ธนาคารแห่งประเทศไทย

SA-IT Examination Guideline

แนวทางการตรวจสอบด้านเทคโนโลยีสารสนเทศ

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สายกำกับระบบการชำระเงินและคุ้มครองผู้ใช้บริการทางการเงิน

ทบทวนล่าสุด มิถุนายน 2567

ประวัติการปรับปรุงเอกสาร

วันที่	เวอร์ชัน	ชื่อผู้จัดทำ/แก้ไข	รายละเอียด
ก.ย. 2556	1.0	ฝ่ายตรวจสอบเทคโนโลยีสารสนเทศ	ฉบับแรก
มิ.ย. 2567	2.0	ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ	ปรับปรุงเนื้อหาให้สอดคล้องกับประกาศหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สารบัญ

Executive Summary

ที่มาและเหตุผลความจำเป็น

สายกำกับสถาบันการเงิน (สกส.) ได้ปรับปรุงแนวทางการตรวจสอบแบบเน้นธุรกรรมที่มีนัยสำคัญ (Significant Activities - SA) โดยระบบเทคโนโลยีสารสนเทศ (IT) ถือเป็น SA หนึ่ง (SA-IT) ของการตรวจสอบสถาบันการเงิน (สง.)

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ฝตท.) จึงได้พัฒนาแนวทางการตรวจสอบ SA-IT ให้สอดคล้องตามกรอบหลักการมาตรฐานสากล รวมถึงปรับปรุงปัจจัยที่ใช้ในการประเมินระดับความเสี่ยงที่มีอยู่ (Inherent Risk - IR) และประเมินคุณภาพการจัดการความเสี่ยง (Quality of Risk Management - QRM) ของ SA-IT เพื่อใช้เป็นแนวทางในการประเมินระดับความเสี่ยงด้าน IT ของ สง.

สรุปกรอบเนื้อหา

สาระสำคัญของแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ แบ่งออกเป็น 5 ส่วน คือ

1. คำจำกัดความของระบบ IT และโครงสร้างระบบ IT ที่สำคัญของสถาบันการเงิน ได้แก่ ศูนย์คอมพิวเตอร์ (Data Center) ระบบเครือข่ายสื่อสาร (Network) ระบบ Core Banking ระบบงานการให้บริการแก่ลูกค้า

2. การประเมิน Inherent Risk (IR) ซึ่งเป็นความเสี่ยงที่มีอยู่ในระบบ IT ที่ใช้รองรับกระบวนการดำเนินธุรกิจด้านต่าง ๆ ดังนี้

2.1 ความเสี่ยงด้านปฏิบัติการ (Operational Risk) พิจารณาครอบคลุมถึงการพัฒนาหรือปรับปรุงด้านการรักษาความปลอดภัยของโครงสร้างพื้นฐานหรือระบบ IT การใช้บริการ IT Outsourcing ที่สำคัญจากผู้ให้บริการภายนอกทั้งในประเทศและต่างประเทศ และการเชื่อมโยงเครือข่าย/ระบบงานกับภายนอก การนำอุปกรณ์ส่วนตัวเชื่อมต่อเข้าเครือข่าย/ระบบงานของธนาคาร การพัฒนาหรือเปลี่ยนแปลงระบบงานที่สำคัญหรือเกี่ยวข้องกับการให้บริการลูกค้า/การทำธุรกรรมการเงินของลูกค้า ความซับซ้อนของระบบ IT การใช้เทคโนโลยีสมัยใหม่ที่ยังไม่ได้รับการรับรองตามมาตรฐาน ความพร้อมของศูนย์คอมพิวเตอร์หลักและศูนย์สำรอง ระบบเครือข่ายสื่อสารและอุปกรณ์เครือข่ายยังมีจุดที่เป็น single point of failure ความพร้อมของระบบงานที่ใช้รองรับการประมวลผลได้อย่างต่อเนื่องตามความต้องการของหน่วยงานธุรกิจทั้งในภาวะปกติและภาวะฉุกเฉิน

2.2 ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) พิจารณาครอบคลุมถึงนโยบาย/แผนกลยุทธ์ และการจัดสรรงบประมาณโครงการด้าน IT ที่สำคัญสอดคล้องกับเป้าหมายเชิงกลยุทธ์ทางธุรกิจ

3. การประเมิน Quality of Risk Management (QRM) เพื่อให้ สง. มีระบบการบริหารจัดการความเสี่ยงที่มีประสิทธิภาพ เพื่อสามารถลดหรือควบคุมความเสี่ยงที่มีอยู่ของระบบ IT โดยมี QRM ใน 2 ระดับ ดังนี้

3.1 ระดับ Operational Management (OM) เป็นการควบคุมเพื่อจัดการความเสี่ยงที่มีอยู่ของการปฏิบัติงานประจำวัน (Day-to-Day Operation) โดยการประเมินครอบคลุมตามกรอบหลักการ Security - Integrity - Availability (SIA) เพื่อให้ระบบ IT ของ สง. มีการรักษาความปลอดภัยที่เพียงพอและสอดคล้องตามมาตรฐาน มีความถูกต้องและความน่าเชื่อถือ และมีความพร้อมใช้งาน

3.2 ระดับ Oversight Functions (OF) ใน 5 ด้าน ได้แก่ คณะกรรมการ สง. ผู้บริหารระดับสูง งานบริหารความเสี่ยง งานกำกับการปฏิบัติตามกฎเกณฑ์ และงานตรวจสอบภายใน เพื่อให้เกิดความมั่นใจว่า สง. มีการกำกับดูแล การดำเนินงานและการบริหารความเสี่ยงด้าน IT ที่เหมาะสมสอดคล้องกับมาตรฐานและแนวปฏิบัติที่ดี

4. การประเมิน Net Risk ซึ่งเป็นความเสี่ยงสุทธิของระบบ IT ที่คงเหลืออยู่ ภายหลังจากการบริหารจัดการ Inherent Risk แล้ว

5. การประเมินแนวโน้มความเสี่ยง (Direction of Net Risk) ซึ่งเป็นโอกาสที่ความเสี่ยงสุทธิของระบบ IT จะเปลี่ยนแปลงไปจากเดิมที่ได้ประเมินไว้ในอีก 1 ปีข้างหน้า จากการเปลี่ยนแปลงของความเสี่ยงที่มีอยู่ (IR) ของระบบ IT และ/หรือคุณภาพการบริหารจัดการความเสี่ยง (QRM)

ประโยชน์ของการจัดทำแนวทางการตรวจสอบ

ฝตท. มุ่งหวังให้แนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศนี้เกิดประโยชน์ในวงกว้าง โดยดำเนินการเผยแพร่ใน Web Portal ของ สกส. เพื่อเป็นแหล่งข้อมูลให้ผู้ตรวจสอบด้าน IT ของ ธปท. สามารถ download ไปใช้ในการปฏิบัติงาน และเพื่อให้คณะทำงาน FSAP สกส. สามารถใช้อ้างอิงในการประเมิน FSAP การกำกับดูแล สง. ด้าน IT ต่อไป

ส่วนที่ 1 ระบบเทคโนโลยีสารสนเทศ (Information Technology)

