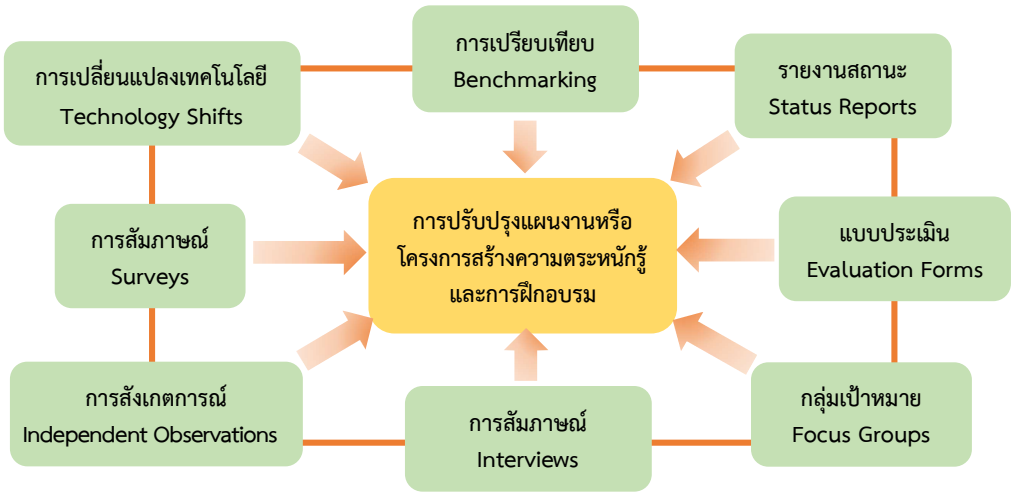
• ผู้ตรวจสอบ (Auditor) สามารถใช้ข้อมูลจากฐานข้อมูลเพื่อตรวจสอบการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยและนโยบายของหน่วยงาน

• หัวหน้าฝ่ายการเงิน (CFO) สามารถใช้ข้อมูลจากฐานข้อมูลเพื่อตอบข้อซักถามเกี่ยวกับงบประมาณ ช่วยในการวางแผนทางการเงิน และจัดทำรายงานต่อหัวหน้าหน่วยงานและหัวหน้าอาวุโสเกี่ยวกับเงินทุนสำหรับกิจกรรมการฝึกอบรมด้านความมั่นคงปลอดภัย

ทั้งนี้ การติดตามการปฏิบัติตามเกี่ยวข้องกับการประเมินสถานะของแผนงานหรือโครงการตามที่ระบุโดยข้อมูลในฐานข้อมูล และทำการเทียบกับมาตรฐานที่กำหนดโดยหน่วยงาน สามารถสร้างรายงานและนำไปใช้เพื่อระบุความแตกต่างหรือปัญหา ซึ่งจะถูกนำมาใช้ในการดำเนินการแก้ไขและติดตามผลที่จำเป็น อาจอยู่ในรูปแบบของการแจ้งเตือนอย่างเป็นทางการถึงฝ่ายบริหาร รวมไปถึงการสร้างความตระหนักรู้ การฝึกอบรมหรือข้อเสนอด้านการศึกษา หรือการจัดทำแผนการแก้ไขที่มีการกำหนดวันแล้วเสร็จ

๔.๒ การประเมินผลและข้อเสนอแนะ

เมื่อจัดแผนงานหรือโครงการเป็นที่เรียบร้อยแล้ว จะต้องทำการประเมินการรับรู้และความเข้าใจที่ได้รับจากการจัดแผนงานหรือโครงการ โดยการกำหนดรูปแบบการประเมินผลให้สอดคล้องกับระดับของแผนงานหรือโครงการ การประเมินผลอย่างเป็นทางการและกลไกของข้อเสนอแนะเป็นองค์ประกอบที่สำคัญของแผนงานหรือโครงการสร้างความตระหนักรู้ การฝึกอบรม และการศึกษาด้านความมั่นคงปลอดภัยการปรับปรุงอย่างต่อเนื่องไม่สามารถเกิดขึ้นได้หากปราศจากความเข้าใจว่าแผนงานหรือโครงการที่มีอยู่ทำงานอย่างไร นอกจากนี้ กลไกของข้อเสนอแนะ ต้องได้รับการออกแบบเพื่อระบุวัตถุประสงค์เบื้องต้นในการจัดตั้งแผนงานหรือโครงการ เมื่อข้อกำหนดพื้นฐานมีความมั่นคงแล้ว กลยุทธ์ของข้อเสนอแนะสามารถออกแบบและถูกนำไปใช้ การประเมินผลและกลไกของข้อเสนอแนะที่หลากหลาย สามารถใช้เพื่อปรับปรุงแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมได้ รายละเอียดดังภาพเทคนิคการประเมินและข้อเสนอแนะ ด้านล่าง



ภาพเทคนิคการประเมินและข้อเสนอแนะ

กลยุทธ์ของข้อเสนอแนะจำเป็นต้องรวมองค์ประกอบที่กล่าวถึงคุณภาพ ขอบเขต ระดับความยากง่ายในการใช้งาน ระยะเวลาดำเนินการ ความเกี่ยวข้อง วิธีการปรับใช้ เช่น บนเว็บไซต์ในสถานที่ตั้ง และคำแนะนำสำหรับการปรับเปลี่ยน

การขอความคิดเห็นหรือข้อเสนอแนะ สามารถทำได้หลายวิธี ที่พบมากที่สุด ได้แก่

• แบบประเมิน/แบบสอบถาม (Evaluation Form/Questionnaire) สามารถใช้งานได้หลากหลายรูปแบบ การออกแบบประเมินที่ดีโดยการช่วยลดความจำเป็นในการเขียนจำนวนมาก ในส่วนที่ผู้ทำการประเมินต้องกรอก ปัจจัยสำคัญคือการออกแบบแบบฟอร์มให้ “เป็นมิตรกับผู้ใช้” มากที่สุด การออกแบบเครื่องมือในการประเมินควรทำงานร่วมกับผู้เชี่ยวชาญภายในหน่วยงานที่คุ้นเคยกับเทคนิคการประเมิน หรือขอความช่วยเหลือจากผู้เชี่ยวชาญภายนอก

• กลุ่มเป้าหมาย (Focus Groups) นำหัวข้อของการฝึกอบรมมาหารือในที่ประชุมแบบเปิด เพื่อรับฟังมุมมองของกลุ่มเป้าหมายเกี่ยวกับประสิทธิผลของแผนงานหรือโครงการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ และขอแนวคิดของกลุ่มเป้าหมายสำหรับการปรับปรุง

• การสัมภาษณ์แบบเจาะจง (Selective Interviews) แนวทางนี้จะระบุกลุ่มเป้าหมายการฝึกอบรมตามผลกระทบ ลำดับความสำคัญ หรือเกณฑ์ที่กำหนดขึ้นอื่น ๆ ก่อน และระบุประเด็นเฉพาะสำหรับข้อเสนอแนะ โดยปกติแล้วจะใช้การสัมภาษณ์แบบตัวต่อตัวหรือกลุ่มเล็ก ๆ (ไม่เกินสิบคน) แนวทางนี้ให้ความสนใจเฉพาะบุคคลและเป็นส่วนตัวมากกว่าแนวทางตามกลุ่มเป้าหมาย และอาจกระตุ้นให้ผู้เข้าร่วมมีความพร้อมมากขึ้นในการวิจารณ์แผนงาน/แผนงานหรือโครงการ

• การสังเกตการณ์/การวิเคราะห์โดยอิสระ (Independent Observation/Analysis) อีกแนวทางหนึ่งสำหรับการขอความคิดเห็น คือ การเข้าร่วมการตรวจสอบแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ เป็นงานสำหรับผู้ให้บริการฝึกอบรมภายนอกหรือบุคคลที่สามอื่น ๆ ซึ่งเป็นหน่วยงานตรวจสอบ หน่วยงานจะทำเช่นนี้นอกเหนือจากกิจกรรมการกำกับดูแลตามปกติ เพื่อรับความคิดเห็นที่เป็นกลางเกี่ยวกับประสิทธิผลของแผนงานหรือโครงการ

• รายงานสถานะอย่างเป็นทางการ (Formal Status Report) เป็นวิธีที่ดีในการให้ความสำคัญกับข้อกำหนดการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยทั่วทั้งหน่วยงาน ที่นำมาใช้เป็นข้อกำหนดสำหรับการรายงานสถานะปกติโดยหัวหน้างาน

• การเปรียบเทียบแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ (มุมมองภายนอก) หลายหน่วยงานนำเอาแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ เป็นส่วนหนึ่งของการเทียบมาตรฐานของกลยุทธ์ในการปรับปรุงอย่างต่อเนื่องและมุ่งมั่นสู่ความเป็นเลิศ รูปแบบการเทียบมาตรฐานความมั่นคงปลอดภัยที่มุ่งเน้นภายนอก จะเปรียบเทียบประสิทธิภาพของหน่วยงานกับองค์กรอื่น ๆ จำนวนหนึ่ง และจัดทำรายงานกลับไปยังหน่วยงานว่าหน่วยงานอยู่ในตำแหน่งใด โดยอ้างอิงจากการสังเกตพื้นฐานที่ได้จากทุกหน่วยงานที่มีข้อมูลอยู่ในปัจจุบัน องค์ประกอบของการเปรียบเทียบประเภทนี้ ควรรวมถึงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัย การเปรียบเทียบประเภทนี้ โดยปกติจะทำโดยผู้เชี่ยวชาญในเทคนิคการเปรียบเทียบซึ่งมีข้อมูลมากมายจากหลากหลายหน่วยงานในระยะเวลาค่อนข้างนาน (ห้าปีขึ้นไป)

