บทที่ 4

ผลการวิจัย

ภาพรวมของนโยบายด้านความปลอดภัยข้อมูลสารสนเทศของธนาคารในปัจจุบัน

ธนาคารมีการจัดทำนโยบายด้านความปลอดภัยข้อมูลสารสนเทศโดยอิงจากมาตรฐาน ISO/IEC 17799:2005 ซึ่งมีเนื้อหาและข้อกำหนดต่างๆเหมือนกับมาตรฐาน ISO/IEC 27001:2005 ทุกประการ และมีการแบ่งระดับของนโยบายออกเป็น 2 ระดับ ได้แก่ ระดับนโยบาย (Policy) ซึ่งมีเนื้อหากว้างๆที่กล่าวถึงเจตจำนงค์ (Intention) ของผู้บริหารระดับสูงและวัตถุประสงค์ของนโยบาย และระดับมาตรฐานและระเบียบวิธีในการปฏิบัติงาน (Standard and Procedure) ซึ่งเป็นข้อกำหนดและแนวทางในการปฏิบัติงานที่ถูกต้องเหมาะสมตามวัตถุประสงค์ที่ได้ระบุไว้ในนโยบายนั้น และเนื่องจากระบบงานต่างๆของธนาคารก็จะมีมาตรฐานที่แตกต่างกันไป เช่น มาตรฐานในเรื่องของรหัสผ่านที่ใช้เข้าสู่ระบบ ดังนั้น มาตรฐานที่ธนาคารกำหนดไว้จะมีลักษณะเป็น Minimum Requirement หรือมาตรฐานกลางเพื่อให้แต่ละระบบนำไปปรับใช้ให้เหมาะสมกับระบบของตน

นอกจากนี้ ธนาคารยังมีกลไกหนึ่งที่ใช้เป็นช่องทางในการรับ Feedback จากผู้ใช้งานหลังจากที่ธนาคารได้มีการประกาศนโยบายออกไป กลไกดังกล่าวเรียกว่า Waiver ซึ่งธนาคารไม่ได้มองว่ากลไกนี้จะเป็นช่องทางให้ผู้ใช้งานหลีกเลี่ยงไม่ปฏิบัติตามนโยบาย แต่ธนาคารจะใช้ช่องทางนี้เป็นช่องทางในการปรับปรุงเปลี่ยนแปลงนโยบายให้มีความเหมาะสมกับลักษณะของการทำงานมากขึ้น เช่น ถ้าหากมีผู้ใช้งานในลักษณะเดียวกันทำเรื่องขอ Waiver เข้ามาเป็นจำนวนมาก ธนาคารก็จำเป็นจะต้องพิจารณาว่านโยบายที่ออกมานั้นขัดกับการทำงานในลักษณะดังกล่าวหรือไม่ เพื่อที่จะพิจารณายกเลิกหรือปรับปรุงนโยบายดังกล่าวให้มีความเหมาะสมมากขึ้น ทั้งนี้ ประเด็นสำคัญที่ธนาคารได้มีการคำนึงถึง ก็คือ หัวหน้างานจะต้องรับทราบถ้ามีกรณียกเว้น (Exception) ไม่ปฏิบัติตามนโยบายของธนาคารเกิดขึ้น

ธนาคารมองว่าการที่ธนาคารจะนำนโยบายด้านความปลอดภัยข้อมูลสารสนเทศออกมาใช้ให้ประสบผลสำเร็จนั้น นโยบายที่ออกมาจะต้องไม่ขัดขวาง (Block) การทำงานของ

พนักงาน แต่ต้องสามารถสนับสนุน (Serve) การทำงานของพนักงานได้ และการจะบังคับใช้นโยบายให้มีประสิทธิภาพนั้น นโยบายดังกล่าวจะต้องมีผลกับทุกคนในธนาคาร ไม่ว่าจะอยู่ในระดับใดก็ตาม เพื่อหลีกเลี่ยงการเกิดกรณียกเว้นในแบบที่อธิบายไม่ได้ ซึ่งในมาตรฐาน ISO/IEC 17799:2005 ก็ได้มีการกล่าวถึงเรื่องนี้ไว้เช่นกัน แต่การจะทำเรื่องดังกล่าวให้สำเร็จได้นั้นก็เป็นสิ่งที่ทำได้ยาก เพราะเรื่องนี้เป็นเรื่องของการผสมผสานระหว่างองค์กรที่มีวัฒนธรรมในการทำงานแบบหนึ่งเข้ากับวิธีการทำงานที่สร้างมาจากวัฒนธรรมในอีกรูปแบบหนึ่ง ดังนั้น การที่ธนาคารจะรับ (Adopt) เอาวิธีการทำงานนั้นมาอยู่ในวัฒนธรรมการทำงานในแบบของธนาคาร ธนาคารจึงจำเป็นต้องมีการปรับ (Adapt) แนวคิดหรือกระบวนการบางอย่าง ซึ่งจำเป็นต้องอาศัยการสร้างความเข้าใจกับทุกคนในธนาคารและสื่อสารออกไปอย่างถูกต้องเหมาะสม

ปัจจุบัน ทางธนาคารกำลังพิจารณาอยู่ว่าธนาคารควรจะนำนโยบายหรือนำมาตรฐานและระเบียบวิธีในการปฏิบัติงานมาให้พนักงานได้อ่านจึงจะมีความเหมาะสม เนื่องจากนโยบายนั้นจัดเป็นข้อมูลประเภทที่ใช้ภายในธนาคาร (Internal Use) ไม่ใช่ข้อมูลที่เป็นความลับ (Confidential) ซึ่งตามหลักการแล้วพนักงานทุกคนมีสิทธิ์ที่จะเข้าถึงได้ แต่จะเข้าถึงได้ด้วยรูปแบบใดนั้นคงต้องมีการพิจารณากันอีกครั้ง เนื่องจากปัจจุบันพนักงานส่วนใหญ่ยังแยกความแตกต่างระหว่างนโยบายกับมาตรฐานและระเบียบวิธีในการปฏิบัติงานไม่ได้ เมื่อพนักงานเข้าไปอ่านนโยบายแล้วอาจจะเกิดความคาดหวังว่าจะต้องทราบว่าข้อกำหนดของธนาคารคืออะไร วิธีปฏิบัติที่ถูกต้องเหมาะสมคืออะไร ซึ่งสิ่งต่างๆเหล่านี้จะถูกระบุอยู่ในมาตรฐานและระเบียบวิธีในการปฏิบัติงาน ไม่ใช่นโยบายของธนาคารซึ่งบอกแต่เพียงวัตถุประสงค์กว้างๆ เท่านั้น

เรื่องของการสื่อสารนโยบายด้านความปลอดภัยข้อมูลสารสนเทศให้พนักงานธนาคารเข้าใจนั้น ธนาคารได้มีการวางแผนงานในระยะยาวไว้เป็นเวลา 4 ปี โดยจะแบ่งออกเป็นไตรมาส ในแต่ละไตรมาสก็จะแบ่งเรื่องที่ต้องการสื่อสารออกเป็นหัวข้อต่างๆ ทั้งนี้ ในครึ่งปีแรกทางธนาคารจะสื่อสารเนื้อหาพื้นฐานทั้งหมดที่มีอยู่ในนโยบาย โดยจะเป็นเนื้อหาที่สามารถเข้าใจได้ง่าย เช่น 10 ข้อที่ควรระวังในการทำงาน ซึ่งเป็นเรื่องที่พนักงานทุกคนจำเป็นต้องรับทราบและควรระวังไว้ หลังจากนั้นจึงจะสื่อสารเนื้อหาในหัวข้อต่างๆต่อไป ส่วนเรื่องของช่องทางที่จะใช้ในการสื่อสารนโยบายเพื่อให้ครอบคลุมถึงพนักงานทั้งหมดนั้น ธนาคารจะใช้วิธีการสื่อสารทางโปสเตอร์และจดหมายอิเล็กทรอนิกส์ของธนาคารเป็นหลัก ส่วนจะมีการจัดอบรมสัมนาหรือใช้

ช่องทางอื่นๆเพิ่มเติมหรือไม่นั้น จะขึ้นอยู่กับเนื้อหาที่ต้องการสื่อสารในแต่ละช่วงเวลาเป็นสำคัญ สิ่งเหล่านี้ถือเป็นโปรแกรมการสร้างความตระหนักรู้เรื่องความปลอดภัยข้อมูลสารสนเทศ (Security Awareness Program) ที่ธนาคารพยายามจะสร้างและสื่อสารออกไปยังพนักงานทุกคน

ธนาคารมีความคาดหวังว่า หลังจากที่ธนาคารได้ออกนโยบายความปลอดภัยข้อมูลสารสนเทศไปแล้วช่วงระยะเวลาหนึ่ง อาจจะเป็นหนึ่งหรือสองปี ธนาคารจะต้องมีการพัฒนาไปในทางที่ดีขึ้น (Improvement) อย่างไรก็ตาม การวัดผลในเรื่องดังกล่าวก็เป็นเรื่องยากเช่นกัน ดังนั้นในช่วงแรก ธนาคารจะทำเรื่องที่สามารถวัดผลได้ด้วยระบบก่อน ส่วนการตรวจสอบหรือการประเมินผลตามสาขาต่างๆรวมถึงสาขาต่างประเทศนั้น เป็นประเด็นที่จะนำไปพิจารณาในลำดับถัดไป ส่วนการวัดผลในเรื่องของความตระหนักรู้เรื่องความปลอดภัยข้อมูลสารสนเทศของพนักงานนั้นกำลังอยู่ในขั้นตอนของการพิจารณาหาวิธีการวัดผลที่เหมาะสมและเป็นไปได้ ซึ่งสิ่งที่ธนาคารให้ความสำคัญก็คือ ธนาคารพยายามที่จะยกระดับของความตระหนักรู้เรื่องความปลอดภัยข้อมูลสารสนเทศของพนักงานโดยรวมให้เพิ่มขึ้น โดยอาศัยกลไกการทำงานของธนาคารเป็นตัวช่วย เพื่อที่พนักงานจะได้ไม่รู้สึกว่านโยบายที่ออกมานั้นเป็นสิ่งที่ต้องจำ แต่นโยบายนั้นคือสิ่งที่เข้าไปอยู่ในวิธีการทำงานของพนักงาน นอกจากนี้ ทางธนาคารยังไม่มีการกำหนดบทลงโทษถ้าหากพนักงานไม่ปฏิบัติตามนโยบาย ซึ่งตามปกติแล้วถ้าเป็นเรื่องที่มีความสำคัญมาก ธนาคารจะออกเป็นคำสั่งและมีบทลงโทษชัดเจน แต่ถ้าเป็นเรื่องที่ไม่ได้มีความสำคัญมากนัก ธนาคารจะออกเป็นแนวทางปฏิบัติ ซึ่งถ้าไม่ทำตามอาจจะมีการตักเตือนหรืออื่นๆ ซึ่งจำเป็นต้องพิจารณาร่วมกับฝ่ายทรัพยากรบุคคลของธนาคารต่อไป