1.1 คำจำกัดความ

ระบบเทคโนโลยีสารสนเทศ (IT) หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ข้อมูลสารสนเทศ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

1.2 โครงสร้างระบบ IT ที่สำคัญ

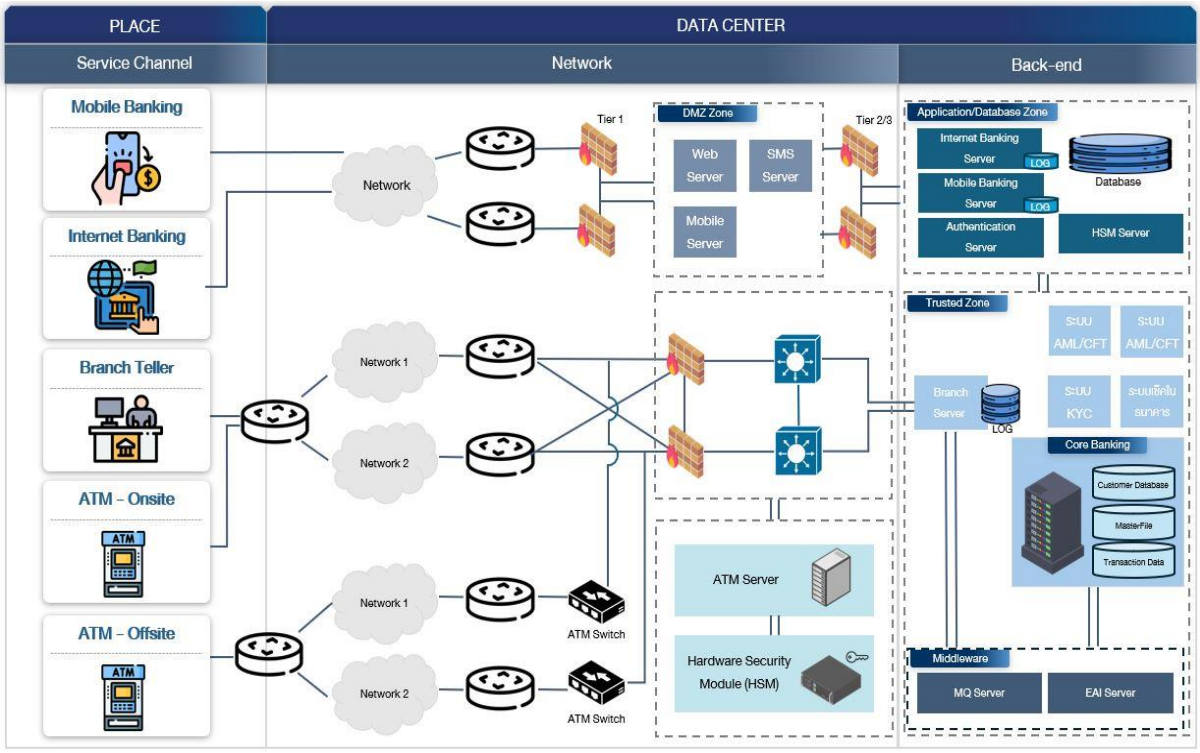
ศูนย์คอมพิวเตอร์ (Data Center) ศูนย์รวมของเครื่องและอุปกรณ์คอมพิวเตอร์สำคัญของธนาคารที่ใช้ประมวลผลกลางรองรับการดำเนินธุรกิจและการให้บริการของธนาคาร เช่น ระบบ Core Banking เป็นต้น

ระบบเครือข่ายสื่อสาร (Network) ระบบเครื่องมือสื่อสารที่ใช้รองรับการเชื่อมโยงเครื่องคอมพิวเตอร์ อุปกรณ์ ระบบงาน และช่องทางบริการจากที่ต่าง ๆ เข้าหากัน

ระบบ Core Banking ระบบประมวลผลกลางที่มีความสำคัญอย่างยิ่งสำหรับรองรับการประมวลผลธุรกรรมหลักของธนาคาร เช่น ธุรกรรมฝาก ถอน และโอนเงิน รวมทั้งสามารถรองรับการทำธุรกรรมจากช่องทางต่าง ๆ ของธนาคาร เช่น สาขา, ATM, Internet Banking และ Mobile Banking เป็นต้น

ระบบงานการให้บริการแก่ลูกค้า เครื่องคอมพิวเตอร์ อุปกรณ์ หรือระบบที่ใช้รับรายการธุรกรรมของลูกค้าเพื่อส่งไปประมวลผลที่ระบบประมวลผลกลาง เช่น ระบบงานสาขา เครื่องคอมพิวเตอร์ที่เจ้าหน้าที่สาขาใช้ปฏิบัติงาน ระบบงาน ATM/ตู้ ATM ระบบ Internet Banking และระบบ Mobile Banking เป็นต้น

1.3 แผนภาพแสดง High-Level IT System Process Flow



ส่วนที่ 2 การประเมิน Inherent Risk (IR)

2.1 คำจำกัดความ

Inherent Risk (IR) หมายถึง ความเสี่ยงที่มีอยู่ในระบบ IT ที่ใช้รองรับกระบวนการดำเนินธุรกิจด้านต่าง ๆ (Business Process) ที่อาจก่อให้เกิดความสูญเสียจากปัจจัยภายในและภายนอก ที่อาจส่งผลกระทบต่อรายได้และเงินกองทุนของ สง.

2.2 หลักการพิจารณา

1. ลักษณะโครงสร้างพื้นฐานและระบบงาน IT

2. ปัจจัยที่ก่อให้เกิดความเสี่ยง (Risk Factors & Risk Drivers) จากระบบ IT

3. ผลกระทบจากสภาพแวดล้อมต่อระดับความเสี่ยงของ Inherent Risk

ทั้งนี้ การประเมิน IR จะประเมินเฉพาะความเสี่ยงหลักที่มีผลกระทบต่อโครงสร้างพื้นฐานและระบบงาน IT เท่านั้น ได้แก่

1. ความเสี่ยงด้านปฏิบัติการ

2. ความเสี่ยงด้านกลยุทธ์ (ประเมินเฉพาะเมื่อมีระบบงานใหม่หรือการเปลี่ยนแปลงที่มีนัยสำคัญ)