๔.๓ การจัดการปรับปรุงเปลี่ยนแปลงเอกสาร/สื่อ เนื้อหา

ทำการปรับปรุงเนื้อหาของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม เพื่อให้รองรับกับเทคโนโลยีใหม่ที่นำมาใช้ และให้สอดคล้องกับข้อกำหนด ระเบียบ มาตรฐาน หรือกฎหมาย ที่อาจมีการเปลี่ยนแปลงในช่วงเวลาที่ผ่านมา

มีความจำเป็นอย่างยิ่งเพื่อให้แน่ใจได้ว่าแผนงานหรือโครงการที่เป็นไปตามโครงสร้าง จะได้รับการปรับปรุงอย่างต่อเนื่อง เมื่อมีเทคโนโลยีใหม่และประเด็นด้านความมั่นคงปลอดภัยที่เกี่ยวข้องเกิดขึ้น ความต้องการในการฝึกอบรมจะเปลี่ยนไป เมื่อมีทักษะและความสามารถใหม่ ๆ ที่จำเป็นต่อการตอบสนองการเปลี่ยนแปลงทางสถาปัตยกรรมและเทคโนโลยี การเปลี่ยนแปลงภารกิจหรือวัตถุประสงค์ของหน่วยงาน มีอิทธิพลต่อแนวคิดเกี่ยวกับการออกแบบสถานที่ฝึกอบรมและเนื้อหา

ประเด็นปัญหาที่เกิดขึ้นใหม่ เช่น การป้องกันมาตุภูมิ จะส่งผลกระทบต่อลักษณะและขอบเขตของกิจกรรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยที่จำเป็น เพื่อให้ผู้รับการอบรมทราบ/ให้ความรู้เกี่ยวกับการหาประโยชน์และมาตรการตอบโต้ล่าสุด กฎหมายใหม่และคำตัดสินของศาลอาจส่งผลกระทบต่อนโยบายของหน่วยงาน ซึ่งอาจส่งผลต่อการพัฒนาหรือการใช้เอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้และการฝึกอบรม เมื่อแนวทางด้านความมั่นคงปลอดภัยเปลี่ยนแปลงหรือได้รับการปรับปรุง เอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้และการฝึกอบรมควรสะท้อนถึงการเปลี่ยนแปลงเหล่านี้ด้วย

๔.๔ การปรับปรุงอย่างต่อเนื่อง (“การยกระดับขอบเขตการพัฒนาทักษะ”)

ขั้นตอนนี้มุ่งเน้นไปที่การสร้างระดับการรับรู้ด้านความมั่นคงปลอดภัยและความเป็นเลิศที่บรรลุการรักษาความมั่นคงปลอดภัยในหลายหน่วยงาน กระบวนการที่สร้างความตระหนักรู้ การฝึกอบรม และการศึกษาแก่พนักงาน ควรรวมทั้งหมดเข้ากับกลยุทธ์ทางธุรกิจ แผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ ที่ครบกำหนดจะมีการกำหนดระดับตัวชี้วัดพื้นฐานควรมีการนำระบบอัตโนมัติมาใช้เพื่อรองรับการบันทึกข้อมูลเชิงปริมาณและการจัดส่งข้อมูลการดำเนินการไปยังฝ่ายที่รับผิดชอบเป็นประจำตามรอบที่กำหนด มีการกำหนดรอบการติดตามผลและขั้นตอนการแก้ไขมีการกำหนดอย่างชัดเจนและเรียบง่าย

ในขั้นตอนนี้ หน่วยงานต่าง ๆ ได้รวมกลไกของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมเข้ากับการวิจัยด้านความก้าวหน้าทางเทคโนโลยี แนวปฏิบัติที่ดี และโอกาสในการเปรียบเทียบ

๔.๕ สรุปความสำเร็จของแผนงานหรือโครงการจากตัวบ่งชี้

ทำการสรุปผลความสำเร็จของแผนงานหรือโครงการตามตัวบ่งชี้ที่กำหนดขึ้นมาเพื่อให้ทั่วทั้งหน่วยงานรับทราบระดับความสำเร็จของแผนงานหรือโครงการ เนื้อหาควรมีเรื่องเหล่านี้ งบประมาณและทรัพยากร บทบาทและหน้าที่ของคนในหน่วยงาน ข้อความของผู้บริหารที่ต้องการสื่อสาร ความครอบคลุมของการสร้างความตระหนักรู้และการฝึกอบรม และการสรุปข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ ควรจัดทำรายงานสรุปในเอกสาร/สื่อ เนื้อหาที่สามารถเผยแพร่ได้สะดวกทั้งหน่วยงาน

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เจ้าหน้าที่แผนงานหรือโครงการและหัวหน้าแผนงานหรือโครงการ ควรเป็นผู้สนับสนุนหลักสำหรับการปรับปรุงอย่างต่อเนื่องและสนับสนุนการสร้างความตระหนักรู้ การฝึกอบรม และการศึกษาของหน่วยงาน จำเป็นอย่างยิ่งที่ทุกคนจะต้องมีความสามารถและเต็มใจที่จะปฏิบัติตามข้อกำหนดบทบาทด้านความมั่นคงปลอดภัย (Security Role) ที่ได้รับมอบหมายในหน่วยงาน การรักษาความมั่นคงปลอดภัยข้อมูลและโครงสร้างพื้นฐานของหน่วยงานเป็นความพยายามและหน้าที่ของทีม

รายการด้านล่างเป็นตัวบ่งชี้บางประการเพื่อวัดการสนับสนุนและการยอมรับของแผนงานหรือโครงการ

• งบประมาณเพียงพอที่จะดำเนินการกลยุทธ์ตามที่ได้ตกลงไว้

• การจัดตำแหน่งหน่วยงานที่เหมาะสมเพื่อให้ผู้ที่มีหน้าที่รับผิดชอบหลัก (ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เจ้าหน้าที่แผนงานหรือโครงการ และหัวหน้าแผนงานหรือโครงการ) สามารถดำเนินการกลยุทธ์ได้อย่างมีประสิทธิภาพ

• รองรับการเผยแพร่ในวงกว้าง เช่น เว็บไซต์ อีเมล โทรทัศน์ และการประกาศรายการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

• ข้อความจากผู้บริหาร/ระดับอาวุโสถึงพนักงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น การประชุมพนักงาน การถ่ายทอดจากหัวหน้าหน่วยงานไปยังผู้ใช้ทุกคนตามหน่วยงาน

• การใช้การวัดผล (Metric) เช่น การระบุการลดลงของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์หรือการละเมิด การระบุข้อแตกต่างระหว่างการสร้างความตระหนักรู้ที่มีอยู่และความครอบคลุมของการฝึกอบรมและการระบุความต้องการที่กำลังลดลง ร้อยละ (เปอร์เซ็นต์) ของผู้รับการอบรมที่ได้รับเอกสาร/สื่อเนื้อหาการสร้างความตระหนักรู้ที่เพิ่มขึ้น ร้อยละ (เปอร์เซ็นต์) ของผู้รับการฝึกอบรมที่รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญซึ่งได้รับการฝึกอบรมอย่างเหมาะสมเพิ่มขึ้น

• ผู้จัดการหรือหัวหน้าไม่ได้ปฏิบัติตามสถานะของตนในหน่วยงานเพื่อหลีกเลี่ยงการควบคุมความมั่นคงปลอดภัยไซเบอร์

• ระดับของผู้เข้าร่วมที่จำเป็นในการประชุม/การบรรยายสรุปด้านความมั่นคงปลอดภัยไซเบอร์

• การยอมรับผลงานด้านความมั่นคงปลอดภัยไซเบอร์ เช่น การให้รางวัลการแข่งขัน

• แรงจูงใจที่แสดงให้เห็นโดยผู้ที่มีบทบาทสำคัญในการจัดการ/ประสานงานแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์

๔.๖ การพัฒนาสู่ความเป็นผู้เชี่ยวชาญ (Professional Development)

การพัฒนาสู่ความเชี่ยวชาญ เป็นความตั้งใจที่จะทำให้แน่ใจว่าพนักงานหรือบุคลากรของหน่วยงานจากพนักงานทั่วไปจนถึงระดับเชี่ยวชาญ มีความรู้ความสามารถเหมาะสมกับบทบาทและหน้าที่ของตน การพัฒนาสู่ความเป็นผู้เชี่ยวชาญ จะวัดจากทักษะผ่านทางใบรับรอง (Certification) ดังนั้น การพัฒนาตนเองและได้รับใบรับรอง จะสามารถยืนยันได้ว่าเป็นผู้เชี่ยวชาญ การเตรียมเพื่อขอทดสอบใบรับรองดังกล่าว โดยปกติจะรวมถึงการเรียนตามหลักสูตรที่กำหนดหรือเนื้อหาทางเทคนิค อาจรวมถึงการฝึกประสบการณ์จากการทำงานจริง การพัฒนาสู่ความเป็นผู้เชี่ยวชาญไม่ได้ระบุแค่สายงานด้านเทคโนโลยีสารสนเทศหรือความมั่นคงปลอดภัยไซเบอร์เท่านั้น แต่อาจรวมถึง พนักงานด้านความมั่นคงปลอดภัยไซเบอร์ ผู้ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ผู้ดูแลระบบ หรืออื่น ๆ ที่เกี่ยวข้อง