ธนาคารได้จัดทำแผนงานเพื่อแสดงให้ผู้บริหารระดับสูงได้เห็นภาพว่าธนาคารต้องการให้ผู้บริหารระดับสูงสนับสนุนนโยบายด้านความปลอดภัยข้อมูลสารสนเทศของธนาคารในเรื่องใดบ้าง นอกเหนือไปจากเรื่องของงบประมาณที่จะใช้เพื่อการสร้างสื่อที่จะส่งไปยังพนักงานทุกคน รวมถึงพนักงานที่อยู่ตามสาขาต่างๆ เช่น เรื่องของรางวัลที่จะให้พนักงานที่เข้าร่วมกิจกรรมต่างๆที่ธนาคารจัดขึ้น เช่น การประกวดคำขวัญในเรื่องของความปลอดภัยข้อมูลสารสนเทศของธนาคาร เป็นต้น ซึ่งรางวัลนั้นควรจะมาจากผู้บริหารระดับสูง เพื่อเป็นการแสดงให้พนักงานเห็นว่าผู้บริหารระดับสูงของธนาคารให้ความสำคัญและมีส่วนร่วมกับกิจกรรมต่างๆที่ออกมาส่งเสริมการปฏิบัติตามนโยบายของธนาคาร อย่างไรก็ตาม ถึงแม้ว่าผู้บริหารระดับสูงของ

ธนาคารจะรับทราบประโยชน์ของการนำนโยบายนี้มาใช้ในธนาคารและให้การสนับสนุนอย่างเต็มที่ แต่ผู้บริหารระดับสูงก็ยังคงมีความกังวลว่านโยบายที่ออกมานั้นสามารถนำไปปฏิบัติจริงได้มากน้อยเพียงใด วิธีการวัดผลเป็นอย่างไร วิธีการตรวจสอบเป็นอย่างไร ซึ่งเป็นคำถามที่เกิดขึ้นกับนโยบายด้านอื่นๆของธนาคารเช่นกัน ทางธนาคารจึงกำหนดให้มีการทบทวนนโยบายและแผนงานต่างๆเป็นระยะ และมีการประเมินผลสำเร็จของนโยบายดังกล่าวเพื่อนำเสนอต่อผู้บริหารระดับสูงอย่างสม่ำเสมออีกด้วย

ความคิดเห็นของผู้เชี่ยวชาญในเรื่องของความปลอดภัยข้อมูลสารสนเทศโดยทั่วไป

ผลสรุปที่ได้จากการสัมภาษณ์ผู้เชี่ยวชาญทั้ง 6 ท่านในเรื่องของความปลอดภัยข้อมูลสารสนเทศโดยทั่วไปมีความสอดคล้องกัน ดังนี้

1. ภัยคุกคามและอาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ต

ผู้เชี่ยวชาญทุกท่านรู้จักภัยคุกคามและอาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ตเป็นอย่างดี ไม่ว่าจะเป็นเรื่องของไวรัส โทรจัน หรือการทำ Social Engineering เพื่อขโมยข้อมูลส่วนตัว เช่น รหัสผ่านเข้าใช้งานระบบ หรือเลขที่บัญชี เป็นต้น โดยอาศัยเทคนิคที่เรียกว่า Phishing ซึ่งในช่วงที่ผ่านมาได้สร้างปัญหาให้กับองค์กรต่างๆ รวมทั้งธนาคารพาณิชย์อื่นๆเป็นอย่างมาก นอกจากนี้ ผู้เชี่ยวชาญทุกท่านยังได้ให้ความเห็นตรงกันในเรื่องของแนวโน้มของภัยคุกคามที่จะเกิดขึ้นในอนาคต ว่าคงจะเกิดจากช่องโหว่ที่พบบนโทรศัพท์เคลื่อนที่มากขึ้น เนื่องจากแนวโน้มของการใช้งานอินเทอร์เน็ตบนโทรศัพท์เคลื่อนที่ในปัจจุบันที่มีจำนวนเพิ่มมากขึ้นเรื่อยๆ ในขณะที่การพัฒนาแอพพลิเคชั่นต่างๆบนโทรศัพท์เคลื่อนที่ยังคงมีข้อจำกัดในเรื่องของความปลอดภัยในการใช้งานอยู่พอสมควร

2. ลักษณะของการรักษาความปลอดภัยข้อมูลสารสนเทศที่ดี

ผู้เชี่ยวชาญทุกท่านมีความเห็นตรงกันว่าในเรื่องของการรักษาความปลอดภัยข้อมูลสารสนเทศนั้น สิ่งที่สำคัญที่สุดคือ ทุกคนที่เกี่ยวข้องกับข้อมูลหรือเอกสารนั้นจำเป็นต้องเข้าใจตรงกันก่อนว่าข้อมูลที่มีอยู่นั้นคืออะไร และจะต้องสามารถแยกแยะประเภทของข้อมูลนั้น

ได้ว่าเป็นข้อมูลที่เป็นความลับ (Confidential) หรือเป็นข้อมูลสำหรับใช้ภายในองค์กรเท่านั้น (Internal Use Only) หรือเป็นข้อมูลประเภทอื่นๆที่ได้มีการจัดลำดับความสำคัญไว้ เพื่อที่จะได้รู้ว่าตัวเองจะต้องปฏิบัติตนต่อข้อมูลนั้นอย่างไร เพราะข้อมูลแต่ละประเภทมีความสำคัญไม่เท่ากัน กระบวนการในการรักษาความปลอดภัยของข้อมูลแต่ละประเภทจึงมีความแตกต่างกัน และนอกจากนี้ก็จะต้องไม่บอกข้อมูลกับคนอื่นที่ไม่จำเป็นต้องรับรู้อีกด้วย

ส่วนเรื่องของความเสียหายที่อาจเกิดขึ้นหากองค์กรไม่มีการรักษาความปลอดภัยข้อมูลสารสนเทศที่เหมาะสมนั้น ผู้เชี่ยวชาญทั้งหมดได้ให้ความเห็นไปในทางเดียวกันว่าระดับของความเสียหายนั้นขึ้นอยู่กับว่าข้อมูลนั้นถูกนำไปใช้ทำอะไร ตัวอย่างเช่น ข้อมูลเรื่องของข้อกำหนดในการติดตั้ง (Configuration) ของระบบ ถ้าหากเป็นเพียงการนำไปเล่าต่อให้บุคคลอื่นฟังโดยที่ผู้ฟังไม่ได้นำข้อมูลนั้นไปทำอะไรต่อ ความเสียหายก็อาจไม่รุนแรง แต่ความเสียหายจะเพิ่มขึ้นหากข้อมูลเรื่องเดียวกันนั้นทำให้ผู้ไม่ประสงค์ดีทราบว่าระบบมีการติดตั้งในลักษณะเป็นแบบนี้ มีช่องโหว่แบบนี้ ก็อาจจะหาทางโจมตีระบบได้โดยง่าย หรือเรื่องของผลิตภัณฑ์และบริการใหม่ๆที่เป็นความลับขององค์กร ถ้าหากรั่วไหลไปถึงบุคคลภายนอกที่ไม่ได้มีส่วนเกี่ยวข้องก็คงไม่สร้างความเสียหายอะไร แต่ถ้าหากข้อมูลนั้นรั่วไหลไปถึงคู่แข่งขององค์กร และคู่แข่งสามารถเลียนแบบและออกผลิตภัณฑ์และบริการนั้นได้ก่อน ก็อาจส่งผลให้องค์กรไม่สามารถขายผลิตภัณฑ์และบริการนั้นๆให้แก่ลูกค้าได้ เป็นต้น

3. มาตรฐานการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศ

ผู้เชี่ยวชาญทุกท่านรู้จักมาตรฐานการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศแบบต่างๆเป็นอย่างดี ไม่ว่าจะเป็นมาตรฐาน ISO/IEC 17799:2005 หรือมาตรฐาน ISO/IEC 27001:2005 ซึ่งเป็นข้อกำหนดในการบริหารจัดการข้อมูลสารสนเทศขององค์กรให้มีความปลอดภัย มาตรฐาน Payment Card Industry (PCI) ซึ่งเป็นข้อกำหนดทางด้านความมั่นคงปลอดภัยของระบบที่เกี่ยวข้องกับข้อมูลของบัตรเครดิต รวมทั้งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ความคิดเห็นของผู้เชี่ยวชาญในเรื่องของความปลอดภัยข้อมูลสารสนเทศของธนาคาร

ผลสรุปที่ได้จากการสัมภาษณ์ผู้เชี่ยวชาญทั้ง 6 ท่านในเรื่องของความปลอดภัยข้อมูลสารสนเทศของธนาคารมีความสอดคล้องกัน ดังนี้