2.2.1 ปัจจัยการประเมิน IR ด้านปฏิบัติการ

ปัจจัยที่ใช้พิจารณา	การประเมินระดับ IR Operational		
	ต่ำ	ปานกลาง	สูง
1. Security			
1.1 การพัฒนาหรือปรับปรุงด้านการรักษาความปลอดภัยของโครงสร้างพื้นฐานหรือระบบ IT ให้เทียบเคียงกับมาตรฐานสากล	ธนาคารมีแผนงานและกรอบแนวทางในการยกระดับด้าน IT Security ขององค์กร (Enterprise Security) ทั้งระยะสั้นและระยะยาวที่มีความชัดเจน และมีการอ้างอิง/สอดคล้องกับมาตรฐานสากล เช่น TIA-942, ISO27001 เป็นต้น ● ข้อสังเกตที่ตรวจพบไม่ส่งผลเสียหาย หรือเป็นข้อสังเกตที่สามารถแก้ไขให้สำเร็จเป็นรูปธรรมได้	● ธนาคารมีแผนงานการพัฒนาด้าน IT Security เพื่อยกระดับ IT Security ส่วนที่มีความสำคัญหรือให้เป็นตามเกณฑ์/ข้อกำหนดของทางการ แต่ยังไม่พบว่ามีแผน Enterprise Security ในระยะยาวที่ชัดเจน ● ข้อสังเกตที่ตรวจพบมีความเสี่ยงระดับปานกลาง หรือเป็นข้อสังเกตที่เมื่อดำเนินการแก้ไขแล้วต้องติดตามผลในทางปฏิบัติในระยะยาวเพื่อเห็นผลลัพธ์ที่เป็นรูปธรรม	● แผนงานการพัฒนาด้าน IT Security ยังไม่ชัดเจนมากนัก รวมทั้งยังไม่พบว่ามีแผนการปรับปรุง IT Security ในระยะยาว ● ข้อสังเกตที่ตรวจพบมีความเสี่ยงสูง และส่งผลเสียหายต่อองค์กร เช่น Data Breach, Hack, Reputation Risk เป็นต้น หรือเป็นข้อสังเกตที่ต้องปรับปรุงแก้ไขที่กระบวนการดำเนินการ
1.2 การใช้บริการ 3rd Party ในส่วนที่เป็นระบบที่รองรับการให้บริการธุรกิจหลัก หรือผู้ให้บริการภายนอกทั้งในประเทศและต่างประเทศและการเชื่อมโยงเครือข่าย/ระบบงานกับภายนอก (เช่น ระบบ Core Banking, ระบบ Mobile Banking, Data Center Operation, Cloud Computing เป็นต้น)	● ไม่มีการใช้บริการ 3rd Party ในส่วนที่เป็นระบบที่รองรับการให้บริการธุรกิจหลัก	● มีการใช้บริการ 3rd Party หรือมีการเชื่อมโยงระบบกับภายนอก แต่ไม่ใช่ระบบที่รองรับการให้บริการธุรกิจหลัก และไม่ส่งผลกระทบต่อการให้บริการการเงินแก่ลูกค้า รวมทั้งไม่มีการส่งข้อมูลลูกค้าไปจัดเก็บไว้ภายนอก ● พบ incident ที่เกี่ยวข้องกับผู้ให้บริการภายนอก แต่ไม่ส่งผลกระทบต่อความปลอดภัย ความถูกต้องของข้อมูล และความต่อเนื่องในการให้บริการแก่ลูกค้า หรือส่งผลกระทบต่อระบบงานอื่น	● มีการใช้บริการ 3rd Party หรือมีการเชื่อมโยงระบบกับภายนอกในส่วนที่เป็นระบบรองรับการให้บริการธุรกิจหลักและมีการส่งข้อมูลความสำคัญ เช่น ข้อมูลส่วนบุคคลของลูกค้า ไปประมวลผลและจัดเก็บไว้ภายนอก ● พบ incident ที่เกี่ยวข้องกับผู้ให้บริการภายนอก ซึ่งส่งผลต่อความปลอดภัย ความถูกต้องของข้อมูลที่จัดเก็บไว้ภายนอก และความต่อเนื่องในการให้บริการแก่ลูกค้า หรือส่งผลกระทบต่อระบบงานอื่นในลักษณะ domino effect
1.3 การนำอุปกรณ์ส่วนตัวเชื่อมต่อเข้าเครือข่าย/ระบบงานของธนาคาร (Bring Your Own Device : BYOD)	● ไม่อนุญาตให้พนักงานนำอุปกรณ์ส่วนตัวเชื่อมต่อเข้าเครือข่าย/ระบบงานของธนาคารได้	● มีการอนุญาตให้พนักงานบางรายเฉพาะที่มีความจำเป็นต้องใช้อุปกรณ์ส่วนตัวเชื่อมต่อเข้าเครือข่าย/ระบบงานของธนาคาร แต่ไม่มีข้อมูลของลูกค้าหรือข้อมูลสำคัญของธนาคารที่อาจส่งผลกระทบให้เกิดความเสียหายได้	● มีการอนุญาตให้พนักงานทุกคนสามารถใช้อุปกรณ์ส่วนตัวเชื่อมต่อเข้าเครือข่าย/ระบบงานของธนาคารได้

