กรณีศึกษาจากการดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานของรัฐ

ฉบับเผยแพร่เดือนกันยายน 2566

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

สำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

คำนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม 2562 และบังคับใช้ตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา เป็นกฎหมายซึ่งกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีประสิทธิภาพ และเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา 26 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ซึ่งมีบทบาทหน้าที่รับผิดชอบตามพระราชบัญญัติฯ และเป็นศูนย์กลางในการให้บริการทางวิชาการและเผยแพร่ความรู้ความเข้าใจเกี่ยวกับกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงรวบรวม และสรุปผลการตอบข้อหารือในการดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดทำเป็น **กรณีศึกษาจากการดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562** เพื่ออำนวยความสะดวกในการสืบค้นและเป็นประโยชน์ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้ศึกษาและปฏิบัติให้สอดคล้องตามพระราชบัญญัติฯ ต่อไป

สารบัญ

ส่วนที่ 1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 1

ส่วนที่ 2 นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ 13

ส่วนที่ 3 ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 16

ส่วนที่ 1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

คำถามที่ 1 เนื่องจากหน่วยงานอยู่ภายใต้การกำกับของรัฐ (องค์การมหาชน) นอกจากจะต้องจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แล้ว หน่วยงานจะต้องดำเนินการหรือจะต้องจัดทำประกาศอะไรเพิ่มเติมหรือไม่

ข้อชี้แจง ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 หน่วยงานของรัฐต้องปฏิบัติตามด้วยกันหลายมาตรา ได้แก่

- มาตรา 43 ดำเนินการตามนโยบายและแผนฯ
- มาตรา 44 จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ
- มาตรา 45 มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ
- มาตรา 46 แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการไปยังสำนักงาน
- มาตรา 58 ตรวจสอบ ประเมิน ป้องกัน รับมือ ลดความเสี่ยง และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

คำถามที่ 2 แผนการตรวจสอบและการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ใครเป็นผู้จัดทำและสามารถดำเนินการจัดทำได้อย่างไร มีตัวอย่างหรือไม่

ข้อชี้แจง เนื่องด้วยหน่วยงานของท่านเป็นหน่วยงานของรัฐ ซึ่งมิได้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จึงมีหน้าที่จะต้องจัดทำและดำเนินการตามประกาศ กกม. เรื่องประมวลแนวทางปฏิบัติฯ โดยมีการกำหนดให้หน่วยงานจะต้องจัดทำแผนการตรวจสอบและประเมิน ความเสี่ยง ตามประมวลฯ ข้อ 17, 18

ในประเด็นที่สอบถามว่าจะต้องทำอย่างไร มีตัวอย่างไหม สกมช. อยู่ระหว่างการจัดทำแนวทางปฏิบัติ ซึ่งคาดว่าจะแล้วเสร็จภายในปีงบประมาณ พ.ศ. 2566 ทั้งนี้ หน่วยงานอาจใช้หลักการประเมินความเสี่ยงด้านไซเบอร์และการตรวจสอบฯ ซึ่งเป็นที่ยอมรับในอุตสาหกรรม (Best Practices) อาทิ ISO/IEC 27001, ISO 19011, NIST SP 800-30, NIST SP 800-53A เป็นต้น

คำถามที่ 3 ถ้าหน่วยงานมีกลุ่มงานบริหารความเสี่ยงฯ จะสามารถเป็นผู้จัดทำแผนการตรวจสอบฯ ประเมินความเสี่ยงฯ และแผนการรับมือภัยคุกคามทางไซเบอร์ ได้หรือไม่

ข้อชี้แจง ในการกำหนดบทบาทหน้าที่ความรับผิดชอบในการจัดทำแผนการตรวจสอบฯ ประเมินความเสี่ยงฯ และแผนการรับมือภัยคุกคามทางไซเบอร์ นั้น ขึ้นอยู่กับบริบทของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะเป็นผู้กำหนด โดยผู้ประเมินความเสี่ยงฯ ควรดำเนินการโดยหน่วยงานหรือผู้ก่อให้เกิดความเสี่ยงและควบคุมความเสี่ยงในชั้นแรก (Business Unit หรือ First Line of Defense) และหน่วยงานหรือผู้กำกับภายใน (Second Line of Defense) เช่น หน่วยงานบริหารความเสี่ยง (Risk Management) หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance) ผู้จัดทำแผนการตรวจสอบฯ ควรดำเนินการโดยกลุ่มงานที่เกี่ยวข้องกับการตรวจสอบภายใน (Internal Audit หรือ Third Line of Defense) ซึ่งผลการตรวจสอบฯ และประเมินความเสี่ยงฯ ควรได้รับการรายงานถึงผู้บริหารสูงสุดของหน่วยงาน ทั้งนี้ ผู้ตรวจสอบฯ และผู้ประเมินความเสี่ยงฯ ควรเป็นคนละคนกัน

ประเด็นการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ ปัจจุบัน ยังมิได้มีการกำหนดว่า ควรเป็นหน้าที่ของกลุ่มงานใด อย่างไรก็ตาม ตามมาตรฐาน ISO/IEC 27001 จะเป็นหน้าที่ของทีม Operation ซึ่งมิใช่หน้าที่ของกลุ่มที่จัดทำบริหารความเสี่ยงฯ

คำถามที่ 4 กรณีหน่วยงานของรัฐ ที่ไม่ได้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ในการทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ จะมีการดำเนินการต่างจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ อย่างไร

ข้อชี้แจง หน่วยงานของรัฐ ที่ไม่ได้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะต้องปฏิบัติตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ เช่นเดียวกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแต่จะมีความแตกต่างกันในบางมาตรา ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ยกตัวอย่างเช่น มาตรา 54 หน่วยงานโครงสร้างพื้นฐานสาคัญทางสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง หรือมาตรา 57 เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศรายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามกำหนดในส่วนที่ 4 ทั้งนี้ กกม. อาจกำหนดหลักเกณฑ์และวิธีการการรายงานด้วยก็ได้ เป็นต้น

คำถามที่ 5 ในกรณีที่หน่วยงานมีนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของหน่วยงานอยู่แล้ว หน่วยงานสามารถใช้นโยบายฯ ดังกล่าวเป็นประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานได้หรือไม่ อย่างไร

ข้อชี้แจง หน่วยงานสามารถใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของหน่วยงานที่มีอยู่แล้ว เป็นประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานได้ ทั้งนี้นโยบายฯ ดังกล่าวจะต้องมีความถูกต้องครบถ้วนตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ด้วย

คำถามที่ 6 การกำหนดหลักเกณฑ์หน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จึงขอสอบถามว่าการตีความภารกิจหรือให้บริการ (Critical Service) ของหน่วยงาน หน่วยงานควรดำเนินการอย่างไร

ข้อชี้แจง ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564 หัวข้อ หลักเกณฑ์ที่นำมาใช้ประกอบการพิจารณา วรรคที่ 2 ประกอบกับ คำแนะนำ เรื่อง แนวทางพิจารณาให้ภารกิจหรือบริการของหน่วยงานที่อยู่ภายใต้การดูแลเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ข้อที่ 4 แนวทางกำหนดหลักเกณฑ์การพิจารณาให้ภารกิจหรือบริการของหน่วยงานที่อยู่ภายใต้การดูแลเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ วรรคที่ 2 กำหนดให้หน่วยงานควบคุมหรือกำกับดูแล ควรพิจารณาดำเนินการ พิจารณา ให้ภารกิจหรือบริการของหน่วยงานที่อยู่ภายใต้การดูแล เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยเป็นการดำเนินการร่วมกันระหว่างหน่วยงานควบคุมหรือกำกับดูแลกับ หน่วยงานที่คาดว่าจะเป็นหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ดังนั้น การตีความภารกิจหรือให้บริการ (Critical Service) ของหน่วยงานว่าจะอยู่ในภารกิจข้อใด จึงควรเป็นการดำเนินการร่วมกันระหว่างหน่วยงานที่คาดว่าจะเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกับหน่วยงานควบคุมหรือกำกับดูแลของตน ตามคำแนะนำ เรื่อง แนวทางพิจารณาให้ภารกิจหรือบริการของหน่วยงานที่อยู่ภายใต้การดูแล เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ข้อที่ 4 แนวทางกำหนดหลักเกณฑ์การพิจารณาให้ภารกิจหรือบริการของหน่วยงานที่อยู่ภายใต้การดูแลเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ วรรคที่ 2 กำหนดให้หน่วยงานควบคุมหรือกำกับดูแลควรพิจารณาดำเนินการตามขั้นตอน