1. การรักษาความปลอดภัยข้อมูลสารสนเทศของธนาคาร

ปัจจุบันธนาคารมีการแบ่งประเภทของเอกสารเป็นระดับต่างๆอยู่แล้ว แต่ก็ยังคงพบปัญหาว่าพนักงานของธนาคารมีความตระหนักถึงระดับความสำคัญของเอกสารไม่เท่ากัน และมีความเข้าใจที่ไม่ตรงกันว่าเอกสารชนิดใดควรจัดอยู่ในประเภทใด หน่วยงานแต่ละหน่วยงานก็จะมีหลักเกณฑ์ของตนเองในการกำหนดว่าเอกสารใดเป็นหรือไม่เป็นความลับ ทำให้พบปัญหาในการควบคุมเอกสารต่างๆอยู่เสมอ อย่างไรก็ตาม ผู้เชี่ยวชาญทั้งหมดได้ให้ความเห็นว่าธนาคารมีนโยบายและระเบียบปฏิบัติในเรื่องของการรักษาความปลอดภัยข้อมูลสารสนเทศที่ดีอยู่แล้ว แต่ปัญหาในการนำนโยบายมาใช้นั้นอยู่ที่ตัวของผู้ปฏิบัติงาน ซึ่งก็คือพนักงานของธนาคารมากกว่า และเมื่อรวมกับวัฒนธรรมขององค์กรที่ไม่ได้มีการบังคับใช้กฎระเบียบอย่างเคร่งครัด จึงทำให้นโยบายต่างๆที่ออกมานั้นดูไม่มีประสิทธิภาพเท่าที่ควร นอกจากนี้ การอะลุ้มอล่วยในเรื่องของการปฏิบัติตามกฎระเบียบของธนาคาร และการที่ธนาคารไม่ได้กำหนดบทลงโทษที่ชัดเจน ก็เป็นส่วนหนึ่งที่ทำให้พนักงานไม่ปฏิบัติตามนโยบายและกฎระเบียบของธนาคารอย่างเคร่งครัด

ในส่วนของนโยบายด้านความปลอดภัยข้อมูลสารสนเทศของธนาคารนั้น ธนาคารได้นำมาตรฐาน ISO/IEC 17799:2005 มาเป็นแม่แบบในการร่างนโยบายดังกล่าว โดยเนื้อหาของนโยบายนั้นจะครอบคลุมถึงหัวข้อในการควบคุมทั้ง 133 หัวข้อที่มีอยู่ในมาตรฐาน ISO/IEC 17799:2005 รวมถึงหัวข้อในการควบคุมที่เพิ่มขึ้นมาอีก 11 หัวข้อซึ่งถูกระบุอยู่ในมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 2) ประจำปี พ.ศ. 2549 ที่จัดทำโดยคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ โดยมีการปรับรายละเอียดของมาตรการในการควบคุมบางอย่างเพื่อให้เหมาะสมกับลักษณะการดำเนินงานของธนาคาร อย่างไรก็ตาม ในส่วนของการประกาศนโยบายเพื่อให้พนักงานทั้งหมดของธนาคารรับทราบนั้นยังอยู่ในขั้นตอนของการพิจารณาของผู้บริหารว่าจะใช้ช่องทางใดจึงจะเหมาะสม และในส่วนของการบังคับใช้นโยบายนั้น ทางธนาคารไม่ได้บังคับใช้นโยบายแบบทันทีทันใด แต่ใช้วิธีค่อยๆสร้าง

ความตระหนักรู้และชี้แจงให้เห็นถึงความจำเป็นและความสำคัญของการปฏิบัติตามนโยบายของธนาคารเพื่อประโยชน์ในการปกป้องความปลอดภัยข้อมูลสารสนเทศให้แก่พนักงาน เพื่อป้องกันไม่ให้เกิดแรงต่อต้านและความรู้สึกกดดันต่อพนักงานจนเกินไป

นอกจากนี้ ในส่วนของการพัฒนาเว็บแอพพลิเคชั่นต่างๆของธนาคารนั้น พบว่าทีมพัฒนา เว็บแอพพลิเคชั่นบางทีมไม่ได้คำนึงถึงเรื่องของความปลอดภัยข้อมูลสารสนเทศตั้งแต่เมื่อเริ่มต้นออกแบบระบบ ทำให้เมื่อพบช่องโหว่ในช่วงของการตรวจสอบระบบ ซึ่งเป็นช่วงระยะเวลาที่แอพพลิเคชั่นใกล้จะเสร็จสมบูรณ์แล้วนั้น จึงต้องเสียเวลาในการรื้อระบบเพื่อแก้ไขช่องโหว่ดังกล่าว ทั้งๆที่ธนาคารก็ได้มีการพัฒนาเอกสารซึ่งเป็นข้อกำหนดทางด้านความปลอดภัยระบบเพื่อเป็นแนวทางในการพัฒนาเว็บแอพพลิเคชั่นให้มีความปลอดภัยอยู่แล้ว อย่างไรก็ดี ทีมพัฒนาเว็บแอพพลิเคชั่นโดยส่วนใหญ่ก็ไม่สามารถทำตามข้อกำหนดดังกล่าวได้ทั้งหมด เนื่องจากเนื้อหาในเอกสารนั้นจะบอกแต่เพียงหลักการในการพัฒนาเว็บแอพพลิเคชั่นให้มีความปลอดภัย โดยที่ไม่ได้บอกว่าจะต้องทำอย่างไร ซึ่งเป็นสิ่งที่ยากสำหรับนักพัฒนาเว็บแอพพลิเคชั่นเหล่านั้นหากพวกเขาไม่ได้มีความเข้าใจในเรื่องของความปลอดภัยข้อมูลสารสนเทศอย่างเพียงพอ

2. การรักษาความปลอดภัยข้อมูลสารสนเทศของบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคาร

ปัจจุบันธนาคารมีการวางรากฐานของโครงสร้างของ Environment รวมถึงการควบคุมต่างๆที่มีแบบแผนที่ดีอยู่แล้ว ซึ่งบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารก็อยู่ในโครงสร้างของ Environment ดังกล่าว จึงถือได้ว่า บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารนั้นมีการควบคุมที่ดี นอกจากนี้ ธนาคารยังได้จัดทำเอกสารที่เรียกว่า Web Application Security Requirement ซึ่งเป็นข้อกำหนดในการพัฒนาเว็บแอพพลิเคชั่นของธนาคาร ซึ่งหมายความรวมถึงบริการทางการเงินผ่านอินเทอร์เน็ต ให้มีความปลอดภัย ทั้งนี้ เอกสารดังกล่าวได้รวบรวมข้อกำหนดและเนื้อหาจากแหล่งที่มาหลายๆแหล่ง เช่น จากเอกสารขององค์กรที่ทำหน้าที่ดูแลทางด้านความปลอดภัยข้อมูลสารสนเทศ เช่น Open Web Application Security Project (OWASP) จากช่องโหว่ของระบบที่เคยพบในอดีต จากการสืบค้นทางอินเทอร์เน็ต และจากการสอบถามข้อมูลจากผู้ที่มีความรู้และประสบการณ์ เป็นต้น

ในส่วนของข้อกำหนดในการติดตั้งระบบของบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารนั้น ไม่ว่าจะเป็นเรื่องของระบบปฏิบัติการ (Operating System) หรือฐานข้อมูล (Database) ทางธนาคารจะใช้ Best Practice ของ Vendor นั้นๆ เช่น ถ้าเป็นระบบปฏิบัติการ Windows ก็จะใช้ Best Practice ของไมโครซอฟท์ แล้วนำมาปรับให้เข้ากับบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคาร นอกจากนี้ ธนาคารยังได้กำหนดให้มีบริษัทภายนอกที่เป็นผู้ตรวจสอบความปลอดภัยของเว็บแอพพลิเคชั่นเข้ามาทำการตรวจสอบบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารอยู่เป็นระยะอีกด้วย

นอกเหนือไปจากกฎระเบียบต่างๆของธนาคารแห่งประเทศไทยที่ธนาคารจำเป็นต้องปฏิบัติตามอย่างเคร่งครัดแล้วนั้น ธนาคารยังได้ปฏิบัติตามข้อกำหนดของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในส่วนที่ว่าด้วยการเก็บข้อมูลจราจร (Log) ของบริการทางการเงินผ่านอินเทอร์เน็ต โดยกำหนดให้มีการเก็บข้อมูลจราจรบางอย่างเพิ่มขึ้นเพื่อให้เพียงพอต่อข้อกำหนดของพระราชบัญญัติดังกล่าว นอกจากนี้ธนาคารยังได้มีการพัฒนาระบบ Centralized Log Management ขึ้นมาเพื่อช่วยให้การบริหารจัดการข้อมูลจราจรของเว็บแอพพลิเคชั่นทั้งหมดของธนาคารมีประสิทธิภาพมากยิ่งขึ้น

นอกจากนี้ธนาคารยังได้นำหัวข้อในการควบคุมที่ระบุอยู่ในมาตรฐาน ISO/IEC 17799:2005 มาใช้เป็นมาตรการในการป้องกันความปลอดภัยของบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารอีกด้วย

ข้อกำหนดในการพัฒนาบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคาร

ข้อกำหนดในการพัฒนาบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารให้มีความปลอดภัยตามที่ได้ระบุไว้ใน Web Application Security Requirement ของธนาคารนั้นประกอบไปด้วยหัวข้อดังต่อไปนี้

1. Input/Parameter Validation คือ ข้อกำหนดสำหรับการตรวจสอบความถูกต้องของข้อมูลรับเข้าหรือค่าพารามิเตอร์ต่างๆก่อนที่จะถูกนำไปใช้ในระบบ โดยค่าที่ระบบจะ