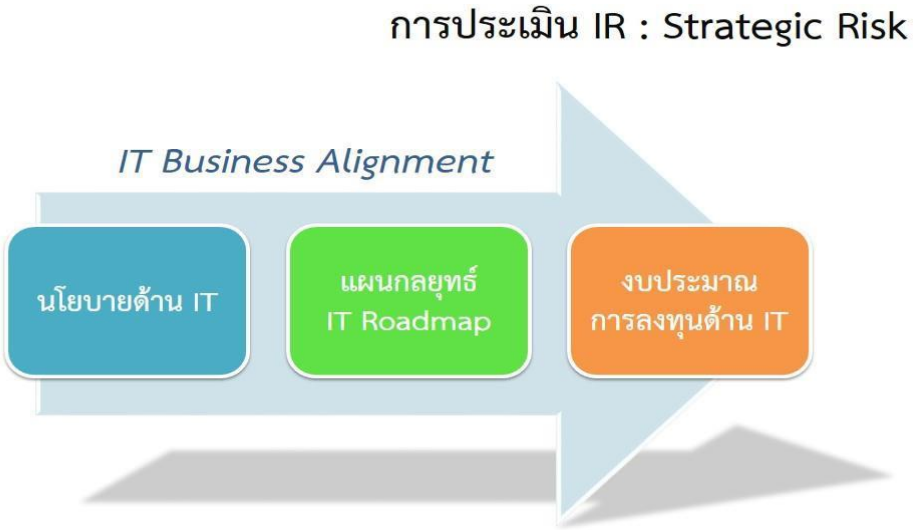
ปัจจัยที่ใช้พิจารณา	การประเมินระดับ IR Operational		
	ต่ำ	ปานกลาง	สูง
1.4 Incidents/Loss/ Complaint related to Security	● ไม่พบว่ามี Incident/ความเสียหาย/ข้อร้องเรียน เกี่ยวกับการถูกบุกรุก/เจาะระบบงาน/หรือโจรกรรมข้อมูลลูกค้าหรือข้อมูลธุรกรรมทางการเงินในปีที่ผ่านมา	● พบว่ามี Incident/ความเสียหาย/ข้อร้องเรียน เกี่ยวกับการถูกบุกรุก/เจาะระบบงาน/หรือโจรกรรมข้อมูลลูกค้าหรือข้อมูลธุรกรรมทางการเงินที่ส่งผลกระทบต่อลูกค้าบางรายในวงจำกัด และไม่ส่งผลกระทบต่อชื่อเสียงของธนาคาร	● พบว่ามี Incident/ความเสียหาย/ข้อร้องเรียน เกี่ยวกับการถูกบุกรุก/เจาะระบบงาน/หรือโจรกรรมข้อมูลลูกค้าหรือข้อมูลธุรกรรมทางการเงินที่ส่งผลกระทบต่อลูกค้าลูกค้าในวงกว้าง และส่งผลกระทบต่อชื่อเสียงของธนาคาร
2. Integrity			
2.1 การพัฒนาหรือเปลี่ยนแปลงระบบงานที่สำคัญหรือเกี่ยวข้องกับการให้บริการลูกค้า/การทำธุรกรรมการเงินของลูกค้าวงกว้าง	● ไม่มีการเปลี่ยนแปลงที่มีนัยสำคัญ มีเพียงการปรับปรุงเล็กน้อย เช่น การเปลี่ยนรูปลักษณ์หน้าจอแสดงผล การเพิ่ม Feature/Function เล็กน้อย เป็นต้น ● ไม่มีการเปลี่ยนแปลงโครงสร้างระบบงาน การประมวลผล หรือเปลี่ยนอุปกรณ์ Hardware ที่สำคัญ	● มีการเปลี่ยนแปลง/แก้ไขโปรแกรมระบบงานที่มีนัยสำคัญอยู่บ้าง เช่น การเปลี่ยน Program Version การแก้ไขข้อบกพร่อง (bug) เป็นต้น ● มีการเปลี่ยนแปลงอุปกรณ์ Hardware บางส่วนเพื่อทดแทนอุปกรณ์เดิม	● มีการพัฒนาหรือเปลี่ยนแปลงระบบงานที่สำคัญ เพื่อใช้ทดแทนระบบงานที่ใช้งานอยู่เดิม เนื่องจากมีความล้าสมัยหรือไม่สามารถรองรับการปรับเปลี่ยนตาม requirement ใหม่ๆ เพิ่มเติมของผู้ใช้งานได้ ● มีการเปลี่ยนแปลงโครงสร้างระบบงาน การประมวลผล หรือเปลี่ยนอุปกรณ์ Hardware ที่สำคัญที่ใช้รองรับระบบงานที่สำคัญหรือเกี่ยวข้องกับการให้บริการลูกค้า
2.2 ความซับซ้อนของระบบ IT เช่น ซ้ำซ้อน และยุ่งยากต่อการปรับเปลี่ยน มีระบบที่เกี่ยวข้อง	● โครงสร้างระบบ IT ไม่ซับซ้อน ใช้รูปแบบ platform เป็นมาตรฐานเดียวกัน อีกทั้งระบบงานที่เกี่ยวข้องมีการเชื่อมโยงระบบถึงกันแบบ Automated หรือเป็นลักษณะ Straight Through Process	● โครงสร้างระบบ IT มีความซับซ้อน ระบบงานมีการเชื่อมโยงข้อมูลกันบางส่วน แต่ยังมีการ rekey ข้อมูลบางส่วน ซึ่งอาจส่งผลให้ข้อมูลที่จัดเก็บแต่ละระบบไม่ตรงกันอยู่บ้าง แต่หากเกิดข้อผิดพลาดจะไม่ส่งผลกระทบต่อการปฏิบัติตามเกณฑ์ทางการ เช่น การรายงานข้อมูลเป็นต้น	● โครงสร้างระบบ IT มีความซับซ้อนมาก มีระบบงานที่เชื่อมโยงเกี่ยวข้องกันหลายระบบ และมีหลาย platform โดยไม่มีการเชื่อมโยงข้อมูลกัน ต้องมีการ rekey ข้อมูลหลายครั้ง จึงมีสัญญาณบ่งชี้ที่มีโอกาสเกิดความเสี่ยงจากการปฏิบัติงานผิดพลาด และส่งผลกระทบต่อความถูกต้องของข้อมูลตลอดจนมีความเสี่ยงต่อการรายงานข้อมูลไม่ถูกต้องตามเกณฑ์ทางการ
2.3 การใช้เทคโนโลยีสมัยใหม่ที่ยังไม่ได้รับการ	● มีการใช้เทคโนโลยี/ระบบงานที่เป็น Proven	● มีการใช้เทคโนโลยี/ระบบงานที่เป็น Unproven technology	● มีการใช้เทคโนโลยี/ระบบงานที่เป็น Unproven

ปัจจัยที่ใช้พิจารณา	การประเมินระดับ IR Operational		
	ต่ำ	ปานกลาง	สูง
รับรองตามมาตรฐาน (Unproven technology)	technology ซึ่งการพัฒนาผ่านขั้นตอนที่ได้รับการรับรองตามมาตรฐาน	ระบบงานที่ไม่สำคัญ และไม่ใช่ระบบที่ใช้รองรับการให้บริการธุรกิจหลัก และไม่ส่งผลกระทบต่อการให้บริการการเงินแก่ลูกค้า	technology สำหรับระบบที่ใช้รองรับการให้บริการธุรกิจหลัก หรือระบบที่ส่งผลกระทบต่อการให้บริการการเงินแก่ลูกค้า
2.4 Incidents/Loss/ Complaint related to data integrity	● ไม่พบว่ามี Incidents/ความเสียหาย/ข้อร้องเรียน ที่เกี่ยวกับระบบทำงานไม่ถูกต้อง หรือความผิดพลาดจากการปฏิบัติงานของพนักงานที่ส่งผลกระทบต่อความถูกต้องของข้อมูลลูกค้าหรือการทำธุรกรรม	● พบว่ามี Incidents/ความเสียหาย/ข้อร้องเรียน ที่เกี่ยวกับระบบทำงานไม่ถูกต้องโดยยังไม่ส่งผลต่อการปฏิบัติที่ไม่เป็นไปตามหลักเกณฑ์ของทางการ หรือเกิดความผิดพลาดจากการปฏิบัติงานของพนักงานที่ส่งผลกระทบต่อความถูกต้องของข้อมูลลูกค้าหรือการทำธุรกรรม แต่อยู่ในวงจำกัด และไม่ส่งผลกระทบต่อชื่อเสียงของธนาคาร	● พบว่ามี Incidents/ความเสียหาย/ข้อร้องเรียน ที่เกี่ยวกับระบบทำงานไม่ถูกต้องที่ส่งผลต่อการปฏิบัติที่ไม่เป็นไปตามหลักเกณฑ์ของทางการ หรือเกิดความผิดพลาดจากการปฏิบัติงานของพนักงานที่ส่งผลกระทบต่อความถูกต้องของข้อมูลลูกค้าหรือการทำธุรกรรม และส่งผลกระทบต่อชื่อเสียงของธนาคาร
3. Availability			
3.1 ความพร้อมของศูนย์คอมพิวเตอร์หลักและศูนย์สำรอง รวมถึงความพร้อมใช้ของข้อมูล (Backup data) เพื่อรองรับการให้บริการทั้งในภาวะปกติและภาวะฉุกเฉิน	● ไม่มีการเปลี่ยนแปลงที่มีนัยสำคัญภายในศูนย์คอมพิวเตอร์ในช่วงปีที่ผ่านมา ● ธนาคารมีศูนย์คอมพิวเตอร์สำรองของธนาคารเอง โดยไม่ได้เช่าอาคารสถานที่และไม่ได้ใช้บริการศูนย์คอมพิวเตอร์สำรองจากผู้ ให้บริการภายนอก ● ระบบงานสำคัญของธนาคารมีการใช้เทคโนโลยีการ backup ที่ทันสมัย และมี การ replicate ข้อมูลแบบ real-time ไปจัดเก็บที่ศูนย์ สำรอง และมีการจัดทำข้อมูล backup อีกชุดไปจัดเก็บที่ภายนอกแยกออกจากศูนย์คอมพิวเตอร์หลักและศูนย์สำรอง	● มีการเปลี่ยนแปลงภายในศูนย์คอมพิวเตอร์ในช่วงปีที่ผ่านมา โดยส่วนใหญ่เป็นการปรับปรุงเพื่อเพิ่มประสิทธิภาพ ● ธนาคารมีการเช่าอาคารสถานที่ตั้งศูนย์สำรอง หรือใช้บริการศูนย์คอมพิวเตอร์สำรองจากผู้ให้บริการภายนอก แต่มีการใช้ Facilities ต่าง ๆ เฉพาะสำหรับธนาคาร โดยแยกออกจากผู้ใช้บริการรายอื่น ๆ ● ระบบงานสำคัญของธนาคารมีการใช้เทคโนโลยีการ backup ข้อมูลที่ค่อนข้างทันสมัย ไปจัดเก็บที่ศูนย์สำรอง (นอกจากการ backup ข้อมูลโดยใช้ Tape backup)	● มีการเปลี่ยนแปลงที่มีนัยสำคัญภายในศูนย์คอมพิวเตอร์ในช่วงปีที่ผ่านมา (เช่น ปรับปรุง facilities ภายในศูนย์ฯ ย้ายศูนย์คอมพิวเตอร์ เป็นต้น) ● ธนาคารมีการเช่าอาคารสถานที่ตั้งศูนย์สำรอง หรือใช้บริการศูนย์คอมพิวเตอร์สำรองจากผู้ให้บริการภายนอก ซึ่งมีการใช้ Facilities ต่าง ๆ ภายในอาคารหรือภายในศูนย์ฯ ร่วมกับผู้ใช้บริการรายอื่น ๆ ● ระบบงานสำคัญของธนาคารมีการ backup ข้อมูลโดยใช้ Tape backup เท่านั้น