นั้น แล้วจึงให้หน่วยงานควบคุมหรือกำกับดูแลดำเนินการ แจ้งผลการพิจารณากลับมายัง สกมช. ตามคำแนะนำที่กล่าวมาแล้วข้างต้น ตามลิงก์นี้ https://www.ncsa.or.th/standards-and-practices.html

คำถามที่ 7 การปฏิบัติตามมาตรา 53 ที่ระบุว่า ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำ เรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตน ขอให้ทาง สกมช. อธิบายเพิ่มเติมถึงการตรวจสอบต้องเป็นในลักษณะของการตรวจสอบ (Audit) หรือไม่ และถ้าเป็นการตรวจสอบ (Audit) หน่วยงานควบคุมหรือกำกับดูแลควรมีใบเซอร์รับรองความรู้ความสามารถในการตรวจสอบ (Audit) อะไรบ้าง เพื่อสร้างความมั่นใจให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต่อความถูกต้องและความเหมาะสมในการดำเนินการตามกฎหมาย

ข้อชี้แจง ตามมาตรา 53 กำหนดให้หน่วยงานควบคุมหรือกำกับดูแล (Regulator) จะต้องตรวจสอบ (Audit) มาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ภายใต้การกำกับควบคุมดูแลของตน อย่างไรก็ตาม มาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์อยู่ระหว่างจัดทำโดยสำนักงานฯ (กันยายน 2566) จึงยังอนุโลมจนกว่ามาตรฐานขั้นต่ำฯ โดยสำนักงานฯ จะแล้วเสร็จ ซึ่งในระหว่างนี้ หน่วยงานควบคุมหรือกำกับดูแลอาจพิจารณากำหนดมาตรฐานขั้นต่ำด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยหน่วยงานควบคุมหรือกำกับดูแลเองก็ได้ ซึ่งจะต้องไม่น้อยกว่าประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ที่สำนักงานฯ กำหนด และสามารถเข้าตรวจสอบตามมาตรฐานขั้นต่ำดังกล่าวได้ ทั้งนี้ ในช่วงแรกของการดำเนินการ หน่วยงานควบคุมหรือกำกับดูแลควรเข้าตรวจสอบเพื่อให้คำแนะนำในการเตรียมความพร้อมของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับก่อน จนเมื่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเริ่มมีความคุ้นเคยกับมาตรฐานขั้นต่ำดังกล่าวแล้ว หน่วยงานควบคุมหรือกำกับดูแลจึงจะเข้าตรวจสอบเพื่อให้ทราบว่าหน่วยรับตรวจได้มีการดำเนินการสอดคล้องตามที่กฎหมายหรือระเบียบข้อบังคับกำหนด

ทั้งนี้ การระบุคุณสมบัติของผู้ตรวจสอบควรมีความรู้ความเข้าใจเกี่ยวกับการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ และผ่านการอบรมหัวข้อการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ หรือหัวข้อผู้นำการตรวจสอบตาม ISO/IEC 27001 หรือหัวข้อผู้นำการตรวจสอบตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 หรือหัวข้อการอบรมในลักษณะเดียวกัน หรืออาจมีใบรับรองตามมาตรฐานสากลที่เกี่ยวข้อง เช่น Certified Information Systems Security Professional (CISSP), Certified Information

Systems Auditor (CISA), IRCA ISO/IEC 27001 Lead Auditor, Certified Information Security Manager (CISM), CompTIA Security+, SANS/GIAC Certification (Various)

ปัจจุบัน สกมช. มีแผนงานโครงการสนับสนุนด้านการพัฒนาบุคลากรให้กับหน่วยงานที่เกี่ยวข้อง เช่น NCSA Cyber Clinic, การอบรมหลักสูตร Lead Auditor/Lead Implementor, Thailand National Cyber Academy, National Cyber Exercise เป็นต้น ซึ่งหน่วยงานควรเข้าไปติดตามและศึกษาเพิ่มเติมต่อไป

คำถามที่ 8 การปฏิบัติตามมาตรา 53 หน่วยงานควบคุมหรือกำกับดูแลที่ไม่มีความพร้อมสามารถว่าจ้างหน่วยงานอื่นให้มาตรวจสอบแทนได้หรือไม่ ซึ่งอาจจะขัดต่อหลักการตามมาตรา 53 ที่กำหนดให้หน่วยงานควบคุมหรือกำกับดูแลตรวจมาตรฐานขั้นต่ำหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้กำกับ และอาจจะส่งผลให้การตรวจสอบไม่ได้มาตรฐานหรือไม่ อย่างไร

ข้อชี้แจง ตามมาตรา 53 หรือแนวทางปฏิบัติและกรอบมาตรฐานฯ ไม่ได้ห้ามให้หน่วยงานควบคุมหรือกำกับดูแลจ้างหน่วยงานอื่นมาตรวจสอบแทนตน ดังนั้นหน่วยงานควบคุมหรือกำกับดูแลสามารถดำเนินการได้ อย่างไร ก็ตาม แม้มีการมอบหมายให้หน่วยงานอื่นดำเนินการตรวจสอบแทน แต่ความรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ยังคงตกอยู่กับหน่วยงานควบคุมหรือกำกับดูแล

คำถามที่ 9 ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 53 และ มาตรา 54 คำว่า "ตรวจสอบ" มีความแตกต่างกันหรือไม่ อย่างไร

ข้อชี้แจง คำว่า "ตรวจสอบ" ในมาตรา 53 และมาตรา 54 มีความหมายเดียวกัน คือ การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit) ซึ่งเป็นส่วนหนึ่งของการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ให้มีการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) ที่มีประสิทธิภาพ

อย่างไรก็ตาม การตรวจสอบตามมาตรา 53 เป็นการกำหนดให้หน่วยงานควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตน ซึ่งมีวัตถุประสงค์เพื่อให้หน่วยงานควบคุมหรือกำกับดูแลเกิดความเชื่อมั่นว่าหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตนจะได้ปฏิบัติตามข้อกำหนดหรือแนวทางที่หน่วยงานควบคุมหรือกำกับดูแลนั้นได้วางไว้

ในขณะที่การตรวจสอบตามมาตรา 54 เป็นการกำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคง

ปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบภายนอก ซึ่งมีวัตถุประสงค์เพื่อให้ผู้บริหารสูงสุดของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นเกิดความเชื่อมั่นว่าผู้ปฏิบัติงานในหน่วยงานของตนจะได้ปฏิบัติตามข้อกำหนดหรือแนวทางที่ผู้บริหารสูงสุดนั้นๆ ได้วางไว้

คำถามที่ 10 ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 54 ประโยคที่ว่า "ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบภายนอก" นั้น หากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้รับการตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์โดยหน่วยงานควบคุมหรือกำกับดูแล ตามมาตรา 53 แล้วนั้น จะถือว่าหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดังกล่าวผ่านการ "ตรวจสอบ" ตามมาตรา 54 ด้วยหรือไม่

ข้อชี้แจง ตามมาตรา 54 วรรคหนึ่ง กำหนดให้ "หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง" กรณีนี้ กฎหมายกำหนดให้เป็นหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ต้องดำเนินการ ดังนี้

- ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน
- ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ไม่ว่าจะเป็นผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอกก็ได้

ส่วนการตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับดูแลของหน่วยงานควบคุมหรือกำกับดูแล ตามมาตรา 53 กฎหมายกำหนดให้เป็นหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล ที่ต้องดำเนินการตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตนว่าจัดทำ ได้มาตรฐานหรือไม่ ดังนั้น การผ่านการตรวจสอบตามมาตรา 53 จึงไม่ถือว่าหน่วยงาน CII ได้ผ่านการ "ตรวจสอบ" ตามมาตรา 54 ไปด้วย ประเด็นดังกล่าวยกตัวอย่างเทียบเคียงกรณีที่หน่วยงานของรัฐจะต้องจัดให้มีการตรวจสอบด้านการเงิน บัญชี และพัสดุ โดยผู้ตรวจสอบภายในของหน่วยงานของรัฐนั้น ในขณะเดียวกันก็ต้องได้รับการตรวจสอบด้านการเงิน บัญชี และพัสดุ จากผู้ตรวจสอบของสำนักงานการตรวจเงินแผ่นดิน ทั้งนี้ หน่วยงานของรัฐ จะอ้างว่าได้รับการตรวจสอบจากผู้ตรวจสอบของสำนักงานการตรวจเงินแผ่นดินแล้วโดยไม่จำเป็นต้องมีการตรวจสอบด้านการเงิน บัญชี และพัสดุ โดยผู้ตรวจสอบภายในไม่ได้

คำถามที่ 11 การติดต่อประสานงานกับ สกมช. เพื่อดำเนินการจัดทำรายงานและนำส่งรายงานตามมาตรา 54 ข้างต้น หน่วยงานจะสามารถดำเนินการได้อย่างไร