อนุญาตให้นำไปใช้ในการประมวลผลต่อนั้นจะต้องอยู่ในรูปแบบที่ระบบได้กำหนดไว้เท่านั้น

2. Access Control/Authorization คือ ข้อกำหนดสำหรับการตรวจสอบสิทธิ์ในการเข้าใช้งานและการเข้าถึงข้อมูลของผู้ที่มีสิทธิ์เข้าใช้งานระบบ
3. Authentication and Session Management คือ ข้อกำหนดในการระบุตัวตนของผู้ใช้งานระบบ การปกป้องข้อมูลส่วนตัวของผู้ใช้งานระบบตลอดระยะเวลาที่เข้าใช้งานระบบ รวมถึงข้อกำหนดที่เกี่ยวข้องกับรหัสผ่านของผู้ใช้งานระบบด้วย
4. Cross Site Scripting คือ ข้อกำหนดสำหรับการตรวจสอบความถูกต้องของค่าต่างๆที่มีการรับส่งระหว่าง Client กับ Server เช่น ค่าของ Headers, Cookies, Query Strings, Form Fields, และ Hidden Fields เพื่อป้องกันการรัน Script ไม่พึงประสงค์ซึ่งอาจนำไปสู่การขโมยข้อมูลส่วนตัวของผู้ใช้งานระบบได้
5. Buffer Overflow คือ ข้อกำหนดเพื่อป้องกันไม่ให้ระบบเกิดช่องโหว่ในเรื่องของ Buffer Overflow ที่เกิดจากการรับข้อมูลที่มีขนาดใหญ่เกินไปมาประมวลผล ซึ่งอาจสร้างความเสียหายต่อระบบโดยทำให้ระบบไม่สามารถให้บริการได้
6. Interpreter Injection คือ ข้อกำหนดเพื่อป้องกันไม่ให้ผู้ใช้งานระบบทั่วไปสามารถรันคำสั่งบางอย่างในระดับปฏิบัติการได้ เช่น คำสั่งที่ใช้ในการเข้าถึงฐานข้อมูล หรือคำสั่งที่ใช้ในการเข้าถึงระบบปฏิบัติการของ Server เป็นต้น
7. Error Handling คือ ข้อกำหนดในการจัดการกับข้อผิดพลาดที่เกิดขึ้นกับระบบอย่างเหมาะสม เช่น มีการขึ้นข้อความแสดงความผิดปกติของระบบให้ผู้ใช้งานรับรู้ แต่ในขณะเดียวกันก็ต้องไม่เปิดเผยข้อมูลของระบบซึ่งผู้ไม่ประสงค์อาจนำไปใช้โจมตีระบบได้ เป็นต้น
8. Data Protection คือ ข้อกำหนดในการเข้ารหัสข้อมูลอย่างเหมาะสมเพื่อปกป้องความลับและความถูกต้องของข้อมูลของผู้ใช้งานระบบ
9. Availability/Denial of Service คือ ข้อกำหนดในการป้องกันการถูกโจมตีระบบจากผู้ไม่ประสงค์ดีจนระบบไม่สามารถให้บริการได้
10. Application/Infrastructure Configuration Management คือ ข้อกำหนดในการ Hardening ระบบและโครงสร้างของระบบให้มีความปลอดภัย โดยการปิดช่องโหว่ของระบบ เช่น Service, Port, หรือ Protocol ที่ไม่จำเป็นต่อการใช้งาน เป็นต้น

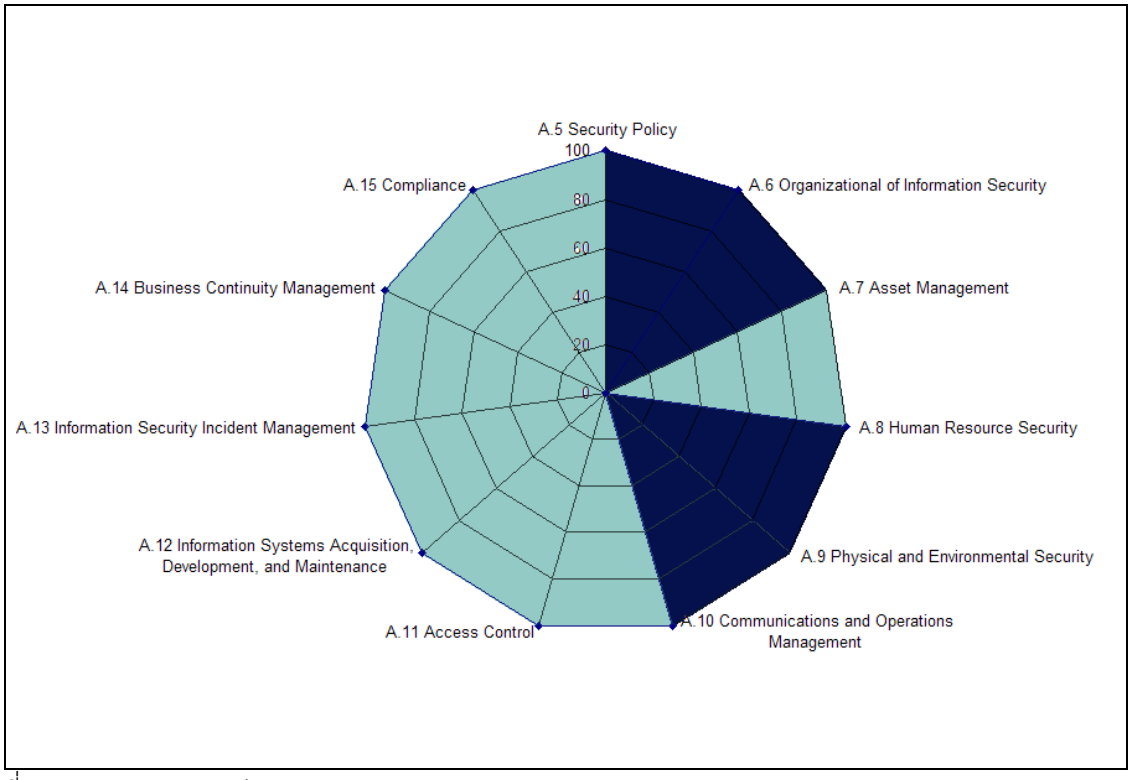
11. Safe Practices in Logging คือ ข้อกำหนดในการเก็บข้อมูลการทำงานและการเปลี่ยนแปลงที่เกิดขึ้นกับระบบ เช่น ข้อมูลเกี่ยวกับการบริหารจัดการผู้ใช้งานระบบ ข้อมูลการเข้าถึงระบบของผู้ใช้งานระบบทุกคน ข้อมูลการเปลี่ยนแปลง Registry Keys ของระบบ เป็นต้น

ผลการทำ Gap Analysis ในส่วนของบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคาร

จากการทำ Gap Analysis โดยการเปรียบเทียบลักษณะของการดำเนินงานและการบริหารจัดการบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารกับหัวข้อของการควบคุมที่ระบุอยู่ในมาตรฐาน ISO/IEC 17799:2005 ทั้ง 11 หัวข้อ 133 มาตรการ พบว่า บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารนั้นมีมาตรการในการควบคุมที่สอดคล้องกับแนวทางและข้อกำหนดในการป้องกันความปลอดภัยข้อมูลสารสนเทศที่ระบุอยู่ในมาตรฐาน ISO/IEC 17799:2005 เป็นอย่างมาก โดยความสอดคล้องนั้นสามารถแบ่งออกได้เป็น 2 ลักษณะ ดังนี้

ภาพที่ 4.1

ผลการทำ Gap Analysis ในส่วนของบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคาร



ที่มา: จากการสัมภาษณ์

1. ความสอดคล้องของการบริหารจัดการบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารกับมาตรฐาน ISO/IEC 17799:2005 โดยตรง หมายความว่า บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารนั้นมีมาตรการในการจัดการความปลอดภัยข้อมูลสารสนเทศในระดับต่างๆเป็นของตนเอง และมาตรการดังกล่าวนั้นก็สอดคล้องกับข้อกำหนดที่ได้ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 อย่างชัดเจน ทั้งนี้ หัวข้อของการควบคุมที่มีความสอดคล้องในลักษณะดังกล่าวประกอบด้วย

    - A.7 Asset Management
    - A.10 Communications and Operations Management
    - A.11 Access Control
    - A.12 Information Systems Acquisition, Development, and Maintenance
    - A.13 Information Security Incident Management
    - A.14 Business Continuity Management
    - A.15 Compliance

2. ความสอดคล้องของการบริหารจัดการบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารกับมาตรฐาน ISO/IEC 17799:2005 โดยอ้อม หมายความว่า บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารนั้นไม่มีมาตรการในการจัดการความปลอดภัยข้อมูลสารสนเทศตามที่ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 อย่างชัดเจน แต่เนื่องจากบริการทางการเงินผ่านอินเทอร์เน็ตนั้นถือเป็นส่วนหนึ่งของการบริหารจัดการภายในธนาคาร ดังนั้น ถ้าหากในภาพรวมแล้วธนาคารมีการวางนโยบายด้านความปลอดภัยข้อมูลสารสนเทศที่สอดคล้องกับข้อกำหนดที่ได้ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 แล้ว ก็สามารถกล่าวได้ว่า บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารมีมาตรการในการจัดการความปลอดภัยข้อมูลสารสนเทศที่สอดคล้องกับข้อกำหนดที่ได้ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 ทั้งนี้ หัวข้อของการควบคุมที่มีความสอดคล้องในลักษณะดังกล่าวประกอบด้วย

    - A.5 Security Policy
    - A.6 Organizational of Information Security

- A.8 Human Resource Security
- A.9 Physical and Environmental Security

ทั้งนี้ รายละเอียดของการเปรียบเทียบลักษณะของการดำเนินงานและการบริหารจัดการบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารกับหัวข้อของการควบคุมที่ระบุอยู่ในมาตรฐาน ISO/IEC 17799:2005 ทั้ง 11 หัวข้อ 133 มาตรการ สามารถแสดงได้ดังตารางต่อไปนี้