ปัจจัยที่ใช้พิจารณา	การประเมินระดับ IR Operational		
	ต่ำ	ปานกลาง	สูง
3.2 ระบบเครือข่ายสื่อสารและอุปกรณ์เครือข่าย ยังมีจุดที่เป็น single point of failure ในส่วนที่สำคัญ	● ระบบเครือข่ายและอุปกรณ์เครือข่ายสื่อสาร มีอุปกรณ์ 2 ชุด สำรองซึ่งกันและกัน และมีประสิทธิภาพความพร้อมใช้งานทดแทนกันได้ทันที อีกทั้งสามารถรองรับปริมาณธุรกรรมทั้งในช่วงปกติและช่วง peak time ได้อย่างเพียงพอ	● ระบบเครือข่ายและอุปกรณ์เครือข่ายสื่อสาร มีอุปกรณ์ 2 ชุด สำรองซึ่งกันและกัน มีเพียงอุปกรณ์บางส่วนที่อาจไม่มีการสำรองเอาไว้ แต่ไม่ใช่จุดที่มีความสำคัญ อีกทั้งสามารถรองรับปริมาณธุรกรรมทั้งในช่วงปกติและช่วง peak time ได้อย่างเพียงพอ	● ระบบเครือข่ายและอุปกรณ์เครือข่ายสื่อสาร มีอุปกรณ์ชุดเดียวในจุดที่มีความสำคัญ สามารถรองรับปริมาณธุรกรรมในช่วงปกติ
3.3 ระบบงานมีความพร้อมรองรับการประมวลผลงานได้อย่างต่อเนื่องตามความต้องการของหน่วยงานธุรกิจทั้งในภาวะปกติและภาวะฉุกเฉิน *หมายเหตุ *ระบบงานสำคัญ ได้แก่ ระบบรองรับการดำเนินธุรกิจหลักของ สง. เช่น Core Banking (เงินฝาก สินเชื่อ) , payment system, สาขา, ATM , Credit Card , Internet Banking , Mobile Banking เป็นต้น*	● ระบบงานมีความทันสมัยหรือมีการ upgrade เพื่อให้เพียงพอรองรับการดำเนินธุรกิจในอนาคต ตลอดจนจัดให้มีเครื่องประมวลผลและโปรแกรมระบบงานไว้ 2 ชุด ซึ่งชุดสำรองสามารถรองรับปริมาณธุรกรรมได้เทียบเท่าชุดหลักทั้งในช่วงปกติและช่วง peak time	● ระบบงานใช้งานมาไม่นาน อาจมีบางส่วนมีความล้าสมัยบ้าง แต่ยังสามารถรองรับการดำเนินธุรกิจปัจจุบันต่อได้ อาจต้องปรับปรุงตามกระบวนการปรับปรุงเปลี่ยนแปลงระบบงานตามรอบระยะเวลาที่กำหนด ตลอดจนมีเครื่องประมวลผลและโปรแกรมระบบงานไว้ 2 ชุด สำรองซึ่งกันและกัน แต่ยังมีอุปกรณ์บางส่วนที่อาจไม่มีการสำรองเอาไว้หรือชุดสำรองมีประสิทธิภาพไม่เทียบเท่าชุดหลัก 100% แต่ยังสามารถรองรับปริมาณธุรกรรมทั้งในช่วงปกติและช่วง peak time ได้อย่างเพียงพอ	● ระบบงานมีการใช้งานมานานบางส่วนมีความล้าสมัย แล้วอีกทั้งมีเครื่องประมวลผลและโปรแกรมระบบงานเพียงชุดเดียว ไม่มีการจัดเตรียมชุดสำรองเอาไว้
3.4 Incidents/Loss/ Complaint related to service disruption	● ไม่พบว่ามี Incidents/ความเสียหาย/ข้อร้องเรียน ที่เกี่ยวกับระบบงานสำคัญของธนาคารหยุดชะงัก เช่น Core Banking, ระบบงานสาขา, ATM, Internet Banking, Mobile Banking เป็นต้น ที่ส่งผลต่อการให้บริการลูกค้า	● พบว่ามี Incidents/ความเสียหาย/ข้อร้องเรียน ที่เกี่ยวกับระบบงานสำคัญของธนาคารหยุดชะงัก เช่น Core Banking, ระบบงานสาขา, ATM, Internet Banking, Mobile Banking เป็นต้น ที่ส่งผลต่อการให้บริการลูกค้าแต่อยู่ในวงจำกัด แต่ไม่ส่งผลกระทบต่อชื่อเสียงของธนาคาร และสามารถกู้คืนระบบได้ตาม RTO ที่กำหนดไว้	● พบว่ามี Incidents/ความเสียหาย/ข้อร้องเรียน ที่เกี่ยวกับระบบงานสำคัญของธนาคารหยุดชะงัก เช่น Core Banking, ระบบงานสาขา, ATM, Internet Banking, Mobile Banking เป็นต้น ที่ส่งผลต่อการให้บริการลูกค้าในวงกว้าง ส่งผลกระทบต่อชื่อเสียงของ ธนาคารและระบบงานหยุดชะงักเป็นเวลานานเกินกว่า RTO ที่กำหนดไว้