ใบรับรอง สามารถแบ่งออกได้เป็น ๒ ประเภท คือ ๑) ใบรับรองประเภททั่วไป และ ๒) ใบรับรองทางเทคนิค โดยใบรับรองประเภททั่วไปจะมุ่งเน้นไปที่การสร้างพื้นฐานความรู้ในหลาย ๆ ด้านเกี่ยวกับวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ ส่วนใบรับรองทางเทคนิคนั้น เป็นประเด็นเกี่ยวกับหลักการด้านความมั่นคงปลอดภัยทางเทคนิคที่เกี่ยวข้องกับแพลตฟอร์มเฉพาะ ระบบปฏิบัติการ ผลิตภัณฑ์ของผู้จัดจำหน่าย และอื่น ๆ

บางหน่วยงาน จะมุ่งเน้นความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ด้วยใบรับรอง โดยใช้เป็นส่วนหนึ่งในการรับสมัครบุคคลเข้าทำงาน บางหน่วยงานเสนอการขึ้นเงินเดือน ค่าประสบการณ์ และโบนัสเพิ่มเติมสำหรับพนักงานที่มีใบรับรอง และสนับสนุนให้พนักงานในสายงานด้านความมั่นคงปลอดภัยไซเบอร์ขอใบรับรอง

๔.๗ การศึกษาและประสบการณ์ (Education and Experience)

ระดับของการศึกษาของการเรียนรู้อย่างต่อเนื่องทางด้านความมั่นคงปลอดภัยไซเบอร์ จะบอกถึงการเพิ่มเติมความรู้ใหม่ สองกรณี คือ

(๑) ทักษะความรู้ในปัจจุบัน

(๒) ทักษะความรู้ด้านเทคโนโลยีสารสนเทศหรือความมั่นคงปลอดภัยไซเบอร์

ระดับผู้เชี่ยวชาญที่คาดหวังที่จะสร้างหรือพัฒนาให้เกิดเป็นองค์ความรู้หรือทักษะนั้น เมื่อเข้ามาทำงานด้านเทคโนโลยีสารสนเทศหรือความมั่นคงปลอดภัยไซเบอร์ จะมีความรู้พื้นฐานทั่วไปที่จำเป็นต่อลักษณะงานที่ตนทำ ประเด็นการศึกษาจะไม่ได้พูดถึงประเด็นการเรียนรู้อย่างต่อเนื่องเพียงอย่างเดียว แต่จะหมายถึงการเพิ่มความสามารถด้านเทคโนโลยีสารสนเทศหรือความมั่นคงปลอดภัยไซเบอร์ โดยมุ่งเน้นการศึกษาที่จะเพิ่มเติมการเรียนรู้หรือประสบการณ์ การศึกษาในทางอุตสาหกรรมรวมถึงการได้มาซึ่งใบรับรองของโครงการหรือหลักสูตรที่สนับสนุนโดยสถาบันการศึกษาระดับสูงการผ่านกระบวนการศึกษา ในสาขาที่มีความต้องการ ซึ่งการศึกษาเพื่อพัฒนาความเชี่ยวชาญนั้น รวมถึงการฝึกอบรม การศึกษาและประสบการณ์ที่สร้างขึ้นจากกระบวนการวัดผลความรู้และทักษะ โดยผ่านใบรับรองผลลัพธ์ที่กำหนดขึ้นในแต่ละระดับ ทั้งนี้ ตัวอย่างของการศึกษาที่จะนำไปสู่การเป็นผู้เชี่ยวชาญ คือ การศึกษาระดับปริญญา หรือการสอบใบรับรอง

ผนวก ก
ตัวอย่างทักษะและความรู้ของบุคลากร

ตำแหน่ง : ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง **(CHIEF INFORMATION OFFICER: CIO)**	
คำอธิบาย บทบาท	ผู้ที่ทำหน้าที่จัดการโครงสร้างพื้นฐาน งบประมาณ การวางแผน การรายงานการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ และดูแลบุคลากรซึ่งมีความสำคัญต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ทำงานร่วมกับหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ และหัวหน้าส่วนงาน
ด้านความรู้	๑. มีความรู้เกี่ยวกับการดำเนินธุรกิจของหน่วยงาน ๒. มีความรู้เกี่ยวกับนโยบาย ขั้นตอน และมาตรฐานความมั่นคงปลอดภัยไซเบอร์ รวมถึงเข้าใจบทบาทในการจัดการการเปลี่ยนแปลงด้านความมั่นคงปลอดภัยไซเบอร์ ๓. มีความรู้เกี่ยวกับการพัฒนาและบำรุงรักษาโครงสร้างพื้นฐานสารสนเทศเพื่อสนับสนุนและปรับปรุงผลิตภัณฑ์ บริการ และการดำเนินการ รวมถึงการวางแผน การรายงาน และการดำเนินกิจกรรมต่าง ๆ ๔. มีความรู้เกี่ยวกับการวางแผนเชิงกลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงการจัดสรรงบประมาณและการวางแผนทรัพยากรบุคคล ระบบสารสนเทศ และการเพิ่มประสิทธิภาพกระบวนการ ๕. มีความรู้เกี่ยวกับแนวคิดการประเมินและปรับปรุงกระบวนการในการสร้างความตระหนักรู้และการพัฒนาทักษะ ความรู้ความสามารถของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ๖. มีความรู้เกี่ยวกับการสื่อสารและการเจรจาต่อรอง ภาวะผู้นำและการนำทีม
ด้านทักษะ	๑. สามารถจัดทำแผนและกำหนดกลยุทธ์โดยรวมสำหรับแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ ๒. สามารถประชาสัมพันธ์นโยบาย แนวคิดและกลยุทธ์ของแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ของหัวหน้าหน่วยงาน เจ้าของระบบ เจ้าของข้อมูล และบุคลากรอื่นของหน่วยงาน รวมถึงประเมินความเข้าใจนโยบาย แนวคิด และกลยุทธ์ดังกล่าว เพื่อปรับปรุงแนวทางประชาสัมพันธ์ ๓. รับทราบและประเมินความก้าวหน้าของการดำเนินแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ และเสนอรายงานความก้าวหน้าของแผนงานหรือโครงการต่อหัวหน้าหน่วยงาน ๔. สามารถกำหนดแหล่งเงินทุนและดำเนินการให้มีการสนับสนุนงบประมาณสำหรับแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานอย่างเพียงพอ ๕. สามารถตรวจสอบ ประเมินและจัดให้มีการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์อย่างเพียงพอต่อการปฏิบัติงานที่อยู่ในความรับผิดชอบของผู้ใช้แต่ละคน ๖. ดำเนินการให้มีกลไกการติดตาม การพัฒนาและการดำเนินการตามนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ และกลไกการรายงานผลที่มีประสิทธิภาพ ๗. มีความเป็นผู้นำและสามารถกระตุ้นทีม และสามารถไกล่เกลี่ยความขัดแย้ง ๘. สามารถติดตามความก้าวหน้าทางเทคโนโลยีและนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์

ตำแหน่ง : ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (CHIEF INFORMATION SECURITY OFFICER: CISO)	
คำอธิบาย บทบาท	ผู้ที่เข้าใจในระบบธุรกิจขององค์กรและการจัดการกับความเสี่ยงที่มีโอกาสเกิดขึ้น ทำหน้าที่จัดการเกี่ยวกับผลกระทบของความมั่นคงปลอดภัยไซเบอร์ต่อองค์กร แผนงาน หรือโครงการเฉพาะ หรือขอบเขตความรับผิดชอบอื่น รวมถึงการกำหนดเป้าหมายกลยุทธ์ นโยบายด้านการรักษาความมั่นคงปลอดภัยที่สอดคล้องกับแผนยุทธศาสตร์ขององค์กร พัฒนานโยบายด้านการรักษาความปลอดภัยของข้อมูล มาตรฐาน ขั้นตอนและแนวปฏิบัติ การบริหารทรัพยากรบุคคล โครงสร้างพื้นฐาน การบังคับใช้นโยบาย การวางแผนรองรับสถานการณ์ฉุกเฉิน การสร้างความตระหนักรู้ และทรัพยากรอื่น
ด้านความรู้	๑. มีความรู้และประสบการณ์เกี่ยวกับการจัดการธุรกิจ การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ การกำหนดกลยุทธ์ การประกันสารสนเทศ ๒. มีความรู้เกี่ยวกับระบบปฏิบัติการ การออกแบบโครงสร้างพื้นฐานสารสนเทศ การจัดการระบบสารสนเทศและเครือข่าย การกำหนดสิทธิ์การเข้าถึง ข้อกำหนดของระบบเฉพาะที่อาจเป็นโครงสร้างสร้างพื้นฐานสารสนเทศสำคัญที่อาจไม่ใช้เทคโนโลยีสารสนเทศมาตรฐาน ๓. มีความรู้เกี่ยวกับการจัดการระบบ มาตรฐานซอฟต์แวร์ นโยบายและการได้รับอนุญาตเกี่ยวกับการออกแบบระบบ การจัดการวงรอบของระบบ (การใช้งานและความมั่นคงปลอดภัยไซเบอร์) ข้อกำหนดของระบบเฉพาะที่อาจเป็นโครงสร้างระบบ ๔. มีความรู้เกี่ยวกับหลักการและเครื่องมือในการสำรองข้อมูล ชนิดของการสำรองข้อมูล การกู้คืน และความต่อเนื่องของการดำเนินการ ๕. มีความรู้เกี่ยวกับภัยคุกคาม ช่องโหว่ การโจมตีระบบและแอปพลิเคชัน ขั้นตอนการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ การทดสอบระบบ ๖. มีความรู้เกี่ยวกับกฎหมาย ข้อบังคับ การกำกับดูแล นโยบาย ขั้นตอน มาตรฐาน และจริยธรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ๗. มีความรู้เกี่ยวกับมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ ตัวอย่างเช่น NIST, ISO, SANS, COBIT, CERT ๘. มีความรู้เกี่ยวกับข้อมูล มาตรฐานความมั่นคงปลอดภัยข้อมูล การจำแนกประเภทข้อมูล และขั้นตอนการบุกรุกสารสนเทศ