ตารางที่ 4.1

ผลการเปรียบเทียบ

บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารกับมาตรฐาน ISO/IEC 17799:2005

หัวข้อและมาตรการ	คำอธิบาย	ความสอดคล้อง (ใช่/ไม่ใช่)
A.5 นโยบายความมั่นคงปลอดภัย (Security Policy)		
A.5.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information Security Policy)	**มีจุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง**	
A.5.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information Security Policy Document)	ต้องจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรอย่างเป็นลายลักษณ์อักษร เอกสารนโยบายต้องได้รับการอนุมัติจากผู้บริหารขององค์กรก่อนนำไปใช้งาน และต้องเผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ	ใช่
A.5.1.2 การทบทวนนโยบายความมั่นคงปลอดภัย (Review of The Information Security Policy)	ต้องดำเนินการทบทวนนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร	ใช่
A.6 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organizational of Information Security)		
A.6.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal Organization)	**มีจุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร**	
A.6.1.1 การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management Commitment to Information Security)	ต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง การมอบหมายงานที่เหมาะสมต่อบุคลากร และการเล็งเห็นถึงความสำคัญของหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ	ใช่
A.6.1.2 การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information Security Coordination)	ต้องกำหนดให้มีตัวแทนพนักงานจากหน่วยงานต่างๆ ภายในองค์กรเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร โดยที่ตัวแทนเหล่านั้นจะมีบทบาทและลักษณะงานที่รับผิดชอบที่แตกต่างกัน	ใช่
A.6.1.3 การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of Information Security Responsibilities)	ต้องกำหนดหน้าที่ความรับผิดชอบของพนักงานในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน	ใช่
A.6.1.4 กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ (Authorization Process for Information Processing Facilities)	ต้องกำหนดกระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศใหม่และบังคับให้มีการใช้งานกระบวนการนี้	ใช่

หัวข้อและมาตรการ	คำอธิบาย	ความสอดคล้อง (ใช่/ไม่ใช่)
A.6.1.5 การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality Agreements)	ต้องจัดให้มีการลงนามในข้อตกลงระหว่างพนักงานกับองค์กรว่าจะไม่เปิดเผยความลับขององค์กร (โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างพนักงานนั้น) รวมทั้งเงื่อนไขหรือข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการไม่เปิดเผยความลับจะต้องได้รับการปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับความต้องการขององค์กร	ใช่
A.6.1.6 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น (Contact with Authorities)	ต้องมีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆ เช่น สำนักงานตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ บมจ. ทศท คอร์ปอเรชั่น บมจ. กสท โทรคมนาคม ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น	ใช่
A.6.1.7 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with Special Interest Groups)	ต้องมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่างๆ ที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มที่ความสนใจด้านความมั่นคงปลอดภัยสารสนเทศ หรือสมาคมต่างๆ ในอุตสาหกรรมที่องค์กรมีส่วนร่วม	ใช่
A.6.1.8 การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ (Independent Review of Information Security)	ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อองค์กร	ใช่
A.6.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties)	**มีจุดประสงค์เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก**	
A.6.2.1 การประเมินความเสี่ยงของการเข้าถึงสารสนเทศของหน่วยงานภายนอก (Identification of Risks Related to External Parties)	ต้องกำหนดให้มีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้	ใช่
A.6.2.2 การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing Security when Dealing with Customers)	ต้องระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ลูกค้าหรือผู้ใช้บริการเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้	ใช่
A.6.2.3 การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing Security in Third Party Agreements)	ต้องระบุและจัดทำข้อกำหนดหรือข้อตกลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศระหว่างองค์กรและหน่วยงานภายนอก เมื่อมีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้	ใช่
A.7 การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)		
A.7.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for Assets)	**มีจุดประสงค์เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจเกิดขึ้นได้**	
A.7.1.1 การจัดทำบัญชีทรัพย์สิน (Inventory of Assets)	ต้องจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้ถูกต้องอยู่เสมอ	ใช่
A.7.1.2 การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of Assets)	ต้องจัดให้มีการระบุผู้เป็นเจ้าของสารสนเทศ (แต่ละชนิด) และทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ ตามที่กำหนดไว้ในบัญชีทรัพย์สิน	ใช่

หัวข้อและมาตรการ	คำอธิบาย	ความสอดคล้อง (ใช่/ไม่ใช่)
A.7.1.3 การใช้งานทรัพย์สินที่เหมาะสม (Acceptable Use of Assets)	จะต้องจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อทรัพย์สินเหล่านั้น เช่น อันเกิดจากการขาดความระมัดระวัง การขาดการดูแลและเอาใจใส่ เป็นต้น	ใช่
A.7.2 การจัดหมวดหมู่สารสนเทศ (Information Classification)	**มีจุดประสงค์เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม**	
A.7.2.1 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification Guidelines)	จะต้องจัดให้มีกระบวนการในการจัดหมวดหมู่ของทรัพย์สินสารสนเทศตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมาย และระดับความสำคัญที่มีต่อองค์กร ทั้งนี้เพื่อจะได้หาวิธีการในการป้องกันได้อย่างเหมาะสม	ใช่
A.7.2.2 การจัดทำป้ายชื่อ และการจัดการทรัพย์สินสารสนเทศ (Information Labeling and Handling)	จะต้องจัดให้มีขั้นตอนปฏิบัติในการจัดทำป้ายชื่อและการจัดการทรัพย์สินสารสนเทศตามที่ได้จัดหมวดหมู่ไว้แล้ว	ใช่
A.8 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคคลากร (Human Resource Security)		
A.8.1 การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to Employment)	**มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง (เช่น เพื่อการบำรุงรักษาอุปกรณ์ต่างๆ ขององค์กร) และหน่วยงานภายนอกเข้าใจถึงบทบาท และหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์**	
A.8.1.1 การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Roles and Responsibilities)	ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับพนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และ/หรือหน่วยงานภายนอกที่องค์กรต้องการว่าจ้างมาปฏิบัติงานให้องค์กร และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร	ใช่
A.8.1.2 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)	ต้องทำการตรวจสอบคุณสมบัติของผู้สมัคร (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญา และการว่าจ้างหน่วยงานภายนอก) โดยละเอียด เช่น ตรวจสอบจากจดหมายรับรอง ประวัติการทำงาน วุฒิการศึกษา บุคคลหรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น และจะต้องพิจารณากฎหมาย ระเบียบ จริยธรรม ชั้นความลับของทรัพย์สินสารสนเทศ และระดับความเสี่ยงในการเข้าถึง ประกอบการคัดเลือกด้วย	ใช่
A.8.1.3 การกำหนดเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)	ต้องกำหนดเงื่อนไขการจ้างงาน (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญา และการว่าจ้างหน่วยงานภายนอก) ซึ่งรวมถึงหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ และบุคลากรที่จะได้รับการว่าจ้างดังกล่าวจะต้องเห็นชอบและลงนามในเงื่อนไขการจ้างงานนั้นด้วย	ใช่
A.8.2 การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During Employment)	**มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และได้เรียนรู้และทำความเข้าใจเกี่ยวกับนโยบายความมั่นคงปลอดภัยขององค์กร รวมทั้งเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่**	

หัวข้อและมาตรการ	คำอธิบาย	ความสอดคล้อง (ใช่/ไม่ใช่)
A.8.2.1 หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management Responsibilities)	ต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงานและผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย ตามนโยบายและขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร	ใช่
A.8.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information Security Awareness, Education and Training)	ต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงาน และผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอก ได้รับการอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ทางด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ การอบรมควรครอบคลุมถึงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยขององค์กรตามลักษณะงานที่พนักงานต้องรับผิดชอบด้วย	ใช่
A.8.2.3 กระบวนการทางวินัยเพื่อลงโทษ (Disciplinary Process)	ต้องจัดให้มีกระบวนการทางวินัยเพื่อลงโทษพนักงานที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร	ใช่
A.8.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination or Change of Employment)	**พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน**	
A.8.3.1 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination Responsibilities)	ต้องกำหนดหน้าที่ความรับผิดชอบสำหรับผู้ที่องค์กรเลิกการจ้างงานหรือองค์กรเปลี่ยนลักษณะการจ้างงาน และกำหนดให้ปฏิบัติตามหน้าที่ดังกล่าว	ใช่
A.8.3.2 การคืนทรัพย์สินขององค์กร (Return of Assets)	ต้องกำหนดให้ผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงานคืนทรัพย์สินขององค์กรที่อยู่ในความครอบครองของตน	ใช่
A.8.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of Access Rights)	ต้องทำการถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน	ใช่
A.9 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)		
A.9.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)	**เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร**	
A.9.1.1 การจัดทำบริเวณล้อมรอบ (Physical Security Perimeter)	ต้องมีการจัดสรรพื้นที่ กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า-ออกที่มีการควบคุม ตั้งโต๊ะทำการของ รปภ. บริเวณทางเข้า-ออกของสำนักงาน เป็นต้น เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร	ใช่
A.9.1.2 การควบคุมการเข้า-ออก (Physical Entry Controls)	ต้องจัดให้มีการควบคุมการเข้า-ออก ในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย และอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น	ใช่
A.9.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing Offices, Rooms and Facilities)	ต้องจัดให้มีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อสำนักงานห้องทำงานและทรัพย์สินอื่นๆ	ใช่
A.9.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting Against External and Environmental Threats)	ต้องจัดให้มีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหว การระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ	ใช่
A.9.1.5 การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in Secure Areas)	ต้องจัดให้มีการป้องกันทางกายภาพและแนวทางสำหรับการปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย	ใช่