ข้อชี้แจง หน่วยงานสามารถติดต่อประสานงานการดำเนินการตามมาตรา 54 ได้ผ่านช่องทาง cii@ncsa.or.th ในขณะที่การจัดส่งผลสรุปรายงานต่อสำนักงาน สามารถดำเนินการได้ใน 2 ช่องทาง คือ

(1) ช่องทางอีเมลกลางงานสารบรรณ saraban@ncsa.or.th ด้วยวิธีการ PGP ทั้งนี้ สามารถดาวน์โหลดกุญแจสำหรับอีเมล saraban@ncsa.or.th ได้ที่ https://www.ncsa.or.th/contact-the-office.html

(2) ช่องทางสารบรรณกลาง สกมช. 120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

ทั้งนี้ หน่วยงานจะดำเนินการส่งผ่านช่องทางเดียว หรือสองช่องทาง ก็ได้ รวมทั้งขอให้มีการติดต่อสอบถามมายังสำนักงานฯ อีกครั้ง เนื่องจากช่องทางดังกล่าวข้างต้นอาจมีการเปลี่ยนแปลงในอนาคต

คำถามที่ 12 หน่วยงานของรัฐที่ไม่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จะต้องจัดส่งผลสรุปรายงานการประเมินความเสี่ยงฯ และการตรวจสอบฯ หรือไม่

ข้อชี้แจง หน่วยงานของรัฐที่ไม่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ต้องจัดส่งผลสรุปรายงานการประเมินความเสี่ยงฯ และการตรวจสอบฯ ตามมาตรา 54 แห่ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

คำถามที่ 13 ในการประเมินความเสี่ยงฯ และการตรวจสอบฯ ภายในหน่วยงานมีขั้นตอนการรายงานผู้บริหารหรือคณะกรรมการต่างๆ อยู่แล้ว (ซึ่งอาจจะไม่ใช่ "ผู้บริหารสูงสุด") ประเด็นนี้หน่วยงานสามารถใช้สายการรายงานปกติที่มีอยู่ได้เลยหรือไม่ หรือจำเป็นต้องนำเรื่องขึ้นรายงานผู้บริหารสูงสุดอีกครั้ง เพื่อจะนำส่ง สกมช.

ข้อชี้แจง หน่วยงานอาจพิจารณาใช้สายการรายงานปกติที่มีอยู่ได้ อย่างไรก็ตามผู้บริหารสูงสุดควรทราบผลการประเมินความเสี่ยงฯ เมื่อเปรียบเทียบกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และการตรวจสอบฯ เมื่อเปรียบเทียบกับนโยบายแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งทั้งสองส่วนดังกล่าวข้างต้นจะกำหนดโดยผู้บริหารสูงสุดของหน่วยงาน นอกจากนี้ ผู้บริหารสูงสุดยังคงเป็นผู้ที่จะต้องรับผิดชอบต่อความเสียหายที่อาจเกิดขึ้นต่อภัยคุกคามทางไซเบอร์ ตามรายงานการประเมินความเสี่ยงดังกล่าว

คำถามที่ 14 เนื่องจากในภาคธนาคาร สถาบันการเงินต้องส่งผลรายงานกรอบการประเมินความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilient Assessment Framework: CRAF) มายังหน่วยงานกำกับดูแลทุกปี เพื่อใช้ประเมินระดับความเสี่ยงตั้งต้นด้านไซเบอร์ (Cyber Inherent Risk Assessment) และกำหนดแนวทางการบริหารจัดการความเสี่ยงด้านไซเบอร์และมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่พึงมี (Maturity Level) ให้สอดคล้องกับระดับความเสี่ยงตั้งต้นของตนเอง โดย CRAF ได้อ้างอิงมาตรฐานมาจาก NIST Cybersecurity Framework และ ISO/IEC 27001 จึงขอหารือ สกมช. ว่าหากมีการตกลงร่วมกันระหว่าง CII และหน่วยงานกำกับดูแล จะขอใช้รายงาน CRAF ในการรายงานผลประเมินความเสี่ยงฯ ไปยัง สกมช. ได้หรือไม่

ข้อชี้แจง สามารถใช้ได้ แต่ต้องคำนึงถึงความถูกต้องครบถ้วนและสอดคล้องตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

คำถามที่ 15 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถส่งผลประเมิน ISO/IEC 27001 ซึ่งมีขอบเขตครอบคลุมบริการสำคัญ ในการรายงานผลการประเมินความเสี่ยงฯ และการตรวจสอบฯ ได้หรือไม่

ข้อชี้แจง หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถส่งผลประเมินความเสี่ยง (Risk Assessment) และผลการตรวจสอบ (Audit) ตามมาตรฐาน ISO/IEC 27001 ซึ่งมีขอบเขตครอบคลุมบริการสำคัญได้ แต่ต้องคำนึงถึงความถูกต้องครบถ้วนและสอดคล้องตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

คำถามที่ 16 จากหลักเกณฑ์ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564 เช่น หมวด 3 ด้านการเงินการธนาคาร ซึ่งมีภารกิจหรือให้บริการ (Critical Services) แยกออกเป็น 5 ประเภท นั้น ทางหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต่างๆ สามารถ Risk based คัดเลือกเฉพาะบางประเภทมาตรวจได้หรือไม่ หรือต้องตรวจทุกประเภทในแต่ละปี หรือสามารถกำหนดรอบในการวนตรวจให้ครบทุกประเภทได้หรือไม่

ข้อชี้แจง หน่วยงานสามารถตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา 54 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ตามข้อ 17.1 โดยต้องดำเนินการจัดทำแผนการตรวจ (Audit Plan) ให้สามารถตรวจสอบระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในลักษณะ Risk based ตามช่วงระยะเวลาที่เหมาะสม โดยอาจจัดทำเป็นแผนระยะเวลา 1 ปี (Annual Audit Plan) หรือแผนระยะเวลาเกินกว่า 1 ปี (Multi-year Audit Plan) ทั้งนี้ขึ้นอยู่กับขนาดและทรัพยากรของหน่วยงานด้วย

คำถามที่ 17 หากระบบที่มีนัยสำคัญมีจำนวนมาก หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถที่จะสุ่มเฉพาะบางระบบที่สำคัญมาตรวจก่อน หรือจำเป็นต้องตรวจทุกระบบภายในแต่ละปี หรือสามารถกำหนดรอบในการวนตรวจให้ครบทุกระบบได้หรือไม่

ข้อชี้แจง หน่วยงานสามารถดำเนินการได้ แต่ต้องคำนึงถึงความถูกต้องครบถ้วนและสอดคล้องตามข้อ 17.1 ของประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

คำถามที่ 18 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ระบุให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถจัดส่งรายงานการประเมินความเสี่ยง ซึ่งมีรายละเอียดครบถ้วนเฉพาะข้อ 18.1 โดยไม่รวมรายละเอียดในข้อ 18.2 - 18.4 ดังนั้นหากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งรายงานเฉพาะข้อ 18.1 จะเพียงพอหรือไม่ อย่างไร

ข้อชี้แจง ตามมาตรา 54 กำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ โดยในส่วนของการประเมินความเสี่ยงฯ จะปรากฏในข้อ 18.1 ซึ่งเป็นส่วนที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะต้องจัดทำผลสรุปรายงานส่งให้ สกมช. ทั้งนี้ ผลสรุปรายงานการประเมินความเสี่ยงตามมาตรา 54 มีเนื้อหาครอบคลุมเฉพาะข้อ 18.1 เท่านั้น โดยในส่วนที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จะต้องดำเนินการในข้อ 18.2 - 18.4 นั้นไม่ต้องรวมอยู่ในผลสรุปรายงานตามมาตรา 54

คำถามที่ 19 การนำส่งรายงานการประเมินความเสี่ยงและการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องมีการรายงานผู้บริหารระดับสูงสุดของหน่วยงานเพื่อรับทราบรายงานการประเมินความเสี่ยงและการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ของส่วนงาน

เป็นลายลักษณ์อักษร ผู้บริหารสูงสุดในที่นี้สามารถให้ผู้รับมอบอำนาจลงนามรับทราบได้หรือไม่ หรือต้องเป็นผู้บริหารสูงสุด โดยตรงเท่านั้น

ข้อชี้แจง ผู้มีอำนาจลงนามรับทราบรายงานฯ สามารถเป็นผู้บริหารสูงสุด หรือผู้บริหารที่ได้รับมอบหมายของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ ขอให้แสดงหลักฐานยืนยันว่าเป็นผู้มีอำนาจลงนามดังกล่าว เช่น คำสั่งแต่งตั้งที่แสดงถึงหน้าที่หรือความรับผิดชอบในเรื่องดังกล่าว เป็นต้น