ตำแหน่ง : ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (CHIEF INFORMATION SECURITY OFFICER: CISO)	
ด้านทักษะ	๑. สามารถกำหนดกลวิธีและสร้างข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ ๒. สามารถขับเคลื่อนการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ที่พัฒนาขึ้นนั้นเหมาะสมและเป็นปัจจุบันต่อกลุ่มเป้าหมาย หรือสามารถปรับเปลี่ยนตามเงื่อนไขกระบวนการ หรือสภาพแวดล้อมที่ส่งผลกระทบต่อผลลัพธ์ ๓. สามารถกำกับและติดตามการเข้าถึงและการใช้งานระบบสารสนเทศเพื่อการสร้างความตระหนักรู้ และการฝึกอบรม ของกลุ่มเป้าหมายอย่างมีประสิทธิภาพ ๔. สามารถกำหนดวิธีการสำหรับการรับข้อเสนอแนะเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และวิธีการนำเสนอจากผู้ใช้งานและหัวหน้าส่วนงาน ๕. สามารถกำหนดมาตรการ หรือตัวชี้วัดประสิทธิภาพของระบบและความพร้อมใช้งานที่ส่งผลต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ๖. สามารถขับเคลื่อนการดำเนินการทบทวนแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์เป็นระยะ ๆ เพื่อปรับปรุง เมื่อมีความจำเป็นหรือมีการเปลี่ยนแปลงความเสี่ยงสูงขึ้น ๗. สามารถสนับสนุนการดำเนินการของผู้บริหารเทคโนโลยีสารสนเทศระดับสูงในการสร้างกลยุทธ์การติดตามและการรายงานผลการดำเนินการ ๘. สามารถไกล่เกลี่ยลดความขัดแย้งในการดำเนินการและกิจกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ๙. สามารถประเมิน หรือรับรองความน่าเชื่อถือของบุคคลหรือองค์กรที่ทำหน้าที่จัดหาผลิตภัณฑ์หรือบริการ

ตำแหน่ง : ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (HEAD OF INFORMATION SECURITY)	
คำอธิบาย บทบาท	ผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือกับภัยคุกคามทางไซเบอร์ สามารถสื่อสาร ประสานงาน บูรณาการ และรับผิดชอบต่อความสำเร็จโดยรวมของแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ และตรวจสอบว่าแผนงานหรือโครงงานได้สอดคล้องต่อลำดับความสำคัญของหน่วยงาน
ด้านความรู้	๑. มีความรู้เกี่ยวกับกระบวนการทางธุรกิจ การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ การกำหนดกลยุทธ์การประกันสารสนเทศ ๒. มีความรู้เกี่ยวกับระบบปฏิบัติการ การออกแบบโครงสร้างพื้นฐานสารสนเทศ การจัดการระบบสารสนเทศและเครือข่าย การกำหนดสิทธิ์การเข้าถึง ข้อกำหนดของระบบเฉพาะที่อาจเป็นโครงสร้างสร้างพื้นฐานสารสนเทศสำคัญที่อาจไม่ใช้เทคโนโลยีสารสนเทศมาตรฐาน ๓. มีความรู้เกี่ยวกับการจัดการระบบ มาตรฐานซอฟต์แวร์ นโยบายและการได้รับอนุญาตเกี่ยวกับการออกแบบระบบ การจัดการวงจรชีวิตของระบบ (การใช้งานและความมั่นคงปลอดภัยไซเบอร์) ผลกระทบต่อการดำเนินการเมื่อความมั่นปลอดภัยไซเบอร์ถูกระงับข้อกำหนดของระบบเฉพาะที่อาจเป็นโครงสร้างพื้นฐาน ๔. มีความรู้เกี่ยวกับหลักการและเครื่องมือในการสำรองข้อมูล ชนิดของการสำรองข้อมูล การกู้คืน และความต่อเนื่องของการดำเนินการ ๕. มีความรู้เกี่ยวกับภัยคุกคาม ช่องโหว่ การโจมตีระบบและแอปพลิเคชัน ขั้นตอนการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ การทดสอบระบบ ๖. มีความรู้เกี่ยวกับกฎหมาย ข้อบังคับ การกำกับดูแล นโยบาย ขั้นตอน มาตรฐานและจริยธรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ๗. มีความรู้เกี่ยวกับมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ ตัวอย่างเช่น NIST, ISO, SANS, COBIT, CERT ๘. มีความรู้เกี่ยวกับข้อมูล ข้อมูลส่วนบุคคล มาตรฐานความมั่นคงปลอดภัยข้อมูล การจำแนกประเภทข้อมูล และขั้นตอนการบุกรุกสารสนเทศ
ด้านทักษะ	๑. สามารถกำหนดกลวิธีและสร้างข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ที่สะท้อนต่อวัตถุประสงค์ ๒. สามารถขับเคลื่อนการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ที่พัฒนาขึ้นนั้นให้เหมาะสมและเป็นปัจจุบันต่อกลุ่มเป้าหมาย หรือสามารถปรับเปลี่ยนตามเงื่อนไขกระบวนการ หรือสภาพแวดล้อมที่ส่งผลกระทบต่อผลลัพธ์ ๓. สามารถกำกับและติดตามการเข้าถึงและการใช้งานระบบสารสนเทศเพื่อการสร้างความตระหนักรู้และการฝึกอบรมของกลุ่มเป้าหมายอย่างมีประสิทธิภาพ ๔. สามารถกำหนดวิธีการสำหรับการรับข้อเสนอแนะเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และวิธีการนำเสนอจากผู้ใช้งานและหัวหน้าส่วนงาน

ตำแหน่ง : ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (HEAD OF INFORMATION SECURITY)	
ด้านทักษะ	๕. สามารถกำหนดมาตรการ หรือตัวชี้วัดประสิทธิภาพของระบบและความพร้อมใช้งาน ที่ส่งผลต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ๖. สามารถขับเคลื่อนการดำเนินการทบทวนแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์เป็นระยะ ๆ เพื่อปรับปรุง เมื่อมีความจำเป็นหรือมีการเปลี่ยนแปลงความเสี่ยงสูงขึ้น ๗. สามารถสนับสนุนการดำเนินการของผู้บริหารเทคโนโลยีสารสนเทศระดับสูงในการสร้างกลยุทธ์การติดตามและการรายงานผลการดำเนินการ ๘. สามารถไกล่เกลี่ยลดความขัดแย้งในการดำเนินการและกิจกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ๙. สามารถประเมิน หรือรับรองความน่าเชื่อถือของบุคคลหรือองค์กรที่ทำหน้าที่จัดหาผลิตภัณฑ์หรือบริการ

ตำแหน่ง : หัวหน้าส่วนงาน (MANAGER)	
คำอธิบาย บทบาท	ทำหน้าที่รับผิดชอบ กำกับและติดตามการดำเนินการด้านการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่บุคลากรของส่วนงานให้เป็นไปตามนโยบายด้านไซเบอร์ขององค์กร
ด้านความรู้	๑. มีความรู้เกี่ยวกับหลักการและเทคนิคในการจัดการทรัพยากรของหน่วยงาน ๒. มีความรู้เกี่ยวกับนโยบายความมั่นคงปลอดภัยไซเบอร์ขององค์กร การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และการกำหนดวัตถุประสงค์และเป้าหมายของการฝึกอบรม ๓. มีความรู้เกี่ยวกับการแปลความหมาย การติดตาม และการจัดลำดับความสำคัญของความต้องการด้านความมั่นคงปลอดภัยไซเบอร์ และการรวบรวมความต้องการทั้งหน่วยงาน ๔. มีความรู้เกี่ยวกับการดำเนินการและภารกิจของหน่วยงาน ๕. มีความรู้เกี่ยวกับฟังก์ชันการทำงาน คุณภาพ และข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์และวิธีการนำไปใช้เสริมกับองค์ประกอบหรือกระบวนการทำงาน ๖. มีความรู้เกี่ยวกับแนวคิดการปรับปรุงกระบวนการในการสร้างความตระหนักรู้และการพัฒนาทักษะความรู้ความสามารถของบุคลากร ๗. มีความรู้เกี่ยวกับความต้องการในการจัดหา หรือการจัดหาเทคโนโลยีสารสนเทศ ๘. มีความรู้เกี่ยวกับประบวนการในการจัดซื้อจัดจ้าง
ด้านทักษะ	๑. สามารถทำงานร่วมกับผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ ๒. สามารถกำกับการดำเนินงานตามแผนงานหรือนโยบายด้านไซเบอร์ขององค์กร ๓. สามารถจัดทำแผนพัฒนาส่วนบุคคล (Individual Development Plan : IDP) สำหรับผู้ใช้งานในบทบาทที่มีความรับผิดชอบสูงด้านความมั่นคงปลอดภัยไซเบอร์ ๔. สามารถกำกับและติดตามความตระหนักรู้และทักษะของผู้ใช้งานระบบทั้งหมด (ทั้งนี้อาจรวมถึงหน่วยงานภายนอกที่ทำหน้าที่ดูแลระบบ) ทั้งระบบสนับสนุนทั่วไปและระบบงานหลัก และได้รับการฝึกอบรมเกี่ยวกับวิธีการปฏิบัติตามความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์อย่างเหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบ ๕. สามารถกำกับและติดตามความเข้าใจข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของแต่ละระบบสารสนเทศที่ผู้ใช้งาน (อาจรวมถึงหน่วยงานภายนอกที่ทำหน้าที่ดูแลระบบ) ต้องใช้งาน ๖. สามารถกำกับและติดตามการพัฒนาและปรับปรุงการประมาณการค่าใช้จ่าย ๗. สามารถประเมิน หรือรับรองความน่าเชื่อถือของบุคคลหรือองค์กรที่ทำหน้าที่จัดหาผลิตภัณฑ์หรือบริการ ๘. สามารถตรวจสอบการปฏิบัติตามแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามกระบวนการที่กำหนด