2.2.2 ปัจจัยการประเมิน IR ด้านกลยุทธ์

ประเมินเฉพาะเมื่อมีระบบงานใหม่หรือการเปลี่ยนแปลงที่มีนัยสำคัญ



ปัจจัยที่ใช้พิจารณา	การประเมินระดับ IR Strategic		
	ต่ำ	ปานกลาง	สูง
IT Business Alignment			
นโยบาย/แผนกลยุทธ์ และการจัดสรรงบประมาณโครงการด้าน IT และ Cyber Security ที่สำคัญสอดคล้องกับเป้าหมายเชิงกลยุทธ์ทางธุรกิจ	● ธนาคารกำหนดนโยบาย/แผนกลยุทธ์ และการจัดสรรงบประมาณลงทุนด้าน IT และ Cyber Security มีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์ธุรกิจ และมีแผนงาน/โครงการในการพัฒนาปรับปรุงระบบ IT และ Cyber Security ที่ชัดเจนในการรองรับการเติบโตทางธุรกิจระยะยาว ทั้งในด้าน Digitization และ Regionalization ● ธนาคารมีโครงการด้าน IT และ Cyber Security ที่สำคัญที่อยู่ระหว่างดำเนินการอยู่บ้าง และไม่มีโครงการที่ล่าช้า	● ธนาคารกำหนดนโยบาย/แผนกลยุทธ์ และการจัดสรรงบประมาณลงทุนด้าน IT และ Cyber Security สอดคล้องกับเป้าหมายเชิงกลยุทธ์ธุรกิจอยู่บ้าง แต่แผนงาน/โครงการในการพัฒนาปรับปรุงระบบ IT ที่จะนำมาสนับสนุนการทำธุรกิจระยะยาวยังไม่ชัดเจน ● ธนาคารมีโครงการด้าน IT และ Cyber Security ที่สำคัญที่อยู่ระหว่างดำเนินการ แต่เป็นเพียงการปรับปรุงหรือเพิ่มประสิทธิภาพ ซึ่งหากโครงการมีความล่าช้า ก็ไม่ส่งผลกระทบต่อเป้าหมายกลยุทธ์การดำเนินธุรกิจหรือส่งผลกระทบต่อการให้บริการลูกค้า	● ธนาคารมีนโยบาย/แผนกลยุทธ์ในการพัฒนาด้าน IT และ Cyber Security แต่แผนอาจไม่มีความชัดเจนและไม่เพียงพอรองรับในการสนับสนุนแผนกลยุทธ์เชิงธุรกิจได้ ● ธนาคารมีโครงการด้าน IT และ Cyber Security ที่สำคัญใหม่ ๆ ที่อยู่ระหว่างดำเนินการเป็นจำนวนมาก และหากโครงการมีความล่าช้าหรือมีการเลื่อนแผนงานจะส่งผลกระทบต่อเป้าหมายกลยุทธ์การดำเนินธุรกิจหรือส่งผลกระทบต่อการให้บริการลูกค้า

ส่วนที่ 3 การประเมิน Quality of Risk Management (QRM)

3.1 คำจำกัดความ

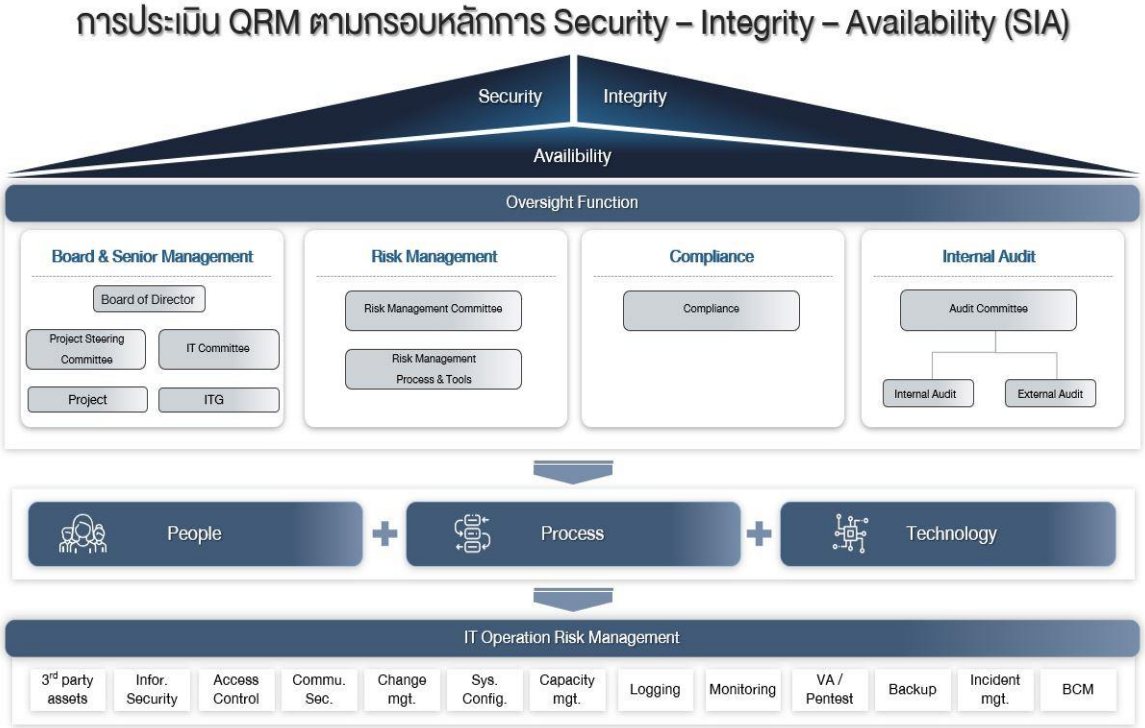
Quality of Risk Management (QRM) หมายถึง การบริหารจัดการเพื่อลดความเสี่ยงที่มีอยู่ของแต่ละ SA นั้น โดยจะแบ่งการประเมินออกตามระดับการควบคุมเป็น 2 ระดับ คือ

1. ระดับการปฏิบัติงานประจำวัน (Operational Management : OM) เป็นการควบคุมเพื่อจัดการความเสี่ยงที่มีอยู่ของการทำธุรกรรมในแต่ละวัน (Day-to-Day Operation) เพื่อให้มั่นใจว่าผู้ปฏิบัติงานเข้าใจความเสี่ยงที่เกิดขึ้นและสามารถจัดการกับความเสี่ยงนั้นได้ โดยมีนโยบาย ขั้นตอนการปฏิบัติงาน และบุคลากรเพียงพอและมีประสิทธิภาพในการจัดการความเสี่ยง ถือเป็น “แนวป้องกันความเสี่ยงชั้นแรก (First Line of Defense)”