คำถามที่ 20 การนำส่งรายงานการประเมินความเสี่ยงฯ และการตรวจสอบฯ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถแยกส่งทีละฉบับได้หรือไม่ เนื่องจากอาจแล้วเสร็จไม่พร้อมกัน

ข้อชี้แจง สามารถแยกฉบับส่งได้ ทั้งนี้จะต้องจัดส่งผลสรุปรายงานการดำเนินการดังกล่าวต่อ สกมช. ภายใน 30 วัน นับแต่วันที่ดำเนินการแล้วเสร็จ ทั้งนี้ ไม่เกินวันที่ 30 มกราคม ของปีถัดไป

คำถามที่ 21 การจัดส่งผลสรุปรายงานการดำเนินการตามมาตรา 54 นั้น ถ้าหากหน่วยงานยังอยู่ระหว่างการดำเนินการตามมาตราดังกล่าว ซึ่งอาจจะยังไม่ครบถ้วนและแล้วเสร็จทันภายใน 30 มกราคม ของปีถัดไป จะถือว่าดำเนินการไม่ครบตามกฎหมายหรือไม่ อย่างไร

ข้อชี้แจง ตามมาตรา 54 แห่ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ความว่า หน่วยงานโครงสร้างพื้นฐานสาคัญทางสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง และให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ และกำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะต้องจัดส่งผลสรุปดังกล่าวภายใน 30 มกราคม ของปีถัดไป

ดังนั้น ในประเด็นที่สอบถามว่า ถ้าหากหน่วยงานยังอยู่ระหว่างการดำเนินการตามมาตราดังกล่าว ซึ่งอาจจะยังไม่ครบถ้วนและแล้วเสร็จทันภายใน 30 มกราคม ของปีถัดไป จะถือว่าดำเนินการไม่ครบตามกฎหมายหรือไม่ นั้น ถือว่าเป็นการดำเนินการที่ไม่สอดคล้องตามมาตรา 54 แห่ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ทั้งนี้ หน่วยงานควรมีหนังสือแจ้ง สกมช. ก่อนถึงวันครบกำหนด (30 มกราคม ของปีถัดไป) ว่ายังอยู่ระหว่างการดำเนินการ พร้อมระบุเหตุผลและความจำเป็นที่ไม่สามารถดำเนินการได้ทัน ซึ่งจะเป็นการแสดงถึงเจตนารมณ์ของหน่วยงานที่พยายามดำเนินการให้แล้วเสร็จ โดย สกมช. จะใช้หนังสือฉบับนี้ในการรายงานต่อคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) เพื่อพิจารณาต่อไป

คำถามที่ 22 เมื่อหน่วยงานจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เสร็จแล้ว หน่วยงานต้องนำเสนอหัวหน้าส่วนราชการผ่าน DCIO เพื่อให้ความเห็นชอบและอนุมัติหรือไม่

ข้อชี้แจง ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570) ส่วนนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ข้อที่ 3.1 ต้องกำหนด และอนุมัตินโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จากภัยคุกคามทางไซเบอร์ โดยผู้ที่มีอำนาจในการอนุมัติควรเป็นผู้บริหารสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) ผ่านผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer: CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงาน

ดังนั้น หน่วยงานควรกำหนดให้ส่วนงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ยกร่างนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ผ่านผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงาน ไปยังผู้บริหารสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) เพื่อให้ความเห็นชอบและอนุมัติต่อไป

ทั้งนี้ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) ส่วนนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ข้อที่ 1.3 กำหนดว่า ผู้บริหารระดับสูงที่ทำหน้าที่ดังกล่าวควรเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT Operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT Development) และมีอำนาจหน้าที่ (Authority) เพียงพอในการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล ดังนั้น หน่วยงานจึงไม่ควรกำหนดให้ DCIO ทำหน้าที่เป็น CISO อีกตำแหน่งหนึ่ง เนื่องจากจะทำให้เกิดปัญหาความขัดกันของผลประโยชน์ (Conflict of Interest)

คำถามที่ 23 เมื่อหน่วยงานจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เสร็จแล้ว หน่วยงานต้องดำเนินการแจ้งเวียนให้หน่วยงานภายในองค์กรทราบหรือไม่ เนื่องจาก พ.ร.บ. และประกาศที่เกี่ยวข้องมิได้กำหนดการดังกล่าว

ข้อชี้แจง หน่วยงานต้องแจ้งเวียนประมวลแนวทางปฏิบัติฯ ดังกล่าวให้หน่วยงานภายในองค์กรทราบ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) ส่วนนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ข้อที่ 3. นโยบายและแนวปฏิบัติ (Policies and Guidelines) ข้อย่อย 3.1 (ข) เนื่องจากจะทำให้บุคลากรในหน่วยงานรับทราบและปฏิบัติตามประมวลแนวทางปฏิบัติฯ ดังกล่าวได้อย่างถูกต้องต่อไป

คำถามที่ 24 เมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องแจ้งหน่วยงานควบคุมหรือกำกับดูแล และ สกมช. ภายในกี่ชั่วโมง

ข้อชี้แจง เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานต่อ สกมช. และหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามประกาศคณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคาม ทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 อย่างไรก็ดี หน่วยงานสามารถหารือร่วมกับหน่วยงานควบคุมหรือกำกับดูแลเพื่อให้มีแนวทางการดำเนินมาตรการที่เหมาะสม และสอดคล้องกับลักษณะการดำเนินภารกิจการให้บริการหรือทรัพยากรที่มีอยู่ภายใต้ความรับผิดชอบของหน่วยงาน โดยดูตัวอย่างเรื่องระยะเวลาการแจ้งหรือรายงานได้ตามข้อ 3 ภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

คำถามที่ 25 กรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สกมช. มีแบบฟอร์มในการแจ้งเหตุหรือไม่

ข้อชี้แจง สามารถศึกษาแบบรายงานภัยคุกคามทางไซเบอร์ได้จากประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566

คำถามที่ 26 กรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแลต้องแจ้ง สกมช. ด้วยอีกหรือไม่ เมื่อได้รับการแจ้งเหตุจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ข้อชี้แจง เมื่อได้รับการแจ้งเหตุภัยคุกคามทางไซเบอร์จากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ไม่ได้กำหนดให้หน่วยงานควบคุมหรือกำกับดูแลต้องแจ้งเหตุภัยคุกคามทางไซเบอร์นั้นมายัง สกมช.

ส่วนที่ 2 นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

คำถามที่ 27 หน่วยงาน เป็นทั้งหน่วยงานของรัฐและหน่วยงาน CII ในส่วนของนโยบายและแผนฯ หน่วยงานจะต้องแต่งตั้งทั้ง CIO และ CISO หรือไม่

ข้อชี้แจง ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) ข้อที่ 1 การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity) ข้อ 1.2 กำหนดให้หน่วยงานของรัฐต้องจัดให้มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือเทียบเท่าที่ปฏิบัติหน้าที่ของหน่วยงาน ข้อ 1.3 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงาน นั้น

มีวัตถุประสงค์เพื่อให้หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีผู้บริหารระดับสูงทำหน้าที่บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงาน ดังนั้น การที่หน่วยงานซึ่งมีฐานะเป็นทั้งหน่วยงานของรัฐและหน่วยงาน CII จึงมีความจำเป็นที่จะต้องแต่งตั้งผู้บริหารระดับสูงให้ทำหน้าที่ดังกล่าว ทั้งนี้ เนื่องจากหน่วยงานมีโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งมีความสำคัญยิ่งต่อประเทศ ประกอบกับการทำหน้าที่ของผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) มีความครอบคลุมงานของผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) ดังนั้น หน่วยงานจึงสามารถแต่งตั้ง CISO เพื่อทำหน้าที่ในการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในส่วนของระบบที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบที่มิใช่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยไม่มีความจำเป็นที่จะต้องแต่งตั้งผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) อีกตำแหน่งหนึ่ง

ในประเด็นที่สอบถามว่าหน่วยงานจะต้องแต่งตั้งผู้ทำหน้าที่ CIO หรือไม่นั้น เนื่องจากมีมติ ครม. ที่เกี่ยวข้องกับการปฏิบัติงานของหน่วยงานของรัฐอยู่แล้ว ซึ่งไม่อยู่ในขอบเขตของอำนาจหน้าที่ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จึงขอให้หน่วยงานศึกษาแนวทางการแต่งตั้งผู้ทำหน้าที่ CIO จากหน่วยงานที่เกี่ยวข้องต่อไป