ตำแหน่ง : ผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ (INFORMATION SECURITY OFFICER)	
คำอธิบาย บทบาท	ผู้ทำหน้าที่ดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ในการรวบรวม ประมวลผล และ/หรือระบุตำแหน่งทางภูมิศาสตร์ของระบบ เพื่อใช้ประโยชน์ในการค้นหา และ/หรือติดตามเป้าหมายที่สนใจ ดำเนินการติดตามระบบเครือข่าย วิเคราะห์ทางยุทธวิธีทางนิติวิทยาศาสตร์ และเมื่อได้รับคำสั่งให้ดำเนินการบนเครือข่าย
ด้านความรู้	๑. มีความรู้เกี่ยวกับอัลกอริทึมการเข้ารหัส ความสามารถในการเข้ารหัส ข้อจำกัด และการมีส่วนร่วมในการปฏิบัติการทางไซเบอร์ ๒. มีความรู้เกี่ยวกับเครือข่ายทั่วไปและโปรโตคอลกำหนดเส้นทาง การบริการ และวิธีการสื่อสารเครือข่าย อุปกรณ์เครือข่ายทางกายภาพและทางตรรกะ ๓. มีความรู้เกี่ยวกับโครงสร้าง แนวทาง และกลยุทธ์ของเครื่องมือเจาะระบบ และเทคนิคการเจาะระบบ ๔. มีความรู้เกี่ยวกับพื้นฐานการพัฒนาซอฟต์แวร์และช่องโหว่ ซอฟต์แวร์ไม่พึงประสงค์ ๕. มีความรู้เกี่ยวกับผลิตภัณฑ์ความมั่นคงปลอดภัยบนโฮสต์และผลกระทบต่อการถูกโจมตีและช่องโหว่ ๖. มีความรู้เกี่ยวกับกระบวนการและเทคนิคที่ใช้ในการตรวจจับกิจกรรมการโจมตี กลยุทธ์ และเทคนิคการหลบเลี่ยง ๗. มีความรู้เกี่ยวกับขั้นตอนพื้นฐานการสำรองข้อมูลและการกู้คืน รวมถึงความแตกต่างของชนิดการสำรองข้อมูล (การสำรองข้อมูลแบบเต็ม/ปกติ การสำรองข้อมูลส่วนต่าง และการสำรองข้อมูลส่วนเพิ่มเติม) ๘. มีความรู้เกี่ยวกับตัวเลือกด้านฮาร์ดแวร์และซอฟต์แวร์การรักษาความมั่นคงปลอดภัยไซเบอร์ สิ่งประดิษฐ์ด้านระบบเครือข่ายที่มีผลต่อการโจมตี และผลกระทบด้านความมั่นคงปลอดภัยของการกำหนดค่าซอฟต์แวร์ ๙. มีความรู้เกี่ยวกับพื้นฐานเครือข่ายไร้สาย ช่องโหว่เครือข่ายไร้สายแบบต่างอัลกอริทึมการเข้ารหัสของเครือข่ายไร้สาย ๑๐. มีความรู้เกี่ยวกับการตรวจสอบและขั้นตอนการบันทึกเหตุการณ์ เพื่อนำมาวิเคราะห์การโจมตีหรือช่องโหว่ ๑๑. ความรู้พื้นฐานทางนิติวิทยาศาสตร์ดิจิทัล โครงสร้างระบบปฏิบัติการและการปฏิบัติเพื่อดึงข้อมูลมาดำเนินการทางนิติวิทยาศาสตร์
ด้านทักษะ	๑. สามารถวิเคราะห์เพื่อสกัดข้อมูลจากการถ่ายโอนข้อมูลหน่วยความจำ ๒. สามารถระบุการทำงานของอุปกรณ์ในแต่ละระดับของรูปแบบโปรโตคอล ๓. สามารถวิเคราะห์เป้าหมายการสื่อสารทั้งภายในและภายนอกที่รวบรวมจากเครือข่ายไร้สาย ๔. สามารถตรวจสอบการทำงานของระบบและการสนองต่อเหตุการณ์เพื่อตอบสนองการกระตุ้น การสังเกตแนวโน้ม หรือกิจกรรมที่ผิดปกติ ๕. สามารถดำเนินการกลวิธี เทคนิค และขั้นตอนการรวบรวมข้อมูลเครือข่าย เครือข่ายไร้สาย รวมถึงความสามารถในการถอดรหัส/เครื่องมือ ๖. สามารถใช้เครื่องมือ เทคนิค และขั้นตอนเพื่อใช้ประโยชน์จากการโจมตีจากระยะไกลและการระบุเป้าหมายได้

ตำแหน่ง : ผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ (INFORMATION SECURITY OFFICER)	
ด้านทักษะ	๗. สามารถสกัดข้อมูลจากการจับข้อมูลเครือข่าย เพื่อวิเคราะห์การโจมตีหรือช่องโหว่ ๘. สามารถใช้พื้นฐานทางนิติวิทยาศาสตร์ดิจิทัลในการเก็บรักษาหลักฐาน และปฏิบัติเกี่ยวกับการตรวจสอบการโจมตีและช่องโหว่ ๙. สามารถเก็บรวบรวมข้อมูลกิจกรรมบนระบบเครือข่ายและเครือข่ายไร้สาย

ตำแหน่ง : ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (INFORMATION TECHNOLOGY OFFICER)	
คำอธิบายบทบาท	ผู้ทำหน้าที่เป็นผู้ดูแลระบบ ติดตั้ง กำหนดค่า แก้ไขปัญหา บำรุงรักษาฮาร์ดแวร์และซอฟต์แวร์ และจัดการบัญชีผู้ใช้ระบบ
ด้านความรู้	๑. มีความรู้เกี่ยวกับหลักการด้านระบบเครือข่ายคอมพิวเตอร์ โปรโตคอล สถาปัตยกรรมและวิธีการรักษาความมั่นคงปลอดภัยเครือข่าย รวมถึงหลักการจัดการบริการบนเครือข่ายที่เกี่ยวข้องกับมาตรฐาน ๒. มีความรู้เกี่ยวหลักการของผู้ดูแลระบบ พื้นฐานการดูแลระบบ ระบบเครือข่ายและเทคนิคการสร้างความแข็งแกร่งระบบปฏิบัติการและเครื่องแม่ข่าย เครื่องมือและเทคนิคการปรับแต่งประสิทธิภาพ ระบบแฟ้มข้อมูล ประเภทและความถี่ของการบำรุงรักษาตามปกติเพื่อให้อุปกรณ์ทำงานได้อย่างถูกต้อง ๓. มีความรู้เกี่ยวกับนโยบายผู้ใช้งานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เช่น บัญชีผู้ใช้งาน การสร้างบัญชีผู้ใช้งาน กฎของรหัสผ่าน การควบคุมการเข้าถึง เป็นต้น ๔. มีความรู้เกี่ยวกับสถาปัตยกรรมเทคโนโลยีสารสนเทศ เทคโนโลยีการจำลองเสมือนและเครื่องเสมือน (Virtual Technology and Virtual Machine) ความมั่นคงปลอดภัยเครือข่ายเสมือน รวมถึงรูปแบบระบบเครือข่าย ๕. มีความรู้เกี่ยวกับเครื่องมือในการวิเคราะห์และเทคนิคในการระบุข้อผิดพลาดเครื่องแม่ข่าย/ระบบ ๖. มีความรู้เกี่ยวกับข้อมูล ข้อมูลส่วนบุคคล มาตรฐานความมั่นคงปลอดภัยข้อมูล การจำแนกประเภทข้อมูล และขั้นตอนการบุกรุกสารสนเทศ ๗. มีความรู้เกี่ยวกับทฤษฎี แนวคิดและวิธีการทางวิศวกรรมระบบ หลักการและวิธีการรวมส่วนประกอบของระบบ
ด้านทักษะ	๑. สามารถติดตั้ง ตั้งค่า และปรับแต่งการทำงานของซอฟต์แวร์และเครื่องแม่ข่าย และมีทักษะในการดูแลระบบปฏิบัติการ ๒. สามารถวิเคราะห์ปัญหาการเชื่อมต่อเครือข่าย และวิเคราะห์ข้อผิดพลาดจากการเชื่อมต่อ ๓. สามารถบำรุงรักษาบริการบัญชีผู้ใช้ ๔. สามารถใช้งานบนเทคโนโลยีการจำลองเสมือนและเครื่องเสมือน (Virtual Technology and Virtual Machine) ๕. สามารถตั้งค่าและใช้ซอฟต์แวร์เครื่องมือป้องกันคอมพิวเตอร์ เช่น ซอฟต์แวร์ป้องกันการบุกรุกเครือข่าย โปรแกรมป้องกันไวรัส โปรแกรมป้องกันสปายแวร์ ๖. สามารถดำเนินการวางแผน การจัดการ การบำรุงรักษาระบบและเครื่องแม่ข่าย การแก้ปัญหาทางกายภาพและทางเทคนิคที่ส่งผลต่อประสิทธิภาพระบบและเครื่องแม่ข่าย ๗. สามารถแก้ปัญหาความล้มเหลวขององค์ประกอบของระบบและกู้คืน ๘. สามารถระบุและคาดการณ์ประสิทธิภาพของระบบและเครื่องแม่ข่าย ความพร้อมใช้งาน สมรรถนะ หรือปัญหาการกำหนดค่า