2. ระดับการควบคุมดูแล (Oversight Functions : OF) เป็นการควบคุมดูแลการจัดการเชิงปฏิบัติการโดยรวมของ สง. โดยมีหน่วยงานหรือผู้ที่มีความเป็นอิสระของ สง. ซึ่งไม่มีหน้าที่รับผิดชอบการปฏิบัติงานประจำวัน ทำหน้าที่ดังกล่าว ประกอบด้วยงาน 5 ด้าน ได้แก่ คณะกรรมการ สง. ผู้บริหารระดับสูง งานบริหารความเสี่ยง งานกำกับการปฏิบัติตามกฎเกณฑ์ และงานตรวจสอบภายใน เพื่อให้เกิดความมั่นใจว่าระบบ IT ของ สง. มีการดำเนินการที่สอดคล้องกับมาตรฐานและแนวปฏิบัติที่ดี

3.2 การประเมิน QRM (OM + OF)

สง. จะต้องจัดให้มีระบบการบริหารจัดการความเสี่ยงที่มีประสิทธิภาพ เพื่อสามารถลดหรือควบคุมความเสี่ยงที่มีอยู่ของระบบงาน IT โดยมีวิธีการประเมิน QRM ในแต่ละด้าน ดังนี้



3.2.1 การประเมิน Operational Management (OM)

(1) ด้านการรักษาความปลอดภัย (Security)

ปัจจัยที่ใช้ประเมิน	วิธีการประเมิน
การกำกับดูแลนโยบายด้านการรักษาความปลอดภัย	• ประเมินการกำหนด Policy/ Standard/ Procedure ที่ครอบคลุมกิจกรรมงาน IT ของ สง. อย่างชัดเจนเป็นลายลักษณ์ และได้รับการอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย ตลอดจนมีกระบวนการทบทวนปรับปรุงอย่างสม่ำเสมอให้ทันสมัยและสอดคล้องตามมาตรฐานสากล (ขอบเขตครอบคลุมตาม ISO) อีกทั้งมีการควบคุมดูแลให้มีการปฏิบัติงานให้เป็นไปตาม Policy/ Standard/ Procedure ที่กำหนด และมีกระบวนการ exception อย่างชัดเจนและตรวจสอบได้ • สอบทานการทบทวนนโยบายด้านการรักษาความปลอดภัย • สอบทานรายงานการปฏิบัติ/ไม่ปฏิบัติตามนโยบายที่กำหนด
การกำหนดนโยบายด้านการรักษาความปลอดภัยและการนำไปกำหนดกรอบเป็นแนวทางการปฏิบัติงาน	• นโยบายด้านการรักษาความปลอดภัยฉบับล่าสุดได้รับอนุมัติจากคณะกรรมการ สง. โดยอ้างอิงตามมาตรฐาน ISO27001/ ISO27002 • มีรายละเอียดครอบคลุมเรื่อง Security, Integrity, Availability และ Data Confidentiality เป็นต้น • นโยบาย มาตรฐาน ระเบียบ ประกาศใช้เป็นการทั่วไป ให้พนักงานทุกคนเข้าถึงได้ และมีการสื่อสารให้พนักงานรับทราบ • นโยบาย มาตรฐาน ระเบียบ มีความสอดคล้องกันและครอบคลุมเรื่องสำคัญ/เทคโนโลยีใหม่ๆ ที่ สง. นำมาใช้แล้ว เช่น เรื่อง Privileged User ID Management, Data Leak Protection, Wireless Network, BYOD, Cloud Computing เป็นต้น • มีหน่วยงานควบคุมดูแลให้มีการปฏิบัติตามนโยบายดังกล่าว และการขอยกเว้นไม่ปฏิบัติตามนโยบาย มาตรฐาน หรือระเบียบ ต้องได้รับความเห็นชอบจากผู้ที่มีอำนาจ
มาตรการรักษาความปลอดภัยด้าน Physical และการปฏิบัติตามนโยบาย	• ประเมินและสอบทานการรักษาความปลอดภัยทางกายภาพของ Area อื่น ๆ ที่สำคัญของธนาคาร/บริษัท เช่น การใช้ Access Control System (บัตร/รหัสผ่าน/สแกนลายนิ้วมือ) การจัดแบ่งโซน (Zoning), Guard และการจัดเก็บทะเบียนและสอบทาน log การผ่านเข้าออก เป็นต้น
มาตรการรักษาความปลอดภัยด้าน Logical และการปฏิบัติตามนโยบาย	• ประเมินมาตรการ เทคโนโลยี และเครื่องมือที่ใช้ในการรักษาความปลอดภัยด้าน Logical แบบ End-to-End ให้ครอบคลุมมาตรการทั้งในเชิงป้องกัน (Prevent) ติดตาม (Detect) และแก้ไข (Correct) หากเกิดการบุกรุก/ภัยคุกคามต่าง ๆ ดังนี้ **(1) ระบบเครือข่ายสื่อสาร (Network Infrastructure)** o Network Diagram : ระบบและข้อมูลสำคัญมีความปลอดภัยจากการถูกบุกรุกทางเครือข่ายทั้งภายในภายนอก การออกแบบระบบ

ปัจจัยที่ใช้ประเมิน	วิธีการประเมิน
	เครือข่ายสอดคล้องตามหลักมาตรฐานสากล และมีจุดใดที่จะก่อให้เกิด Single Point of Failure หรือไม่ o การประเมินช่องโหว่ (VA) ของอุปกรณ์ระบบเครือข่ายสื่อสาร o แนวปฏิบัติที่ดี : การแบ่งเครือข่ายย่อยออกเป็น DMZ zone, database zone, server zone, extranet zone, BOT zone, UAT and Dev zone และ WAN zone เป็นต้น เพื่อกำหนดมาตรการรักษาความปลอดภัยให้เหมาะสม โดยใช้ฟังก์ชั่น Virtual Local Area Network (VLAN) ในอุปกรณ์ Switch o ธนาคารแยกเครือข่าย internet ออกจากเครือข่าย intranet อย่างชัดเจน รวมทั้งมีการแยกเครือข่าย Internet ที่ให้พนักงานใช้ทั่วไปกับเครือข่าย internet ที่ใช้สำหรับงานของธนาคาร เช่น การ update patch, virus signature, IPS signature เป็นต้น มีการติดตั้ง firewall ป้องกันที่จุดเชื่อมต่อไปยังเครือข่าย internet อย่างเหมาะสม o มีการใช้ IPS เพื่อตรวจจับ และป้องกันการบุกรุก ผ่านช่องทางสำคัญ o Network Security Monitoring : ประเมินความชัดเจนของหน่วยงานผู้รับผิดชอบ ความครอบคลุมของการ Monitor เครื่องมือที่ใช้ และกระบวนการดำเนินการหากพบความผิดปกติหรือที่น่าสงสัย หากมีการ outsource งานด้าน Network Security Monitoring ประเมินตามแนวทาง 3rd Party และให้ความสำคัญกับประเมินความเสี่ยงที่ผู้ให้บริการสามารถเข้าถึงระบบงาน/ข้อมูลภายในของธนาคาร o *[Refer to ภาคผนวก ก : 2.1 Network Access Control, 2.2 Network Security Management]* **(2) ระบบปฏิบัติการ (OS) และโปรแกรมระบบงาน (Application)** o ประเมินกระบวนการ/วิธีการในการกำหนด/ควบคุม/สอบทานสิทธิ์การใช้งาน OS/Application การตั้งค่าและปรับแต่งค่า parameter การจัดเก็บและสอบทาน log และการจัดการ patch โดยครอบคลุมถึง กระบวนการควบคุมสิทธิ หน่วยงานผู้กำหนดสิทธิ หน่วยงานผู้สอบทานสิทธิ ความถี่ในการสอบทาน o สอบทานการ set policy ใน AD เช่น รหัสผ่านขั้นต่ำ 8 ตัวอักษร บังคับเปลี่ยนรหัสผ่านทุก 90 วัน และตั้งรหัสผ่านห้ามซ้ ากับของเดิม 5 ครั้งก่อนหน้า พิมพ์รหัสผ่านผิดได้ไม่เกิน 3 ครั้ง และทำการ lock screen server อัตโนมัติเมื่อไม่ได้ใช้งานหน้าจอเกิน 15 นาที เป็นต้น