หัวข้อและมาตรการ	คำอธิบาย	ความสอดคล้อง (ใช่/ไม่ใช่)
A.9.1.6 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access, Delivery, and Loading Areas)	ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ ควรจัดเป็นบริเวณแยกออกมาต่างหาก	ใช่
A.9.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)	**เพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และการทำให้กิจกรรมการดำเนินงานต่างๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก**	
A.9.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment Sitting and Protection)	ต้องจัดวางและป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต	ใช่
A.9.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)	ต้องกำหนดให้มีกลไกการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนต่างๆ ได้แก่ ระบบกระแสไฟฟ้า ระบบน้ำประปา ระบบควบคุมอุณหภูมิ ระบบระบายอากาศ ระบบปรับอากาศ ระบบกระแสไฟฟ้าสำรอง ระบบสายสื่อสารสำรอง เป็นต้น	ใช่
A.9.2.3 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)	ต้องกำหนดให้การเดินสายไฟฟ้า สายสื่อสาร และสายเคเบิ้ลอื่นๆ ได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต การทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายสัญญาณเหล่านั้นเสียหาย	ใช่
A.9.2.4 การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)	ต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่างๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน	ใช่
A.9.2.5 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of Equipment Off-Premises)	ต้องกำหนดให้มีการป้องกันอุปกรณ์ต่างๆ ที่ใช้งานอยู่นอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้น การป้องกันให้พิจารณาจากความเสี่ยงต่างๆ ที่มีต่ออุปกรณ์เหล่านั้น	ใช่
A.9.2.6 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-Use of Equipment)	ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทับก่อนที่จะทิ้งอุปกรณ์ดังกล่าวไป ทั้งนี้เพื่อเป็นการป้องกันข้อมูลดังกล่าวหากมีการนำอุปกรณ์กลับมาใช้งานอีกครั้ง	ใช่
A.9.2.7 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of Property)	ต้องไม่อนุญาตการนำทรัพย์สินขององค์กร ได้แก่ อุปกรณ์ สารสนเทศ หรือซอฟต์แวร์ ออกนอกองค์กร เว้นเสียแต่จะได้รับอนุญาตแล้วเท่านั้น	ใช่
A.10 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and Operations Management)		
A.10.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational Procedures and Responsibilities)	**เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย**	
A.10.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented Operating Procedures)	ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงาน ปรับปรุงตามระยะเวลาอันสมควร และแจกจ่ายให้กับผู้ที่เกี่ยวข้อง	ใช่
A.10.1.2 การควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ (Change Management)	ต้องกำหนดให้มีการควบคุมการปลี่ยนแปลง ปรับปรุง หรือ แก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ	ใช่

หัวข้อและมาตรการ	คำอธิบาย	ความสอดคล้อง (ใช่/ไม่ใช่)
A.10.1.3 การแบ่งหน้าที่ความรับผิดชอบ (Segregation of Duties)	ต้องกำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต หรือใช้ผิดวัตถุประสงค์ต่อทรัพย์สินสารสนเทศขององค์กร	ใช่
A.10.1.4 การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development, Test, and Operational Facilities)	ต้องจัดให้มีการแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขต่อระบบสำหรับการให้บริการจริงโดยไม่ได้รับอนุญาต	ใช่
A.10.2 การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third Party Service Delivery Management)	**เพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก**	
A.10.2.1 การให้บริการโดยหน่วยงานภายนอก (Service Delivery)	ต้องกำหนดให้ผู้ให้บริการจากภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กรและผู้ให้บริการ ข้อตกลงควรกล่าวถึงมาตรการการรักษาความมั่นคงปลอดภัย ลักษณะของการให้บริการ และระดับของการให้บริการ	ใช่
A.10.2.2การตรวจสอบการให้บริการโดยหน่วยงานภายนอก (Monitoring and Review of Third Party Services)	ต้องตรวจสอบการให้บริการโดยหน่วยงานภายนอกอย่างสม่ำเสมอ เช่น การดูจากการให้บริการ การศึกษาจากรายงานและข้อมูลต่างๆ ที่กำหนดให้บันทึกไว้ เป็นต้น	ใช่
A.10.2.3 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ (Managing Changes to Third Party Services)	ต้องกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอกเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การปรับปรุงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัย การเปลี่ยนเทคโนโลยีใหม่ การใช้ผลิตภัณฑ์ใหม่ เป็นต้น ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก	ใช่
A.10.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System Planning and Acceptance)	**เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ**	
A.10.3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity Management)	ต้องมีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพที่เหมาะสมและเพียงพอต่อการใช้งาน	ใช่
A.10.3.2 การตรวจรับระบบ (System Acceptance)	ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติม หรือที่เป็นรุ่นใหม่ รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน	ใช่
A.10.4 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection Against Malicious and Mobile Code)	**เพื่อรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลาย โดยซอฟต์แวร์ที่ไม่ประสงค์ดี**	
A.10.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls Against Malicious Code)	ต้องมีมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืนเพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานด้วย	ใช่
A.10.4.2 การป้องกันโปรแกรมชนิดเคลื่อนที่ (Controls Against Mobile Code)	ต้องมีมาตรการเพื่อควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่ (โปรแกรมที่เคลื่อนที่จากหน่วยความจำของเครื่องคอมพิวเตอร์หนึ่งเพื่อไปทำงานในหน่วยความจำของอีกเครื่องคอมพิวเตอร์หนึ่ง) ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยขององค์กร และต้องป้องกันไม่ให้โปรแกรมชนิดเคลื่อนที่อื่นๆ สามารถทำงานหรือใช้งานได้	ใช่
A.10.5 การสำรองข้อมูล (Back-Up)	**เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ**	

หัวข้อและมาตรการ	คำอธิบาย	ความสอดคล้อง (ใช่/ไม่ใช่)
A.10.5.1 การสำรองข้อมูล (Information Back-Up)	ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอและให้เป็นไปตามนโยบายการสำรองข้อมูลขององค์กร	ใช่
A.10.6 การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network Security Management)	**เพื่อป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย**	
A.10.6.1 มาตรการทางเครือข่าย (Network Controls)	ต้องบริหารและจัดการเครือข่าย กำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆ ทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอพพลิเคชั่นที่ใช้งานเครือข่าย รวมทั้งสารสนเทศต่างๆ ที่ส่งผ่านทางเครือข่าย	ใช่
A.10.6.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services)	ต้องกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดในการบริหารจัดการสำหรับบริการเครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่าย โดยที่บริการเครือข่ายเหล่านี้อาจจะเป็นบริการเครือข่ายภายในขององค์กรเองหรือบริการที่ได้รับจากหน่วยงานภายนอก	ใช่
A.10.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media Handling)	**เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต และการติดขัดหรือหยุดชะงักทางธุรกิจ**	
A.10.7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media)	ต้องกำหนดขั้นตอนปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้	ใช่
A.10.7.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of Media)	ต้องกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไปแล้ว การทำลายต้องเป็นไปอย่างมั่นคงและปลอดภัย	ใช่
A.10.7.3 ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information Handling Procedures)	ต้องกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและการจัดเก็บสารสนเทศเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์	ใช่
A.10.7.4 การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of System Documentation)	ต้องกำหนดมาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต	ใช่
A.10.8 การแลกเปลี่ยนสารสนเทศ (Exchange of Information)	**เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก**	
A.10.8.1 นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information Exchange Policies and Procedures)	ต้องกำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการรองรับ เพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร (เช่น องค์กรและหน่วยงานภายนอก) โดยผ่านทางช่องทางการสื่อสารทุกชนิด	ใช่
A.10.8.2 ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange Agreements)	ต้องจัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศและซอฟต์แวร์ระหว่างองค์กร อย่างเป็นลายลักษณ์อักษร	ใช่
A.10.8.3 การส่งสื่อบันทึกข้อมูลออกไปนอกองค์กร (Physical Media in Transit)	ต้องป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตการใช้งานผิดวัตถุประสงค์ และการทำให้ข้อมูลเกิดความเสียหายในระหว่างที่ส่งข้อมูลนั้นออกไปนอกองค์กร	ใช่
A.10.8.4 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging)	ต้องกำหนดมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์	ใช่

หัวข้อและมาตรการ	คำอธิบาย	ความสอดคล้อง (ใช่/ไม่ใช่)
A.10.8.5 ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems)	ต้องกำหนดนโยบายและขั้นตอนปฏิบัติเพื่อป้องกันสารสนเทศที่เกี่ยวข้องกับระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน	ใช่
A.10.9 การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce Services)	**เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และในการใช้งาน**	
A.10.9.1 การพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce)	ต้องกำหนดมาตราการสำหรับการป้องกันสารสนเทศของระบบพาณิชย์อิเล็กทรอนิกส์ที่มีการส่งผ่านทางเครือข่ายสาธารณะจากการฉ้อโกง การปฏิเสธ การเปิดเผย และการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต	ใช่
A.10.9.2 การทำธุรกรรมออนไลน์ (On-Line Transactions)	ต้องกำหนดมาตราการสำหรับการป้องกันสารสนเทศที่รับ-ส่งที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ ทั้งนี้เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ-ส่ง สารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่าย การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผยสารสนเทศโดยไม่ได้รับอนุญาต หรือการทำสำเนาสารสนเทศโดยไม่ได้รับอนุญาต	ใช่
A.10.9.3 สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ (Publicly Available Information)	ต้องกำหนดให้มีการป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ	ใช่
A.10.10 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)	**เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต**	
A.10.10.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit Logging)	ต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้ การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้	ใช่
A.10.10.2 การตรวจสอบการใช้งานระบบ (Monitoring System Use)	ต้องกำหนดให้มีขั้นตอนปฏิบัติ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ อาทิ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่	ใช่
A.10.10.3 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of Log Information)	ต้องกำหนดให้มีมาตรการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต	ใช่
A.10.10.4 บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and Operator Logs)	ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่นๆ	ใช่
A.10.10.5 การบันทึกเหตุการณ์ข้อผิดพลาด (Fault Logging)	ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร	ใช่
A.10.10.6 การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock Synchronization)	ต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก	ใช่
A.11 การควบคุมการเข้าถึง (Access Control)		
A.11.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)	**เพื่อควบคุมการเข้าถึงสารสนเทศ**	
A.11.1.1 นโยบายการควบคุมการเข้าถึงระบบ (Access Control Policy)	ต้องกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ	ใช่