คำถามที่ 28 ตามนโยบายบริหารจัดการฯ ระบุบทบาทหน้าที่ของ CIO และ CISO นั้น ไม่เหมือนกัน หากกรณีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแต่งตั้งเฉพาะ CISO ตามบทบาทหน้าที่ในนโยบายบริหารจัดการฯ จะไม่ครอบคลุมบทบาทหน้าที่ที่ควรดำเนินการภายในหน่วยงาน แต่ถ้ากำหนดมากเกินไปก็จะไม่สอดคล้องตามที่ระบุไว้ในนโยบายบริหารจัดการฯ ขอทราบแนวทางว่าหน่วยงานควรกำหนด อย่างไร

ข้อชี้แจง การที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงาน มีวัตถุประสงค์เพื่อให้ทำหน้าที่บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เท่านั้น มิได้กำหนดให้ทำหน้าที่เป็น CIO อีกทั้งยังมีการกำหนดไว้อย่างชัดเจนว่าผู้บริหารระดับสูงที่ทำหน้าที่ดังกล่าวควรเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT Operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT Development) และมีอำนาจหน้าที่ (Authority) เพียงพอในการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล ซึ่งเป็นการเน้นย้ำว่ามีเจตนารมณ์ที่จะแยกผู้ทำหน้าที่ CISO ออกจากผู้ทำหน้าที่ CIO

คำถามที่ 29 การแต่งตั้งผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) เนื่องจาก นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ระบุว่าหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ต้องมีตำแหน่ง Chief Information Security Officer (CISO) เพื่อทำหน้าที่บริหารความเสี่ยงด้านความปลอดภัยทางไซเบอร์ ทั้งนี้ ทำหน้าที่เป็นอิสระจากงานด้านปฏิบัติงานเทคโนโลยีสารสนเทศ (IT Operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT Development) ดังนั้น หน่วยงานสามารถดำเนินการแต่งตั้ง ท่านรองผู้ว่าการเทคโนโลยีดิจิทัลและการสื่อสาร มาเป็น Chief Information Security Officer (CISO) ได้หรือไม่ อย่างไร

ข้อชี้แจง จากนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ข้อ 1.3 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information

Security Officer : CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงาน ทั้งนี้ ผู้บริหารระดับสูงที่ทำหน้าที่ดังกล่าวควรเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT Operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT Development) และมีอำนาจหน้าที่ (Authority) เพียงพอในการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล

จากคำถามที่ว่าหน่วยงานสามารถดำเนินการแต่งตั้ง ท่านรองผู้ว่าการเทคโนโลยีดิจิทัลและการสื่อสารมาเป็น Chief Information Security Officer (CISO) ได้หรือไม่นั้น สกมช. ขอชี้แจงว่าเป็นการดำเนินการที่ไม่สอดคล้องกับข้อกำหนดในข้อ 1.3 เนื่องจากรองผู้ว่าการเทคโนโลยีดิจิทัลและการสื่อสารมีหน้าที่รับผิดชอบโดยตรงเกี่ยวกับปฏิบัติงานเทคโนโลยีสารสนเทศ (IT Operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT Development) ดังนั้น การแต่งตั้งรองผู้ว่าการเทคโนโลยีดิจิทัลและการสื่อสารทำหน้าที่เป็น CISO ด้วยจึงไม่มีความเป็นอิสระจากการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT Operation) ทั้งนี้ หน่วยงานควรพิจารณาแต่งตั้งผู้บริหารระดับสูงท่านอื่นเพื่อทำหน้าที่ CISO เช่น รองผู้ว่าการท่านอื่น หรือผู้ช่วยผู้ว่าการ หรือผู้บริหารระดับสูงท่านอื่นตามที่ผู้ว่าการเห็นว่าเหมาะสม

คำถามที่ 30 การแต่งตั้งตำแหน่ง CISO มีคุณสมบัติขั้นพื้นฐานอย่างไรบ้าง

ข้อชี้แจง ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) ควรมีคุณสมบัติขั้นพื้นฐานซึ่งเพียงพอต่อการทำงานตามข้อ 1.3 (1) และ (2) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) ตัวอย่างเช่น

- ปริญญาตรีหรือสูงกว่าในสาขาที่เกี่ยวข้อง เช่น วิทยาการคอมพิวเตอร์ ความปลอดภัยของข้อมูล หรือการจัดการ เป็นต้น
- มีประสบการณ์ที่เกี่ยวข้องกับงานด้านการรักษาความปลอดภัยของข้อมูล รวมทั้งมีประสบการณ์ในบทบาทผู้บริหาร
- มีความรู้ที่เพียงพอเกี่ยวกับเทคโนโลยีด้านการรักษาความปลอดภัยของข้อมูล ด้านมาตรฐาน และแนวทางปฏิบัติที่ดีที่สุดที่เกี่ยวข้อง

- มีความสามารถในการจัดการความเสี่ยง การพัฒนาและดำเนินการตามนโยบายและขั้นตอนปฏิบัติด้านความปลอดภัยของข้อมูล และสื่อสารประเด็นด้านความปลอดภัยอย่างมีประสิทธิภาพแก่ผู้มีส่วนได้ส่วนเสียทั้งด้านเทคนิคและไม่ใช่ด้านเทคนิค
- ได้รับการรับรองความสามารถด้านการักษาความมั่นคงปลอดภัยสารสนเทศ เช่น Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) หรือ Certified in the Governance of Enterprise IT (CGEIT) เป็นต้น
- ได้รับการอบรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ เช่น หลักสูตร Executive CISO ที่จัดโดย สกมช. เป็นต้น

ส่วนที่ 3 ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

คำถามที่ 31 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อที่ 21.1.1 ต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อยดังนี้ (ข) ฟังก์ชันที่สำคัญของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โปรดช่วยขยายความเพิ่มเติมสำหรับ “ฟังก์ชั่นที่สำคัญของทรัพย์สิน” หมายถึงอะไร พร้อมช่วยยกตัวอย่างเพิ่มเติม

ข้อชี้แจง การกำหนดฟังก์ชั่นที่สำคัญของทรัพย์สิน ในข้อ 21.1.1 (ข) มีวัตถุประสงค์เพื่อให้ทราบว่าทรัพย์สินดังกล่าวนั้นนำไปใช้เพื่อวัตถุประสงค์ใด หรือเพื่อสนับสนุนส่วนใดของบริการที่สำคัญหรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งจะทำให้ทราบว่า หากทรัพย์สินดังกล่าวสูญเสียคุณสมบัติทางด้านการรักษาความลับ ความถูกต้องครบถ้วน หรือความพร้อมใช้งาน จะบางส่วนหรือทั้งหมดแล้ว จะทำให้บริการที่สำคัญซึ่งเกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีปัญหา ทั้งนี้ ท่านสามารถศึกษาข้อมูลเพิ่มเติมได้ที่ NIST Special Publication 800-128 หัวข้อ Create or Update System Component Inventory หน้าที่ 24-26

คำถามที่ 32 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อที่ 21.1.1 (ฉ) "การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศบนระบบ/เครือข่ายภายใน และ/หรือภายนอก" หมายความว่าอย่างไร

ข้อชี้แจง ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้าง

พื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ข้อที่ 21 หัวข้อหลักที่ 1 การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify) ข้อย้อย 21.1 การจัดการทรัพย์สิน (Asset Management) 21.1.1 (ฉ) การขึ้นต่อกันของทรัพย์สิน ของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศบนระบบ/เครือข่ายภายใน และ/หรือภายนอก นั้น การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศบนระบบ/เครือข่ายภายใน และ/หรือภายนอก หมายถึงการที่ทรัพย์สินใดๆ ซึ่งสนับสนุนส่วนหนึ่งของระบบ (single system component) และมีการไปสนับสนุนส่วนอื่นของระบบ (additional information systems) ยกตัวอย่างเช่น การให้บริการระบบฐานข้อมูลขององค์กรโดยทั่วไปจะประกอบด้วย เครื่องแม่ข่าย ซอฟต์แวร์บริหารฐานข้อมูล (Database Management System) สื่อบันทึกข้อมูล และระบบเครือข่าย ซึ่งมีการทำงานร่วมกันเพื่อให้บริการตามวัตถุประสงค์ของหน่วยงาน หากส่วนหนึ่งส่วนใดของระบบดังกล่าวข้างต้นมีปัญหาย่อมส่งผลให้บริการมีปัญหาตามไปด้วย ดังนั้น อาจกล่าวได้ว่าเครื่องแม่ข่าย ซอฟต์แวร์บริหารฐานข้อมูล (Database Management System) สื่อบันทึกข้อมูล และระบบเครือข่าย มีการขึ้นต่อกัน เป็นต้น ทั้งนี้ ท่านสามารถศึกษาข้อมูลเพิ่มเติมเกี่ยวกับการขึ้นต่อกันของทรัพย์สินได้ที่ NIST Special Publication 800-128 หัวข้อ Create or Update System Component Inventory หน้าที่ 24-26 รวมทั้งแนวทางการวิเคราะห์ความขึ้นต่อกันของกระบวนการได้ที่ NISTIR 8179 Criticality Analysis Process Mode หัวข้อ B.2 – Design, Document, or Obtain High-level Processes and Identify Interactions, Intersections, Connections, and Dependencies Between Processes