ตำแหน่ง : ผู้ปฏิบัติงานด้านระบบควบคุมอุตสาหกรรมและเทคโนโลยีการปฏิบัติงาน (INDUSTRIAL CONTROL SYSTEMS AND OPERATIONAL TECHNOLOGIES OFFICER)	
คำอธิบายบทบาท	ผู้ทำหน้าที่เกี่ยวข้องกับการกำกับดูแลความปลอดภัยทางไซเบอร์ การบริหารความเสี่ยงและการปฏิบัติตาม การออกแบบและการพัฒนา การดำเนินงานและการบริหารการปกป้องและป้องกันระบบเทคโนโลยีการปฏิบัติงาน (OT) เช่น ระบบควบคุมอุตสาหกรรม (ICS) และการกำกับดูแลระบบควบคุมและเก็บข้อมูล (SCADA) สามารถแยกย่อยตามลักษณะงานได้ ดังนี้ ๑. สถาปนิกด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Architect) ๒. ผู้เชี่ยวชาญด้านโครงสร้างพื้นฐานความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Infrastructure Specialist) ๓. นักวิเคราะห์การป้องกันด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Defense Analyst) ๔. เจ้าหน้าที่ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Officer) ๕. เจ้าหน้าที่รับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Responder)
ด้านความรู้	๑. มีความรู้เกี่ยวกับหลักการด้านระบบเครือข่ายคอมพิวเตอร์ ส่วนประกอบของระบบเครือข่ายโปรโตคอลสื่อสาร เทคโนโลยีระบบเครือข่ายทั้งด้านสารนเทศและด้านระบบควบคุมอุตสาหกรรมและเทคโนโลยีการปฏิบัติงาน การดำเนินการและความเหมาะสมของการกระบวนการและการความคุมด้านความมั่นคงปลอดภัยเครือข่าย ๒. มีความรู้ด้านอุปกรณ์ระบบควบคุมอุตสาหกรรมและภาษาการโปรแกรมสำหรับอุตสาหกรรม สภาพแวดล้อมและการทำงาน การควบคุมดูแลและองค์ประกอบของระบบเก็บข้อมูล ๓. มีความรู้เกี่ยวกับหลักการของความมั่นคงปลอดภัยไซเบอร์และความเป็นส่วนตัว ภัยคุกคาม ช่องโหว่ของระบบ การพิสูจน์ตัวตน การกำหนดสิทธิ์ และกระบวนการควบคุมการเข้าถึง ข้อกำหนดทางกฎหมายและข้อบังคับที่เกี่ยวข้องกับจริยธรรมและความเป็นส่วนตัว ๔. มีความรู้เกี่ยวกับภาพรวมของภัยคุกคามต่อระบบควบคุมอุตสาหกรรม ภัยคุกคามและช่องโหว่ในระบบควบคุมอุตสาหกรรมและสภาพแวดล้อม กระบวนการและเทคโนโลยีด้านความมั่นคงปลอดภัยระบบควบคุมอุตสาหกรรม ๕. มีความรู้เกี่ยวกับวิธีการตรวจจับการบุกรุกและเทคนิคในการตรวจจับการบุกรุกสำหรับระบบควบคุมอุตสาหกรรม ๖. มีความรู้ความเข้าใจเกี่ยวกับการประเมินความเสี่ยง การลดความเสี่ยง และวิธีการจัดการผลกระทบจากการปฏิบัติงานที่อาจเกิดขึ้นกับองค์กรจากการละเมิดความมั่นคงปลอดภัยไซเบอร์ ๗. มีความรู้เกี่ยวกับแนวปฏิบัติที่ดีที่สุดสำหรับการตอบสนองเหตุการณ์และการจัดการเหตุการณ์ ๘. มีความรู้เกี่ยวกับกฎระเบียบความมั่นคงปลอดภัยไซเบอร์และข้อกำหนดที่เกี่ยวข้องกับองค์กร การจัดประเภทเอกสารและข้อมูลระดับชาติและระดับองค์กร มาตรฐานการทำเครื่องหมาย นโยบายและระเบียบปฏิบัติความรู้ข้างต้นเป็นความรู้พื้นฐานสำหรับตำแหน่ง

ตำแหน่ง : ผู้ปฏิบัติงานด้านระบบควบคุมอุตสาหกรรมและเทคโนโลยีการปฏิบัติงาน (INDUSTRIAL CONTROL SYSTEMS AND OPERATIONAL TECHNOLOGIES OFFICER)	
ด้านความรู้	ผู้ปฏิบัติงานด้านระบบควบคุมอุตสาหกรรมและเทคโนโลยีการปฏิบัติงาน หน่วยงานอาจกำหนดความรู้เพิ่มเติมให้เหมาะสมกับลักษณะงานได้ เช่น - มีความรู้เกี่ยวกับการตั้งค่า ปรับแต่ง เครื่องมือสำหรับป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์ระบบเครือข่าย - มีความรู้เกี่ยวกับเครื่องมือวิเคราะห์การจราจรเครือข่าย ทั้งด้านวิธีการวิเคราะห์และกระบวนการทำงาน - มีความรู้เกี่ยวกับการดูแลระบบ การจัดการเครือข่าย และวิธีการทำให้ระบบปฏิบัติการมีความรู้เกี่ยวกับต่อการโจมตีพอร์ตและบริการของระบบปฏิบัติการวินโดวส์และยูนิกซ์ - มีความรู้เกี่ยวกับแหล่งข้อมูลข่าวกรองภัยคุกคาม ความสามารถและข้อจำกัด - มีความรู้เกี่ยวกับวิธีการทดสอบและประเมินความมั่นคงปลอดภัยของระบบ - มีความรู้เกี่ยวกับระบบฝังตัวและวิธีการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่สามารถนำไปใช้กับระบบเหล่านี้ได้
ด้านทักษะ	ทักษะข้างต้นเป็นทักษะพื้นฐานสำหรับตำแหน่งผู้ปฏิบัติงานด้านระบบควบคุมอุตสาหกรรมและเทคโนโลยีการปฏิบัติงาน หน่วยงานอาจกำหนดทักษะเพิ่มเติมให้เหมาะสมกับลักษณะงานได้ เช่น - สามารถสแกนช่องโหว่และระบุช่องโหว่จากผลลัพธ์ที่ดำเนินการได้ - สามารถใช้เครื่องมือ วิธีการ และเทคนิคในการออกแบบระบบที่ปลอดภัย - สามารถทำงานร่วมกับเจ้าหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้คำแนะนำที่มีประสิทธิภาพในเรื่องต่างๆ ด้านความมั่นคงปลอดภัยไซเบอร์แก่ผู้นำขององค์กร - สามารถทำงานร่วมกับสถาปนิกองค์กร วิศวกรความมั่นคงปลอดภัยของระบบ เจ้าของระบบ เจ้าของการควบคุม และเจ้าหน้าที่รักษาความมั่นคงปลอดภัยของระบบเพื่อใช้การควบคุมความมั่นคงปลอดภัยในการควบคุมระบบเฉพาะ ระบบผสมผสานหรือระบบทั่วไป ในสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศและด้านระบบควบคุมอุตสาหกรรมและเทคโนโลยีการปฏิบัติงาน - สามารถรวบรวมข้อมูลจากแหล่งข้อมูลความมั่นคงปลอดภัยไซเบอร์ที่หลากหลาย - สามารถทำงานร่วมกับผู้นำขององค์กรในการพัฒนากลยุทธ์การจัดการความเสี่ยงเพื่อจัดการกับความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ - สามารถทำงานร่วมกับผู้นำขององค์กรเพื่อกำหนดสถานะความเสี่ยงขององค์กรโดยพิจารณาจากความเสี่ยงโดยรวมจากการดำเนินงานและการใช้ระบบ - สามารถประเมินความเพียงพอของการออกแบบระบบรักษาความมั่นคงปลอดภัยไซเบอร์ - สามารถวิเคราะห์เครื่องมือ เทคนิค และกระบวนการที่ผู้บุกรุกใช้ในการโจมตีจากระยะไกลเพื่อแสวงหาประโยชน์และการฝังตัวเพื่อดำเนินการต่อไปกับเป้าหมาย - มีความสามารถในการทบทวนกลยุทธ์ขององค์กรหรือเอกสารทางกฎหมาย ระเบียบข้อบังคับ หรือนโยบายที่เกี่ยวข้อง เพื่อระบุประเด็นที่ต้องชี้แจงหรือดำเนินการ - สามารถประเมินศักยภาพของแหล่งข้อมูลเพื่อสร้างความน่าเชื่อถือในการสืบสวนทางไซเบอร์