หัวข้อและมาตรการ	คำอธิบาย	ความสอดคล้อง (ใช่/ไม่ใช่)
A.11.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management)	**เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต**	
A.11.2.1 การลงทะเบียนพนักงาน (User Registration)	ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป หรือเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น	ใช่
A.11.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege Management)	ต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน	ใช่
A.11.2.3 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)	ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย	ใช่
A.11.2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)	ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้	ใช่
A.11.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)	**เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ**	
A.11.3.1 การใช้งานรหัสผ่าน (Password Use)	ต้องกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน	ใช่
A.11.3.2 การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended User Equipment)	ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล	ใช่
A.11.3.3 ควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy)	มีการจัดทำนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย เช่น สามารถเข้าถึงได้ทางกายภาพ อยู่ในบริเวณที่เป็นที่สาธารณะหรือพบเห็นได้ง่าย เป็นต้น	ใช่
A.11.4 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)	**เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต**	
A.11.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on Use of Network Services)	ต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้	ใช่
A.11.4.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User Authentication for External Connections)	ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้	ใช่
A.11.4.3 การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment Identification in Networks)	ต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว	ใช่
A.11.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)	ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย	ใช่
A.11.4.5 การแบ่งแยกเครือข่าย (Segregation in Networks)	ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ	ใช่
A.11.4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)	ต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอพพลิเคชั่นที่ใช้งานทางธุรกิจได้ระบุไว้	ใช่

หัวข้อและมาตรการ	คำอธิบาย	ความสอดคล้อง (ใช่/ไม่ใช่)
A.11.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network Routing Control)	ต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง	ใช่
A.11.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)	**เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต**	
A.11.5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure Log-On Procedures)	ต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ	ใช่
A.11.5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User Identification and Authentication)	ต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ	ใช่
A.11.5.3 ระบบบริหารจัดการรหัสผ่าน (Password Management System)	ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ	ใช่
A.11.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of System Utilities)	ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว	ใช่
A.11.5.5 การหมดเวลาการใช้งานระบบสารสนเทศ (Session Time-Out)	ต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้	ใช่
A.11.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)	ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง	ใช่
A.11.6 การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and Information Access Control)	**เพื่อป้องกันการเข้าถึงสารสนเทศของแอพพลิเคชันโดยไม่ได้รับอนุญาต**	
A.11.6.1 การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)	ต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของแอพพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน	ใช่
A.11.6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive System Isolation)	ต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ	ใช่
A.11.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Tele-Working)	**เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร**	
A.11.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile Computing and Communications)	ต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้	ใช่
A.11.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Tele-Working)	ต้องกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน	ใช่
A.12 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development, and Maintenance)		
A.12.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)	**เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ**	
A.12.1.1 การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Requirements Analysis and Specification)	ต้องวิเคราะห์และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่ หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว	ใช่

หัวข้อและมาตรการ	คำอธิบาย	ความสอดคล้อง (ใช่/ไม่ใช่)
A.12.2 การประมวลผลสารสนเทศในแอพพลิเคชัน (Correct Processing in Applications)	**เพื่อป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศ การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งานสารสนเทศผิดวัตถุประสงค์**	
A.12.2.1 การตรวจสอบข้อมูลนำเข้า (Input Data Validation)	ต้องกำหนดกลไกสำหรับตรวจสอบข้อมูลนำเข้าของแอพพลิเคชันว่าข้อมูลนั้นมีความถูกต้องและเหมาะสมก่อนที่จะนำไปประมวลผลต่อไป	ใช่
A.12.2.2 การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล (Control of Internal Processing)	ต้องกำหนดกลไกสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่ เช่น อาจมีสาเหตุจากความผิดพลาดในการประมวลผล การกระทำโดยเจตนาของผู้ที่เกี่ยวข้อง เป็นต้น	ใช่
A.12.2.3 การตรวจสอบความถูกต้องของข้อความ (Message Integrity)	ต้องระบุข้อกำหนดสำหรับการตรวจสอบความถูกต้องของข้อความสำหรับแอพพลิเคชัน (เพื่อให้สามารถตรวจสอบได้ว่าเป็นข้อความต้นฉบับที่ถูกต้อง) รวมทั้งกำหนดมาตรการรองรับเพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อความนั้นโดยไม่ได้รับอนุญาต	ใช่
A.12.2.4 การตรวจสอบข้อมูลนำออก (Output Data Validation)	ต้องกำหนดกลไกสำหรับการตรวจสอบข้อมูลนำออกจากแอพพลิเคชันเพื่อเป็นการทบทวนว่าการประมวลผลของสารสนเทศที่เกี่ยวข้องเป็นไปอย่างถูกต้องและเหมาะสม	ใช่
A.12.3 มาตรการการเข้ารหัสข้อมูล (Cryptographic Controls)	**เพื่อรักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยใช้วิธีการการเข้ารหัสข้อมูล**	
A.12.3.1 นโยบายการใช้งานการเข้ารหัสข้อมูล (Policy on The Use of Cryptographic Controls)	ต้องกำหนดให้มีนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูล และให้มีผลบังคับใช้งานภายในองค์กร	ใช่
A.12.3.2 การบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key Management)	ต้องกำหนดให้มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล โดยกุญแจเหล่านี้จะใช้งานร่วมกับเทคนิคการเข้ารหัสข้อมูลที่กำหนดเป็นมาตรฐานขององค์กร	ใช่
A.12.4 การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (Security of System Files)	**เพื่อสร้างความมั่นคงปลอดภัยให้กับไฟล์ต่างๆ ของระบบที่ให้บริการ**	
A.12.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of Operational Software)	ต้องจัดให้มีขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงไปยังระบบที่ให้บริการ ทั้งนี้ เพื่อลดความเสี่ยงที่จะทำให้ระบบให้บริการนั้นเกิดความเสียหายทำงานผิดปกติ หรือไม่สามารถใช้งานได้	ใช่
A.12.4.2 การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ (Protection of System Test Data)	ต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่ใช้งานอยู่บนระบบให้บริการสำหรับทำการทดสอบระบบ หากมีความจำเป็นต้องใช้ ต้องกำหนดให้มีการป้องกันและควบคุมการใช้งาน เช่น ควรลบทิ้งบางส่วนของข้อมูลที่เป็นความลับ ข้อมูลส่วนตัว หรือข้อมูลสำคัญ	ใช่
A.12.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access Control to Program Source Code)	ต้องจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ ทั้งนี้เพื่อป้องกันการเปลี่ยนแปลงที่อาจเกิดขึ้นโดยไม่ได้รับอนุญาต หรือโดยไม่ได้เจตนา	ใช่
A.12.5 การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน (Security in Development and Support Processes)	**เพื่อรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และสารสนเทศของระบบ**	
A.12.5.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change Control Procedures)	ต้องกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศ ทั้งนี้เพื่อลดความเสี่ยงที่จะทำให้ระบบเกิดความเสียหาย ทำงานผิดปกติ หรือไม่สามารถใช้งานได้	ใช่

หัวข้อและมาตรการ	คำอธิบาย	ความสอดคล้อง (ใช่/ไม่ใช่)
A.12.5.2 การตรวจสอบการทำงานของแอพพลิเคชันภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications after Operating System Changes)	ต้องทำการตรวจสอบทางเทคนิคภายหลังจากที่ทำการเปลี่ยนแปลงระบบปฏิบัติการเพื่อดูว่าแอพพลิเคชันที่ทำงานอยู่บนระบบปฏิบัติการนั้น ทำงานผิดปกติ ไม่สามารถใช้งานได้ หรือมีปัญหาทางด้านความมั่นคงปลอดภัยเกิดขึ้นหรือไม่	ใช่
A.12.5.3 การจำกัดการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต (Restrictions on Changes to Software Packages)	ต้องหลีกเลี่ยงการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต หากจำเป็นต้องแก้ไข ต้องแก้ไขตามความจำเป็นเท่านั้น และต้องมีการควบคุมการแก้ไขนั้นอย่างเข้มงวดด้วย	ใช่
A.12.5.4 การป้องกันการรั่วไหลของสารสนเทศ (Information Leakage)	ต้องกำหนดมาตรการเพื่อป้องกันการรั่วไหลของสารสนเทศขององค์กร หรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหลออกไป	ใช่
A.12.5.5 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development)	ต้องกำหนดมาตรการเพื่อควบคุมและตรวจสอบการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก	ใช่
A.12.6 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)	**เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆ**	
A.12.6.1 มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of Technical Vulnerabilities)	ต้องกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ ที่ใช้งาน ประเมินความเสี่ยงของช่องโหว่เหล่านั้น รวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว	ใช่
A.13 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information Security Incident Management)		
A.13.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events and Weaknesses)	**เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม**	
A.13.1.1 การรายงานเหตุการณ์ที่เกียวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events)	ต้องทำการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร โดยผ่านช่องทางการรายงานที่กำหนดไว้ และต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้	ใช่
A.13.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting Security Weaknesses)	ต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่	ใช่
A.13.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of Information Security Incidents and Improvement)	**เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม**	
A.13.2.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)	ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนเพื่อปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยขององค์กร และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี	ใช่
A.13.2.2 การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from security incidents)	(ผู้ดูแลระบบ) ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหายเพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า	ใช่
A.13.2.3 การเก็บรวบรวมหลักฐาน (Collection of Evidence)	ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา	ใช่