คำถามที่ 33 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อที่ 21.1.2 ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface) หมายถึงอะไร พร้อมช่วยยกตัวอย่างเพิ่มเติม

ข้อชี้แจง การระบุขอบเขตเครือข่ายของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายถึง การระบุทรัพย์สินสารสนเทศที่เกี่ยวข้องกับบริการที่สำคัญ หน่วยงานสามารถระบุขอบเขตโดยพิจารณาเฉพาะส่วนที่รับผิดชอบโดยหน่วยงานของตน และมีการเชื่อมต่อเข้ากับเครือข่ายของหน่วยงาน ยกตัวอย่างเช่น การเขียนหรือระบุ Network Diagram ที่ครอบคลุมทั้งเครื่องแม่ข่าย อุปกรณ์เครือข่าย ช่องทางการสื่อสาร ระบบฐานข้อมูล ระบบศูนย์ข้อมูล ระบบรักษาความปลอดภัย ระบบพิสูจน์และยืนยันตัวตน ระบบสภาพแวดล้อม ระบบ SCADA และระบบส่วนต่างๆ ที่เกี่ยวข้อง เป็นต้น

คำถามที่ 34 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อที่ 21.1.2 ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface) ขอบเขตเครือข่ายของบริการที่สำคัญสามารถใช้การจัดทำ Network Diagram ทดแทนได้หรือไม่ หรือโปรดยกตัวอย่างการระบุขอบเขตเครือข่ายที่ สกมช. คาดหวังเพื่อเป็นแนวทางให้ Auditor ใช้ในการตรวจประเมินหน่วยงานต่อไป

ข้อชี้แจง การระบุขอบเขตตามข้อ 21.1.2 มีวัตถุประสงค์เพื่อให้หน่วยงานสามารถทราบถึงขอบเขตในการกำหนดมาตรการควบคุม (Security Controls) ได้อย่างถูกต้องและครอบคลุม ดังนั้นหน่วยงานสามารถใช้ Network Diagram เป็นเครื่องมือในการกำหนดขอบเขตเครือข่ายของบริการที่สำคัญได้ อย่างไรก็ตาม หน่วยงานอาจจะพิจารณาสิ่งอื่นที่ไม่ได้อยู่ใน Diagram ด้วย เช่น ระบบไฟฟ้าสำรอง ระบบ HVAC เป็นต้น โดยที่ Auditor จะต้องเข้าไปตรวจสอบการดำเนินการตามมาตรการควบคุมที่ได้กำหนดไว้ในนโยบายและแนวปฏิบัติของหน่วยงาน ซึ่งจะต้องครอบคลุมตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ที่ได้ประกาศไปแล้วด้วย

คำถามที่ 35 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อที่ 21.1.4 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ สกมช. คาดหวังต้องดำเนินการอย่างไร โปรดยกตัวอย่างอ้างอิง

ข้อชี้แจง หน่วยงานดำเนินการประเมินความเสี่ยงฯ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อ 18.1 ซึ่งสามารถใช้แนวทางในการประเมินความเสี่ยงฯ ตามมาตรฐานสากล เช่น NIST Special Publication 800-30 Rev.1, Guide for Conducting Risk Assessments, ISO/IEC 27001, COBIT, CIS CSC, ISA/IEC 62443 เป็นต้น ทั้งนี้ สำหรับการจัดส่งผลสรุปการประเมินความเสี่ยงฯ หน่วยงานอาจดำเนินการร่วมกับหน่วยงานควบคุมหรือกำกับดูแลของตนเพื่อจัดทำแบบฟอร์มรายงาน หรืออาจจัดทำแบบฟอร์มรายงานตาม Appendix K ของ NIST SP 800-30 Rev.1

คำถามที่ 36 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อที่ 21.1.4 การประเมินความเสี่ยงฯ ตามทะเบียนทรัพย์ (Asset inventory) หากในทะเบียนทรัพย์สินมีอุปกรณ์เป็นจำนวนมาก หน่วยงานจำเป็นต้องประเมินให้ครบทุกรายการ หรือสามารถสุ่มเลือกประเมินบางรายการได้หรือไม่

ข้อชี้แจง ไม่สามารถสุ่มเลือกประเมินได้ จะต้องประเมินความเสี่ยงทุกรายการที่ระบุไว้ในทะเบียนทรัพย์ในข้อ 21.1.1 ทั้งนี้ หน่วยงานฯ สามารถพิจารณารูปแบบการประเมินความเสี่ยงเพื่อลดภาระในการปฏิบัติงานได้ โดยหากรูปแบบการประเมินความเสี่ยงเป็นแบบ Asset Base สามารถจัดกลุ่มของ Asset ที่มีลักษณะคล้ายกัน เช่น อุปกรณ์รุ่นใกล้เคียงกัน ใช้ระบบปฏิบัติการรุ่นใกล้เคียงกัน หรือมีคุณลักษณะใกล้กัน เป็นต้น แล้วประเมิน

ความเสี่ยงกลุ่มอุปกรณ์ดังกล่าวให้ครบทุกกลุ่ม หรือ กรณี Scenario Base ก็สามารถประเมินโดยพิจารณาว่ามีทรัพย์สินใดที่เกี่ยวข้องกับ Scenario ได้เช่นกัน

คำถามที่ 37 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อที่ 21.3.2 (ค) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review) หมายถึงอะไร พร้อมช่วยยกตัวอย่างเพิ่มเติม

ข้อชี้แจง การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review) หมายถึง การประเมินความปลอดภัยแบบองค์รวม ทั้งในส่วนของบุคลากร กระบวนการ สถาปัตยกรรม แอพพลิเคชัน เพื่อระบุความเสี่ยงและแนวทางการลดผลกระทบของภัยคุกคามที่อาจจะเกิดขึ้น ยกตัวอย่างเช่น การตรวจสอบว่ามีจุดไหนของสถาปัตยกรรมเครือข่ายที่มีลักษณะเป็น Single Point of Failure หรือการตรวจสอบว่ามีเครื่องแม่ข่ายหรือบริการซึ่งมิได้มีการใช้งานแต่ยังคงปรากฏในสถาปัตยกรรมเครือข่าย เป็นต้น

คำถามที่ 38 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อที่ 21.3.5 ขอบเขตในการทดสอบเจาะระบบต้องมีการทดสอบในระดับใดบ้าง รวมถึง การทดสอบเจาะระบบนั้นต้องเป็นการทำแบบใด เช่น Black box หรือ Grey box

ข้อชี้แจง ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ไม่ได้กำหนดรูปแบบการทดสอบเจาะระบบ หน่วยงานสามารถพิจารณารูปแบบทดสอบเจาะระบบตามความเหมาะสม เพื่อให้เหมาะสมกับความเสี่ยงและบริบทของหน่วยงาน เช่น ทดสอบเจาะระบบแบบ Back box เนื่องจากพิจารณาแล้วว่าความเสี่ยงไซเบอร์ส่วนใหญ่จากภายนอก หรือทดสอบแบบ Grey box เนื่องจากอาจมีความเสี่ยงจากภายใน เป็นต้น อย่างไรก็ตามจะต้องครอบคลุมการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญของหน่วยงานฯ โดยเฉพาะอย่างยิ่ง ทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

คำถามที่ 39 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อที่ 21.3.6 การทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้ง (ตามความจำเป็น) คำว่า “ตามความจำเป็น” หมายถึงอะไร

ข้อชี้แจง ตามความจำเป็น พิจารณาจากความเสี่ยงและความคุ้มค่า หากเป็นระบบที่มีความเสี่ยงสูง เช่น ระบบที่มีผลกระทบต่อบริการที่สำคัญของหน่วยงานฯ และสามารถเข้าถึงได้จาก Internet เป็นต้น ควรพิจารณาทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้ง แต่หากระบบที่มีความเสี่ยงต่ำหรืออาจไม่คุ้มค่าเมื่อเทียบกับค่าใช้จ่ายในการทดสอบเจาะระบบ สามารถพิจารณากำหนดรอบการทดสอบเจาะระบบนานขึ้นได้ตามความเหมาะสม

คำถามที่ 40 อ้างอิงประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ซึ่งหน่วยงานได้ดำเนินการตรวจสอบการปฏิบัติตามประมวล ฯ ของธนาคารและนำส่งสรุปผลการตรวจสอบให้สำนักงานฯ ไปตามกำหนดที่ผ่านมาแล้วนั้น