ตำแหน่ง : ผู้ตรวจสอบภายใน (INTERNAL AUDITOR)	
คำอธิบาย บทบาท	ผู้ตรวจสอบภายใน เป็นผู้ดำเนินการประเมินระบบสารสนเทศ ประเมินความมั่นคงปลอดภัยไซเบอร์ หรือส่วนประกอบอื่นแต่ละรายการ เพื่อพิจารณาการปฏิบัติตามมาตรฐานที่องค์กรกำหนด และมาตรฐานที่เผยแพร่สาธารณะ
ด้านความรู้	๑. มีความรู้เกี่ยวกับหลักการด้านระบบเครือข่ายคอมพิวเตอร์ โปรโตคอล และวิธีการรักษาความมั่นคงปลอดภัยเครือข่าย รวมถึงหลักการจัดการบริการบนเครือข่ายที่เกี่ยวข้องกับมาตรฐาน ๒. มีความรู้เกี่ยวกับกระบวนการจัดการความเสี่ยง การประเมินความเสี่ยง วิธีการลดความเสี่ยง ความต้องการตามกรอบแนวคิดการจัดการความเสี่ยง ๓. มีความรู้เกี่ยวกับกฎหมาย ข้อบังคับ การกำกับดูแล นโยบาย และจริยธรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงหลักการและวิธีการวิเคราะห์ที่เป็นมาตรฐานในอุตสาหกรรมและเป็นที่ยอมรับขององค์กร ๔. มีความรู้เกี่ยวกับหลักการด้านความมั่นคงปลอดภัยไซเบอร์ ภัยคุกคามทางไซเบอร์ และช่องโหว่ ๕. มีความรู้เกี่ยวกับหลักการและกรอบแนวคิดของสถาปัตยกรรมเทคโนโลยีสารสนเทศ หลักการของวงจรการจัดการระบบ รวมถึงความมั่นคงปลอดภัยซอฟต์แวร์ และการนำไปใช้ ๖. มีความรู้เกี่ยวกับข้อกำหนดในการจัดซื้อจัดจ้างด้านสารสนเทศ และกระบวนการของวงจรการจัดซื้อจัดจ้าง ๗. มีความรู้เกี่ยวกับการแปลความหมาย การติดตาม และการจัดลำดับความสำคัญของความต้องการด้านความมั่นคงปลอดภัยไซเบอร์ และการรวบรวมความต้องการจากทั้งหน่วยงาน ๘. มีความรู้เกี่ยวกับหลักการและเทคนิคในการจัดการทรัพยากรของหน่วยงาน
ด้านทักษะ	๑. สามารถระบุมาตรการหรือตัวชี้วัดประสิทธิภาพของระบบ และการดำเนินการที่จำเป็นในการปรับปรุงหรือแก้ไขประสิทธิภาพ ที่สัมพันธ์กับเป้าหมายของระบบ ๒. สามารถดำเนินการตรวจสอบหรือทบทวนระบบทางเทคนิค ๓. สามารถรับรองได้ว่ามีการปฏิบัติตามแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ตามกระบวนการที่กำหนด ๔. สามารถตรวจสอบการวางแผนและปฏิบัติงานตรวจสอบภายในที่ได้รับมอบหมายโดยสอดคล้องกับมาตรฐานที่เกี่ยวข้อง ๕. สามารถระบุและดำเนินการกับความเสี่ยงที่มีโดยเฉพาะต่อความมั่นคงปลอดภัยไซเบอร์และต่อสภาพแวดล้อมองค์กร ๖. สามารถกำหนดทิศทางเชิงกลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์ และสื่อสารอย่างมีประสิทธิผล รักษาความสัมพันธ์ และบริหารบุคลากรและกระบวนการของการตรวจสอบภายใน

ตำแหน่ง : เจ้าหน้าที่ปฏิบัติงานด้านการกำกับดูแล ความเสี่ยง และการปฏิบัติตามข้อกำหนด (GOVERNANCE, RISK AND COMPLIANCE OFFICER)	
คำอธิบาย บทบาท	ผู้ทำหน้าที่บริหารจัดการและกำกับดูแลองค์กร ให้คำแนะนำแก่ผู้บริหารเพื่อดำเนินการให้เป็นไปตามกฎระเบียบที่เกี่ยวข้อง มีการบริหารความเสี่ยงที่เป็นระบบและตรงประเด็น สามารถจัดกระบวนการทำงานให้ปฏิบัติตามระเบียบและการควบคุมภายในอย่างเหมาะสม สามารถสื่อสารข้อมูลที่ถูกต้องเหมาะสมต่อผู้เกี่ยวข้องทุกระดับ
ด้านความรู้	๑. มีความรู้เกี่ยวกับหลักการด้านระบบเครือข่ายคอมพิวเตอร์ โปรโตคอล และวิธีการรักษาความมั่นคงปลอดภัยเครือข่าย รวมถึงหลักการจัดการบริการบนเครือข่ายที่เกี่ยวข้องกับมาตรฐาน ๒. มีความรู้เกี่ยวกับกระบวนการจัดการความเสี่ยง การประเมินความเสี่ยง วิธีการลดความเสี่ยง ความต้องการตามกรอบแนวคิดการจัดการความเสี่ยง ๓. มีความรู้เกี่ยวกับกฎหมาย ข้อบังคับ การกำกับดูแล นโยบาย และจริยธรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงหลักการและวิธีการวิเคราะห์ที่เป็นมาตรฐานในอุตสาหกรรมและเป็นที่ยอมรับขององค์กร ๔. มีความรู้เกี่ยวกับหลักการด้านความมั่นคงปลอดภัยไซเบอร์ ภัยคุกคามและช่องโหว่ การป้องกันทางไซเบอร์ เครื่องมือประเมินช่องโหว่ เครื่องมือและเทคนิคการทดสอบการเจาะระบบ การจัดการความเสี่ยงที่เกี่ยวกับการใช้งาน กระบวนการ การเก็บข้อมูลและการสื่อสารข้อมูลหรือสารสนเทศ ๕. มีความรู้เกี่ยวกับหลักการและกรอบแนวคิดของสถาปัตยกรรมเทคโนโลยีสารสนเทศ หลักการของวงจรการจัดการระบบ รวมถึงความมั่นคงปลอดภัยซอฟต์แวร์ และการนำไปใช้ ๖. มีความรู้เกี่ยวกับข้อมูล ข้อมูลส่วนบุคคล มาตรฐานความมั่นคงปลอดภัยข้อมูล การจำแนกประเภทข้อมูล และขั้นตอนการบุกรุกสารสนเทศ ๗. มีความรู้เกี่ยวกับวิธีการทางอุตสาหกรรมในปัจจุบันสำหรับการประเมินการนำไปใช้และการเผยแพร่การประเมินความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ การตรวจสอบการตรวจจับ และเครื่องมือและขั้นตอนการแก้ไขโดยใช้แนวคิดและสมรรถนะตามมาตรฐาน ๘. มีความรู้เกี่ยวกับกระบวนการกำหนดเป้าหมาย วัตถุประสงค์ ภารกิจหลักขององค์กรด้านความมั่นคงปลอดภัยสารสนเทศ
ด้านทักษะ	๑. สามารถกำกับและติดตามการดำเนินการขององค์กร ให้เป็นไปตามกฎระเบียบที่เกี่ยวข้อง ๒. สามารถแยกแยะความต้องการในการป้องกันระบบสารสนเทศและเครือข่าย เช่น การควบคุมความมั่นคงปลอดภัยของระบบและแอปพลิเคชัน การสำรองข้อมูล การบริการบนเครือข่าย เป็นต้น ๓. สามารถใช้หลักการด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อการรักษาความลับ ความถูกต้องครบถ้วน ความพร้อมใช้งาน การพิสูจน์ตัวตน และการห้ามปฏิเสธความรับผิดชอบ ต่อการใช้งานระบบ ๔. สามารถพิจารณาว่าความมั่นคงปลอดภัยของระบบควรทำงานอย่างไร และสามารถปรับเปลี่ยนตามเงื่อนไข กระบวนการ หรือสภาพแวดล้อมที่ส่งผลกระทบต่อผลลัพธ์

ตำแหน่ง : เจ้าหน้าที่ปฏิบัติงานด้านการกำกับดูแล ความเสี่ยง และการปฏิบัติตามข้อกำหนด (GOVERNANCE, RISK AND COMPLIANCE OFFICER)	
ด้านทักษะ	๕. สามารถระบุมาตรการหรือตัวชี้วัดประสิทธิภาพของระบบและการดำเนินการที่จำเป็นในการปรับปรุงหรือแก้ไขประสิทธิภาพ ที่สัมพันธ์กับเป้าหมายของระบบ ๖. สามารถเลือกใช้เครื่องมือและเทคนิคการเจาะระบบเพื่อตรวจสอบความมั่นคงปลอดภัยไซเบอร์และระบุช่องโหว่ของระบบและสามารถระบุความเสี่ยงที่เกิดขึ้น ๗. สามารถประเมินหรือรับรองความน่าเชื่อถือของบุคคลหรือองค์กรที่ทำหน้าที่จัดหาผลิตภัณฑ์หรือบริการ ๘. สามารถแยกแยะและกำหนดปัจจัยเสี่ยงต่อระบบสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ รวมถึงดัชนีชี้วัดความสำเร็จของการบริหารความเสี่ยงและการรายงานสถานะความเสี่ยง