หัวข้อและมาตรการ	คำอธิบาย	ความสอดคล้อง (ใช่/ไม่ใช่)
A.14 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)		
A.14.1 หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Information Security Aspects of Business Continuity Management)	**เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆ ทางธุรกิจ เพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม**	
A.14.1.1 กระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ (Including Information Security in The Business Continuity Management Process)	ต้องกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ การบริหารจัดการและการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอ กระบวนการนี้จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับธุรกิจ	ใช่
A.14.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business Continuity and Risk Assessment)	ต้องระบุเหตุการณ์ที่สามารถทำให้ธุรกิจขององค์กรเกิดการติดขัดหรือหยุดชะงัก โอกาสที่จะเกิดขึ้น ผลกระทบที่เป็นไปได้ รวมทั้งผลที่เกิดขึ้นต่อความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร	ใช่
A.14.1.3 การจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ (Developing and Implementing Continuity Plans Including Information Security)	ต้องจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจและการดำเนินงานต่างๆ ให้สามารถดำเนินต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ ภายหลังจากที่มีเหตุการณ์ที่ทำให้ธุรกิจเกิดการติดขัด หยุดชะงัก หรือล้มเหลว	ใช่
A.14.1.4 การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ (Business Continuity Planning Framework)	ต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ เพื่อให้แผนงานที่เกี่ยวข้องทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดทางด้านความมั่นคงปลอดภัยที่กำหนดไว้ และจัดลำดับความสำคัญของงานต่างๆ ที่ต้องดำเนินการ	ใช่
A.14.1.5 การทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ (Testing, Maintaining and Re-Assessing Business Continuity Plans)	ต้องกำหนดให้มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจอย่างสม่ำเสมอ เพื่อให้แผนมีความทันสมัยและได้ผลเป็นอย่างดี	ใช่
A.15 การปฏิบัติตามข้อกำหนด (Compliance)		
A.15.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with Legal Requirements)	**เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ**	
A.15.1.1 การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย (Identification of Applicable Legislation)	ต้องระบุข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) ที่เกี่ยวข้องกับการดำเนินงานหรือธุรกิจขององค์กร ต้องบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร และปรับปรุงข้อกำหนดเหล่านั้นให้ทันสมัยอยู่เสมอ รวมทั้งกำหนดแนวทางการปฏิบัติเพื่อให้สอดคล้องกับข้อกำหนดดังกล่าว	ใช่
A.15.1.2 การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual Property Rights (IRP))	ต้องกำหนดขั้นตอนปฏิบัติเพื่อป้องกันการละเมิดสิทธิหรือทรัพย์สินทางปัญญา ขั้นตอนปฏิบัติดังกล่าวต้องกำหนดหรือควบคุมให้ปฏิบัติตามข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) รวมทั้งข้อกำหนดในการใช้งานผลิตภัณฑ์ซอฟต์แวร์จากผู้ขายด้วย	ใช่
A.15.1.3 การป้องกันข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร (Protection of Organizational Records)	ต้องกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจ จากการสูญหาย การถูกทำลายให้เสียหาย และการปลอมแปลง	ใช่
A.15.1.4 การป้องกันข้อมูลส่วนตัว (Data Protection and Privacy of Personal Information)	ต้องกำหนดให้มีการป้องกันข้อมูลส่วนตัวตามที่ระบุหรือกำหนดไว้ในกฎหมาย ระเบียบปฏิบัติ และข้อสัญญาที่เกี่ยวข้อง	ใช่

หัวข้อและมาตรการ	คำอธิบาย	ความสอดคล้อง (ใช่/ไม่ใช่)
A.15.1.5 การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of Misuse of Information Processing Facilities)	ต้องป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ประมวลผลสารสนเทศขององค์กรผิดวัตถุประสงค์หรือโดยไม่ได้รับอนุญาต	ใช่
A.15.1.6 การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด (Regulation of Cryptographic Controls)	ต้องกำหนดให้ใช้มาตรการการเข้ารหัสข้อมูลโดยให้ยึดถือตาม หรือต้องสอดคล้องกับข้อตกลง กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง	ใช่
A.15.2 การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัย และข้อกำหนดทางเทคนิค (Compliance with Security Policies and Standards, and Technical Compliance)	**เพื่อให้ระบบเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร**	
A.15.2.1 การปฏิบัติตามนโยบายและมาตรฐานความมั่นคงปลอดภัย (Compliance with Security Policies and Standards)	ต้องกำหนดให้ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร	ใช่
A.15.2.2 การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร (Technical Compliance Checking)	ต้องกำหนดให้มีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอ เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคขององค์กร	ใช่
A.15.3 การตรวจประเมินระบบสารสนเทศ (Information Systems Audit Considerations)	**เพื่อให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด**	
A.15.3.1 มาตรการการตรวจประเมินระบบสารสนเทศ (Information Systems Audit Controls)	ต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบสารสนเทศขององค์กร เพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจ เช่น การหยุดชะงักของกระบวนการทางธุรกิจในระหว่างที่ทำการตรวจประเมิน	ใช่
A.15.3.2 การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of Information Systems Audit Tools)	ต้องกำหนดให้มีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (เช่น ซอฟต์แวร์ที่ใช้ในการตรวจประเมิน) เพื่อป้องกันการใช้งานผิดวัตถุประสงค์ หรือการเปิดเผยข้อมูลการตรวจประเมินโดยไม่ได้รับอนุญาต	ใช่

ที่มา: จากการสัมภาษณ์

การบริหารจัดการบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารด้วยหลักการ PDCA

ธนาคารได้นำหลักการของ PDCA ที่ได้ระบุไว้ในมาตรฐาน ISO/IEC 27001:2005 เข้ามาประยุกต์ใช้ในการบริหารจัดการบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคาร เพื่อให้การปฏิบัติงานในทุกขั้นตอนที่เกี่ยวข้องกับบริการดังกล่าว ตั้งแต่การเริ่มต้นสร้างระบบ การดูแลรักษาระบบ จนกระทั่งการปรับปรุงและพัฒนาระบบให้มีประสิทธิภาพและมีความปลอดภัยสูงขึ้น มีขั้นตอนการทำงานที่ชัดเจน เป็นระเบียบแบบแผน สามารถตรวจสอบได้ อันจะนำไปสู่การพัฒนาบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารอย่างต่อเนื่อง (Continuous Improvement) ในที่สุด

ทั้งนี้ ขั้นตอนในการดำเนินงานตามหลักการของ PDCA ในส่วนของการบริหารจัดการบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารมีรายละเอียดดังต่อไปนี้

Plan

- กำหนดความต้องการของระบบในด้านต่างๆ ไม่ว่าจะเป็นเรื่องของฟังก์ชั่นการทำงานของระบบ ทรัพยากรระบบ ประสิทธิภาพของระบบ และความปลอดภัยของระบบ เป็นต้น
- กำหนดหน้าที่และความรับผิดชอบของบุคลากรแต่ละคน
- วางแผนการทำงานในแต่ละขั้นตอนอย่างชัดเจน
- มีการวางแผนการแก้ไขปัญหาล่วงหน้ากรณีที่เกิดเหตุการณ์ที่อาจมีผลกระทบต่อการพัฒนาระบบ

Do

- มีการประเมินความเสี่ยงและบริหารความเสี่ยงอย่างเหมาะสม
- จัดทำเอกสารประกอบการทำงานในแต่ละขั้นตอนอย่างเหมาะสม
- มีการฝึกอบรมบุคลากรที่มีหน้าที่ให้ความช่วยเหลือลูกค้าในกรณีที่ลูกค้าไม่สามารถใช้งานระบบได้
- มีการฝึกอบรมบุคลากรที่มีหน้าที่แก้ไขปัญหาในกรณีที่เกิดเหตุการณ์ผิดปกติต่างๆขึ้นกับระบบ
- ให้ความรู้เรื่องของความปลอดภัยข้อมูลสารสนเทศแก่บุคลากรที่เกี่ยวข้องทุกคน

Check

- มีการทดสอบระบบในระดับต่างๆอย่างสม่ำเสมอ เช่น Unit Test, Application Test, Regression Test, Performance Test, Security Test, และ User Acceptance Test เป็นต้น
- มีการตรวจประเมินระบบโดยผู้ตรวจสอบระบบที่เป็นบุคลากรของธนาคาร
- มีการตรวจสอบความปลอดภัยของระบบโดยหน่วยงานภายนอกธนาคาร
- เฝ้าระวังและตรวจสอบการทำงานของระบบอย่างสม่ำเสมอ

- ทบทวนระบบโดยผู้บริหาร (Project Sponsor) และเจ้าของระบบ (Project Owner) อย่างสม่ำเสมอ

Act

- วิเคราะห์สาเหตุของปัญหาเพื่อหาวิธีแก้ไขและป้องกันไม่ให้เกิดปัญหาดังกล่าวขึ้นในอนาคต
- ดำเนินการแก้ไขปรับปรุงระบบตามที่ได้ทดสอบและตรวจประเมินระบบ
- จัดทำรายงานการแก้ไขปรับปรุงระบบอย่างเหมาะสม
- บำรุงรักษาระบบเพื่อให้สามารถให้บริการได้อย่างต่อเนื่อง
- จัดทำคู่มือในการบำรุงรักษาระบบอย่างเหมาะสม
- พัฒนาระบบให้มีประสิทธิภาพและความปลอดภัยสูงขึ้น