ปัจจุบันธนาคารอยู่ระหว่างดำเนินการปรับปรุงการปฏิบัติตามประมวลฯ ข้อที่ 21.4 การจัดการผู้ให้บริการภายนอก (Third Party Management) เพื่อให้สอดคล้องตามที่สำนักงานกำหนด ทั้งนี้เพื่อให้เกิดความถูกต้อง หน่วยงานจึงเรียนขอคำชี้แนะหรือข้อแนะนำเพิ่มเติมตามรายละเอียดดังต่อไปนี้

อ้างอิงประมวลและกรอบฯ ข้อที่ 21.4.2 ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามความต้องการทางธุรกิจขององค์กร และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โปรดช่วยชี้แนะรายละเอียดที่ควรระบุในสัญญาตามที่สำนักงานคาดหวัง

ข้อชี้แจง หน่วยงานควรสามารถระบุรายการและประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญได้ จากนั้นเพื่อให้หน่วยงานสามารถบริหารความเสี่ยงของผู้ให้บริการภายนอกได้อย่างมีประสิทธิภาพ จึงจำเป็นที่จะต้องจัดทำโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละผู้ให้บริการภายนอก ซึ่งจะนำไปสู่การจัดทำแผนบริหารความเสี่ยงผู้ให้บริการภายนอกได้ต่อไป ทั้งนี้หน่วยงานสามารถศึกษารายละเอียดเพิ่มเติมได้ที่ NIST SP 800-161r1 หัวข้อ 3.4. C-SCRM Key Practices หน้าที่ 46

(ข) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจากภัยคุกคามทางไซเบอร์ โปรดช่วยชี้แนะรายละเอียดที่ควรระบุในสัญญาตามที่สำนักงานคาดหวัง

ข้อชี้แจง ในการดำเนินการบริหารความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์เป็นหน้าที่ของทั้งหน่วยงานและหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจากภัยคุกคามทางไซเบอร์ ทั้งนี้ในส่วนของภาระหน้าที่ของผู้ให้บริการภายนอกมีด้วยกันหลายประการ ยกตัวอย่างเช่น

- รักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมาย มาตรฐาน ร่วมถึงนโยบายและแนวปฏิบัติของผู้ให้บริการภายนอก
- ศึกษาและทำความเข้าใจเกี่ยวกับความเสี่ยงด้านไซเบอร์ โดยเฉพาะความเสี่ยงที่มีต่ออุตสาหกรรมของตน
- แลกเปลี่ยนข่าวกรองทางไซเบอร์กับหน่วยงานที่อยู่ในอุตสาหกรรมของตนเพื่อให้ทราบถึงแนวโน้มภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อการให้บริการภายนอก

ทั้งนี้หน่วยงานสามารถศึกษารายละเอียดเพิ่มเติมได้ที่ NIST SP 800-161r1 หัวข้อ 3.4. C-SCRM Key Practices หน้าที่ 46

(ค) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์ โปรดช่วยชี้แนะรายละเอียดที่ควรระบุในสัญญาตามที่สำนักงานคาดหวัง

ข้อชี้แจง การระบุความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์จะทำให้หน่วยงานสามารถวางแผนบริหารความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์ได้อย่างถูกต้อง ทั้งนี้ หน่วยงานอาจพิจารณาแยกแผนบริหารความเสี่ยงฉบับนี้ออกจากแผนบริหารความเสี่ยงด้านไซเบอร์ของหน่วยงาน หรือพิจารณารวมเข้าด้วยกันก็ได้ ยกตัวอย่างเช่น

- ความเสี่ยงจากผู้ปฏิบัติงานภายในหน่วยงาน (Insiders) ทำงานให้กับหน่วยงานอื่นซึ่งอาจส่งผลเสียต่อองค์กร
- ความเสี่ยงจากบุคคลหรือกลุ่มบุคคลที่เป็นภัยคุกคามซึ่งแฝงตัวมากับบริษัทซึ่งพัฒนาผลิตภัณฑ์ให้กับหน่วยงาน

ทั้งนี้หน่วยงานสามารถศึกษารายละเอียดเพิ่มเติมได้ที่ NIST SP 800-161r1 หัวข้อ 2.2. Cybersecurity Risks Throughout Supply Chains หน้าที่ 20

(ง) สิทธิ์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก โปรดช่วยชี้แนะรายละเอียดที่ควรระบุในสัญญาตามที่สำนักงานคาดหวัง

ข้อชี้แจง การกำหนดสิทธิ์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก สามารถดำเนินการได้โดยการพูดคุยกับผู้ให้บริการ

ภายนอกตั้งแต่ในขั้นตอนเริ่มต้นการจัดซื้อจัดจ้าง หรืออาจดำเนินการทบทวนการกำหนดสิทธิ์ดังกล่าวภายหลังการบริหารสัญญาก็ได้ ทั้งนี้หน่วนงานควรระบุสิทธิ์ในการดำเนินการ ดังนี้

- สิทธิ์ในการกำหนดผู้รับผิดชอบของหน่วยงานในการติดตามการดำเนินงานของผู้ให้บริการภายนอก
- สิทธิ์ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก (หากสามารถกระทำได้)
- สิทธิ์ในการรับทราบหรือได้รับรายงานการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Report) (หากสามารถกระทำได้)

ทั้งนี้หน่วยงานสามารถศึกษารายละเอียดเพิ่มเติมได้ที่ NIST SP 800-161r1 หัวข้อ FAMILY: AUDIT AND ACCOUNTABILITY หน้าที่ 80 และหัวข้อ FAMILY: ASSESSMENT, AUTHORIZATION, AND MONITORING หน้าที่ 84

คำถามที่ 41 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อที่ 21.4.3 สกมช. คาดหวังให้หน่วยงาน 1st LOD (IT Staff), หน่วยงาน 2nd LOD (Compliance, Risk) หรือหน่วยงาน 3rd LOD (Auditor) เป็นผู้สร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกฯ อย่างไร

ข้อชี้แจง หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถพิจารณากำหนดกระบวนการตรวจสอบให้หน่วยงานทำหน้าที่ดังกล่าวตามความเหมาะสม โดยคำนึงถึงข้อตกลงระดับการให้บริการ (Service Level Agreement) ทั้งนี้ ผู้ทำหน้าที่ดังกล่าวควรมีทักษะความรู้เพียงพอในการตรวจสอบความถูกต้อง มีอิสระเพียงพอในการดำเนินการ และมีการสอบทานดำเนินการดังกล่าว เช่น หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอาจจัดตั้งทีมตรวจสอบซึ่งประกอบด้วยบุคลากรของหน่วยงานจาก 1st LOD (IT Staff), หน่วยงาน 2nd LOD (Compliance, Risk) หรือหน่วยงาน 3rd LOD (Auditor) เพื่อเข้าตรวจสอบผู้ให้บริการภายนอก (หากเป็นไปได้) หรือกำหนดไว้ในข้อตกลงระดับการให้บริการว่าผู้ให้บริการจะต้องได้รับการตรวจสอบโดยบุคคลที่สาม (Third Party) เป็นต้น

คำถามที่ 42 นิยามของคำว่าทรัพย์สิน (Asset) จะต้องนิยามเป็นบริการ (Services) หรือเป็นระบบ (Systems) หรือรายอุปกรณ์ (Components)

ข้อชี้แจง ทรัพย์สิน (Asset) ในบริบทด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หมายถึง ทรัพย์สินทางสารสนเทศ (Information Assets) ซึ่งเป็นสิ่งที่มีมูลค่าด้านสารสนเทศและอาจสร้างผลกระทบต่อวัตถุประสงค์ขององค์กร โดยหน่วยงานฯ จะต้องจัดให้มีการประเมินความเสี่ยงฯ เพื่อหาแนวทางป้องกันให้เหมาะสมและมีความคุ้มค่า ทั้งนี้ ตามมาตรฐานสากล เช่น ISO/IEC 27002 ระบุ Assets ประกอบไปด้วย Primary asset

และ Supporting asset ยกตัวอย่างเช่น ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) ข้อมูล (Data) บุคลากรในองค์กร (Personnel) เป็นต้น

คำถามที่ 43 การประเมินความเสี่ยงรายอุปกรณ์ (component) หากความเสี่ยงรายอุปกรณ์ ถูกปกปิด หรือลดทอนด้วยอุปกรณ์อื่น เช่น Firewall จะถือว่าอุปกรณ์นั้นๆ ความเสี่ยงลดลงหรือไม่