ผนวก ข

ตัวอย่างการวัดผลการสร้างความตระหนักรู้และการฝึกอบรม

๑. คำถามหลัก (Critical Element)	บุคลากรได้รับการฝึกอบรมอย่างเพียงพอเพื่อตอบสนองความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์หรือไม่
๒. คำถามลำดับรอง (Subordinate Question)	มีการบันทึกและติดตามการฝึกอบรมและการพัฒนาวิชาชีพของบุคลากรหรือไม่
๓. การวัด/ค่าที่ใช้ในการวัด (Metric)	สัดส่วนของบุคลากรที่มีหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้รับการฝึกอบรมเฉพาะทาง
๔. วัตถุประสงค์ (Purpose)	เพื่อวัดระดับความเชี่ยวชาญระหว่างหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่กำหนดและความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์สำหรับระบบสารเทศเฉพาะภายในหน่วยงาน
๕. หลักฐานการดำเนินการ (Implementation Evidence)	๑. มีการกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญพร้อมเกณฑ์คุณสมบัติและจัดทำเป็นเอกสารหรือไม่ ☐ มี ☐ ไม่มี ๒. มีการเก็บบันทึกว่าบุคลากรคนใดมีหน้าที่ความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นพิเศษหรือไม่ ☐ มี ☐ ไม่มี ๓. มีบุคลากรที่มีหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญจำนวนกี่คนในหน่วยงาน ..... ๔. มีการบันทึกการฝึกอบรมที่บ่งบอกได้ว่าการอบรมของบุคลากรตรงกับความรู้ที่บุคลากรควรได้รับหรือไม่ ☐ มี ☐ ไม่มี ๕. แผนการฝึกอบรมระบุว่าการฝึกอบรมนั้นจำเป็นต้องมีในการฝึกอบรมเฉพาะทางหรือไม่ ☐ มี ☐ ไม่มี ๖. มีบุคลากรที่มีหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญเท่าใด ที่ได้รับการฝึกอบรมที่จำเป็นตามที่ระบุไว้ในแผนการฝึกอบรม ..... ๗. หากมีบุคลากรที่ไม่ได้รับการฝึกอบรม ให้ระบุเหตุผลทั้งหมดที่เกี่ยวข้อง: ☐ งบประมาณไม่เพียงพอ ☐ เวลาไม่เพียงพอ ☐ ไม่มีหลักสูตร/ไม่สามารถระบุหลักสูตรได้ ☐ บุคลากรยังไม่ได้บรรจุลงกรอบอัตราจ้าง ☐ อื่นๆ (ระบุ) .....
๖. ความถี่ (Frequency)	อย่างน้อยปีละครั้ง

๗. สูตรการคำนวน (Formula)	จำนวนบุคลากรที่มีหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญที่ได้รับการฝึกอบรมที่จำเป็นตามที่ระบุไว้ในแผนการฝึกอบรม (คำถามที่ ๖) / จำนวนบุคลากรที่มีหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญในหน่วยงาน (คำถามที่ ๓)
๘. แหล่งที่มาของข้อมูล (Data Source)	ฐานข้อมูลหรือบันทึกการฝึกอบรม หัวข้อข้อมูลของบุคลากรที่ได้รับใบรับรองหรือผ่านหลักสูตร
๙. ตัวชี้วัด (Indicators)	เป้าหมาย คือ ร้อยละ ๑๐๐ (๑๐๐%) หากไม่ครบ หน่วยงานอาจไม่มีความพร้อมในการต่อสู้กับภัยคุกคามทางไซเบอร์และช่องโหว่ล่าสุด เพราะข้อกำหนดและเครื่องมือสำหรับควบคุมความมั่นคงปลอดภัยไซเบอร์เฉพาะมีการเปลี่ยนแปลงและพัฒนาอย่างรวดเร็ว การฝึกอบรมอย่างต่อเนื่องจึงมีความสำคัญต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ตัวชี้วัดนี้จะสัมพันธ์กับจำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และจำนวนการป้องกันช่องโหว่ เพื่อพิสูจน์ว่าการเพิ่มจำนวนของการฝึกอบรมให้บุคลากรที่มีหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้รับการฝึกอบรมเฉพาะทาง สามารถลดจำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์บางประเภท และจำนวนช่องโหว่ได้

หมายเหตุ : คำถามที่ ๑ และ ๒ ใช้เพื่อวัดความน่าเชื่อถือของข้อมูลสำหรับการวัดผลนี้ ต้องกำหนดบทบาทและความรับผิดชอบในนโยบายและระเบียบปฏิบัติ และระบุบุคลากรเพื่อดำเนินการตามบทบาท คำถามที่ ๔ และ ๕ ให้ข้อมูลเพื่อช่วยระบุการฝึกอบรมเฉพาะทางที่บุคลากรต้องการ หากไม่มีการฝึกอบรมบุคลากรอย่างเพียงพอ คำถามที่ ๗ ช่วยระบุสาเหตุของการฝึกอบรมที่ไม่เพียงพอ ฝ่ายบริหารสามารถดำเนินการเพื่อแก้ไขจากข้อบกพร่องนี้ได้

ผนวก ค

ตัวอย่างโครงร่างแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม

บทสรุปผู้บริหาร (Executive Summary)
ข้อมูลพื้นฐาน (Background) ● OMB A-130, Appendix III ● Federal Information Security Management Act (FISMA) ● นโยบายเฉพาะของแผนก/ส่วนงานหรือหน่วยงาน (ข้อมูลหรือเหตุผลที่เกี่ยวข้องอื่น ๆ ที่อาจผลักดันการสร้างความตระหนักรู้ แผนงานหรือโครงการและแผนการฝึกอบรม)
นโยบายความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Agency Cybersecurity Policy) ● เป้าหมาย (Goals) ● วัตถุประสงค์ (Objectives) ● บทบาท/ความรับผิดชอบ (Roles/Responsibilities)
การสร้างความตระหนักรู้ (Awareness) ● กลุ่มเป้าหมายที่เข้าร่วม (Audience; Management and All Employees) ● กิจกรรมและวันที่จัดกิจกรรม (Activities and Target Dates) ● กำหนดการ (Schedule) ● ทบทวนและปรับปรุงเอกสาร/สื่อ เนื้อหา และกระบวนการ (Review and Updating of Materials and Methods)
การฝึกอบรม/การศึกษา (Training/Education) ● **บทบาท ๑ : ผู้บริหารระดับสูง และหัวหน้าส่วนงาน (Executives and Managers)** ○ ผลลัพธ์การเรียนรู้ (Learning Objectives) ○ ประเด็นที่ให้ความสนใจ (Focus Areas) ○ วิธีการ/กิจกรรม (Methods/Activities) ○ กำหนดการ (Schedule) ○ เกณฑ์การประเมิน (Evaluation Criteria) ● **บทบาท ๒ : เจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Staff)** ○ ผลลัพธ์การเรียนรู้ (Learning Objectives) ○ ประเด็นที่ให้ความสนใจ (Focus Areas) ○ วิธีการ/กิจกรรม (Methods/Activities) ○ กำหนดการ (Schedule) ○ เกณฑ์การประเมิน (Evaluation Criteria) ● **บทบาท ๓ : ผู้ดูแลระบบ/ผู้ดูแลระบบเครือข่าย (System/Network Administrators)** ○ ผลลัพธ์การเรียนรู้ (Learning Objectives) ○ ประเด็นที่ให้ความสนใจ (Focus Areas) ○ วิธีการ/กิจกรรม (Methods/Activities) ○ กำหนดการ (Schedule)

บทสรุปผู้บริหาร (Executive Summary)	
○ เกณฑ์การประเมิน (Evaluation Criteria) . . และบทบาทอื่นที่มีความสำคัญต่อความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์	
ใบรับรองความเป็นผู้เชี่ยวชาญ (Professional Certification) ● **บทบาท ๑ : เจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Staff)** ○ ผลลัพธ์การเรียนรู้ (Learning Objectives) ○ ประเด็นที่ให้ความสนใจ (Focus Areas) ○ วิธีการ/กิจกรรม (Methods/Activities) ○ กำหนดการ (Schedule) ○ เกณฑ์การประเมิน (Evaluation Criteria) ● **บทบาท ๒ : ผู้ดูแลระบบ/ผู้ดูแลระบบเครือข่าย (System/Network Administrators)** ○ ผลลัพธ์การเรียนรู้ (Learning Objectives) ○ ประเด็นที่ให้ความสนใจ (Focus Areas) ○ วิธีการ/กิจกรรม (Methods/Activities) ○ กำหนดการ (Schedule) ○ เกณฑ์การประเมิน (Evaluation Criteria) . . และบทบาทอื่นที่มีความสำคัญต่อความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์	
ความต้องการด้านทรัพยากร (Resource Requirements)	**ค่าใช้จ่าย (Cost)**
● คณะทำงาน (Staffing) ● สนับสนุนการทำสัญญา (Contracting Support) ● สิ่งอำนวยความสะดวก (Facilities) เช่น ห้องฝึกอบรม ห้องประชุมทางไกล ● สื่อ (Media) เช่น เครื่องแม่ข่ายสำหรับเอกสาร/สื่อ เนื้อหาบนเว็บไซต์และคอมพิวเตอร์	xxx,xxx บาท xxx,xxx บาท xxx,xxx บาท xxx,xxx บาท