ข้อชี้แจง ถือว่าความเสี่ยงลดลง โดยหากความเสี่ยงตั้งต้น (Inherent risk) ของอุปกรณ์นั้น ๆ ได้รับการจัดการหรือมีแนวทางการควบคุมความเสี่ยง (Controls) ซึ่งจะช่วยลดความเสี่ยงเหลือเพียงความเสี่ยงคงเหลือ (Residual risk) ของอุปกรณ์นั้นๆ แล้วเทียบกับเกณฑ์/กลยุทธ์ของหน่วยงานฯ ว่าอยู่ในระดับความเสี่ยงที่ยอมรับได้ (Risk appetite) หรือไม่

คำถามที่ 44 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อที่ 22.1.1 การเข้าถึงบริการที่สำคัญสามารถพิจารณาเพียงเฉพาะระดับ Application เพียงพอหรือไม่ หรือว่าจำเป็นต้องครอบคลุมทั้งระดับ Operating System, Database, และ Network ที่เกี่ยวข้องกับบริการที่สำคัญดังกล่าว

ข้อชี้แจง การจัดทำ Access Controls ที่ไม่ครอบคลุมทรัพย์สินสารสนเทศตามขอบเขตที่กำหนดไว้ในข้อ 21.1.2 อาจส่งผลให้ไม่สามารถลดความเสี่ยงได้ตามระดับที่กำหนด เช่น ผู้ไม่ประสงค์ดีอาจเข้าถึงบริการที่สำคัญโดยไม่ได้รับอนุญาตในระดับ Operating System, Database หรือ Network Physical เป็นต้น จนอาจส่งผลให้บริการสำคัญไม่สามารถดำเนินการได้อย่างต่อเนื่อง หรืออาจเกิดข้อมูลสำคัญรั่วไหล

คำถามที่ 45 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อที่ 22.3.2 (ง) Issuing system commands หมายถึงชุดคำสั่งผ่านโปรแกรมที่มีความสามารถในการสั่งงานทางไกล เช่น SNMP สำหรับระบบงานทั่วไปหรือไม่ หรือหมายถึงชุดคำสั่งที่ใช้สำหรับ OT Network เท่านั้น

ข้อชี้แจง Issuing System Commands หมายถึงชุดคำสั่งระดับ System ของระบบปฏิบัติการ ดังนั้น ข้อ 22.3.2 (ง) ไม่อนุญาตให้ใช้คำสั่งระบบ (Issuing System Commands) ผ่านการเชื่อมต่อระยะไกล ไม่ว่าจะเป็นอุปกรณ์ใดๆ เช่น Network Devices, Network Security Tools, Endpoints, Server เป็นต้น ซึ่งอาจจะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญของหน่วยงาน CII ยกเว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ

คำถามที่ 46 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อที่ 24.3.1 โปรดอธิบายความคาดหวังของ สกมช. ว่าต้องการให้หน่วยงานดำเนินการอย่างไร และโปรดช่วยชี้แนะว่า Auditor ของหน่วยงานควรดำเนินการตรวจสอบอย่างไร ในข้อดังกล่าว

ข้อชี้แจง ตามข้อ 24.3.1 ตามมาตรา 22 วรรคหนึ่ง (13) หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำโดยคณะกรรมการ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าวอาจดำเนินการได้ ทั้งในระดับชาติหรือระดับภาคส่วน หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว นั้น

ผู้บริหารระดับสูงของหน่วยงานต้องสนับสนุนพนักงานของตนเข้าร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise) ทั้งในระดับชาติหรือระดับภาคส่วน เมื่อได้รับการประสาน รวมถึงให้ความร่วมมือในการฝึก โดยบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์ มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าวเพื่อให้เข้าใจบทบาทหน้าที่ และมั่นใจได้ว่าเมื่อเกิดเหตุภัยคุกคามไซเบอร์หน่วยงานจะสามารถรับมือภัยคุกคามไซเบอร์ได้ตามที่แผนกำหนด

ทั้งนี้ Auditor ควรตรวจสอบว่าหน่วยงานได้มีการส่งบุคคลากรที่ระบุไว้ในแผนการรับมือภัยคุกคามไซเบอร์เข้าร่วม Cybersecurity Exercise ในระดับชาติหรือระดับภาคส่วน หรือไม่ รวมถึงตรวจสอบการนำผลการร่วมฝึกซ้อมฯ ของหน่วยงานตนเองมาปรับปรุงแก้ไขพัฒนาเครื่องมือ กระบวนการ และบุคลากรให้สามารถรับมือภัยคุกคามไซเบอร์มีประสิทธิภาพมากยิ่งขึ้น

คำถามที่ 47 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อที่ 24.3.2 โปรดอธิบายความคาดหวังของ สกมช. ว่าต้องการให้หน่วยงานดำเนินการอย่างไร และโปรดช่วยชี้แนะว่า Auditor ของหน่วยงานควรดำเนินการตรวจสอบอย่างไร ในข้อดังกล่าว

ข้อชี้แจง ตามข้อ 24.3.2 ต้องปฏิบัติตามคำขอใดๆ ของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤตที่กำหนดขึ้นตามข้อ 24.1 และข้อ 24.2 ขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญ ของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ นั้น

สกมช. คาดหวังให้หน่วยงานให้ข้อมูลเกี่ยวข้องกับบริการที่สำคัญ เมื่อคณะกรรมการฯ ร้องขอ เช่น ภัยคุกคามที่เคยเกิดขึ้น แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) เป็นต้น ซึ่งข้อมูลดังกล่าวข้างต้นจะนำไปใช้ในการวางแผนการจัดการฝึกซ้อมฯ ให้มีความสอดคล้องกับบริบทขององค์กร รวมถึงระดับความเสี่ยงจากภัยคุกคามทางไซเบอร์ ซึ่งจะส่งผลให้การฝึกซ้อมฯ ใกล้เคียงกับสถานการณ์จริงมากยิ่งขึ้น

ทั้งนี้ Auditor ควรตรวจสอบว่าหน่วยงานได้สนับสนุนการฝึกซ้อมฯ โดยให้ข้อมูล เช่น บริการที่สำคัญ แผนการรับมือภัยคุกคามทางไซเบอร์ แผนการสื่อสารในภาวะวิกฤต เป็นต้น เพื่อสนับสนุนการวางแผนและการจัดทำสถานการณ์ฝึก โดย สกมช. หรือไม่

คำถามที่ 48 ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ข้อที่ 25.1.1 ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

อ้างอิงตามประโยคที่ระบุว่า “รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น” ขอสอบถามเพิ่มเติมว่าหน่วยงานจำเป็นต้องสอบทานแผนของผู้ให้บริการภายนอกทุกรายหรือไม่ เช่น สำหรับผู้ให้บริการในลักษณะของ Maintenance service ที่ไม่มีระบบของหน่วยงานไปตั้งอยู่ จำเป็นต้องสอบทาน BCP ของผู้ให้บริการภายนอกรายดังกล่าวหรือไม่ หรือหน่วยงานสามารถพิจารณาจากเงื่อนไขสัญญาที่ระบุเรื่องของการตอบสนองต่อบริการ เช่น Service response time เป็นต้น ทดแทนได้

ข้อชี้แจง หน่วยงานไม่จำเป็นต้องสอบทานแผนของผู้ให้บริการภายนอกทุกราย โดยคำนึงถึงระดับความเสี่ยงจากผู้ให้บริการภายนอกที่จะมีผลกระทบต่อภารกิจหรือบริการที่สำคัญของหน่วยงาน ทั้งนี้ หากหน่วยงานมีเหตุผลความจำเป็นที่ไม่สามารถเข้าถึงแผนของผู้ให้บริการภายนอกได้ หน่วยงานสามารถพิจารณาจากเงื่อนไขสัญญาที่ระบุเรื่องของการตอบสนองต่อบริการ เช่น Service response time เป็นต้น ทดแทนได้

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ
80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

เว็บไซต์: https://www.ncsa.or.th
เฟซบุ๊ก: https://www.facebook.com/NCSA.Thailand
โทรศัพท์: 02 142 6888 (ติดต่อเวลาทำการ)
โทรสาร: 02 143 7593
อีเมล: แจ้งเหตุภัยคุกคามไซเบอร์ thaicert@ncsa.or.th
อีเมลกลางงานสารบรรณ: saraban@ncsa.or.th
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
National Computer Emergency Response Team (NCERT):
โทรศัพท์ 02-142-6885 (ติดต่อเวลาทำการ)
ศูนย์แจ้งเหตุภัยคุกคามทางไซเบอร์: โทรศัพท์ 02-114-3531 (24 ชั่วโมง)

สำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (สบพ.)
โทรศัพท์: 02 502 7826 (ติดต่อเวลาทำการ)
อีเมล: ให้คำปรึกษา cii@ncsa.or.th

NCSA Line Openchat
Code: 4loTus

แบบประเมินฯ
ข้อเสนอแนะเพิ่มเติม