ปัจจัยที่ใช้ประเมิน	วิธีการประเมิน
	○ สอบทานการควบคุมสิทธิ Privilege User เช่น หน่วยงานที่ควบคุม/ใช้ระบบ Vault เพื่อควบคุมการขอเข้าใช้งาน การจัดเก็บ Log ของการใช้งาน Privilege User หน่วยงานที่สอบทาน เป็นต้น ○ Non-Repudiation, Session Control, Audit Trail, Logging ○ Administration : System Admin, Application Admin, Security Admin ○ การตั้งค่าความปลอดภัยของเครื่อง เช่น การสอบทาน firewall rule ○ การ maintenance : Hardening : พนักงานออกและสอบทาน hardening checklist การติดตามและปรับปรุง patch ของระบบปฏิบัติการ Windows ○ การประเมินช่องโหว่ (VA) ของ OS และ Application ต่างๆ ○ *[Refer to ภาคผนวก ก : 3.1 Logical Access Control, 3.2 System Security Management]* **(3) Information/Data Confidentiality** ○ การจัดลำดับความสำคัญของข้อมูล มีมาตรการและเครื่องมือในการรักษาความปลอดภัยและความลับให้เหมาะสมและสอดคล้องกับลำดับความสำคัญของข้อมูล (Data at Rest, Data in Transit, Data in use) และทบทวนอย่างสม่ำเสมอ ให้เป็นปัจจุบัน เช่น ■ การเข้ารหัสข้อมูลบนเครือข่ายสื่อสาร บน Disk เช่น เข้ารหัสแบบ end-to-end encryption ด้วยมาตรฐาน SSL (Secure Socket Layer) ■ การส่งข้อมูลบริษัทไปยังภายนอก ใช้ PGP Standard ในการ encrypt รูปแบบ Algorithm เป็น RSA (2048 bits) และมีการแลกเปลี่ยน Public Key ทุกปี ■ การรายงาน Security Violation Report ต่อ ITSC ทุกเดือน ■ ข้อสังเกตจากการสุ่มตรวจสอบมาตรการรักษาความปลอดภัยของบริษัทภายนอก
การทดสอบการเจาะระบบงานโดยที่ปรึกษาภายนอก เพื่อตรวจหาช่องโหว่ของระบบรักษาความปลอดภัย	● สอบทานรายงานผลการทดสอบเจาะระบบโดยบริษัทที่เชี่ยวชาญภายนอกหรือโดยหน่วยงานภายในบริษัท ประเด็นที่มีความเสี่ยงและการแก้ไข ● ประเมินความครอบคลุมของการทดสอบ (เทียบกับ OWASP)
Loss incident ที่เกี่ยวข้อง	● สอบทานรายงาน Loss Incident ที่สำคัญที่เป็นการ Attack ด้าน Security เช่น Malware, DDoS เป็นต้น

(2) ด้านความถูกต้องและความน่าเชื่อถือ (Integrity)

ปัจจัยที่ใช้ประเมิน	วิธีการประเมิน
การกำกับดูแลด้านความถูกต้องและความน่าเชื่อถือ	• องค์ประกอบ และบทบาทหน้าที่ของคณะกรรมการ/หน่วยงานที่เกี่ยวข้องกับความถูกต้องและความน่าเชื่อถือของข้อมูลและระบบงาน ครอบคลุมหัวข้อดังต่อไปนี้ ○ การควบคุมการพัฒนา การเปลี่ยนแปลงโปรแกรม/ระบบงาน ○ การควบคุมการเปลี่ยนแปลง Parameter และค่า configuration ต่าง ๆ ○ การควบคุมการเปลี่ยนแปลงอัตราดอกเบี้ยและค่าธรรมเนียมต่าง ๆ ○ การควบคุมไม่ให้มีการแก้ไขข้อมูลจริงบน Production โดยตรง ○ การควบคุม Version ของการออกใช้ Software
การกำหนดนโยบายด้านความถูกต้องและน่าเชื่อถือ	• มีนโยบาย ระเบียบกำหนดขั้นตอนควบคุม ครอบคลุมเพียงพอกับการปฏิบัติงานในการพัฒนา เปลี่ยนแปลงระบบงานหรือการจัดหาระบบงานใหม่ เช่น คู่มือพัฒนาระบบ Change Management Policy & Procedure , Incident Management Policy & Procedure โดยได้รับอนุมัติจากคณะกรรมการที่เกี่ยวข้อง
กระบวนการหรือมาตรการที่ใช้ในการทดสอบความถูกต้องและความน่าเชื่อถือ	**(1) SDLC** • ประเมินกระบวนควบคุมการพัฒนา/เปลี่ยนแปลงระบบงาน IT รวมถึงการนำระบบงานออกใช้ใน Production อย่างเหมาะสมและสอดคล้องตามนโยบายและระเบียบที่กำหนด *[Refer to ภาคผนวก ข: ตารางการควบคุมที่สำคัญ 6. Switching/Clearing ข้อ 6.8]* • ประเมินกระบวนการ โดยเลือกสุ่มขั้นตอนต่าง ๆ ได้แก่ Feasibility Study, Develop, Test, Go live • มาตรฐานการทดสอบที่ครอบคลุม Unit Test, System Test, System Integrated Test (SIT), User Acceptance Test (UAT), Operation Acceptance Test (OAT) **(2) Batch Processing** • การประมวลผลสิ้นวันมีมาตรการ ขั้นตอน/เครื่องมือ ในการควบคุมการประมวลผลสิ้นวัน *[Refer to ภาคผนวก ข : ตารางการควบคุมที่สำคัญ 6. Switching/Clearing ข้อ 6.9 – 6.12]* **(3) Application Control** • Switching/Clearing ครอบคลุมการทำธุรกรรมแบบ End-to-End *[Refer to ภาคผนวก ข : ตารางการควบคุมที่สำคัญ 6. Switching/Clearing ข้อ 6.1- 6.5, 6.9-6.15]*

ปัจจัยที่ใช้ประเมิน	วิธีการประเมิน
	• Payment Gateway ครอบคลุมการทำธุรกรรมแบบ End-to-End *[Refer to ภาคผนวก ข: ตารางควบคุมที่สำคัญ 5. e-commerce (payment gateway) ข้อ 5.1-5.6]*
Loss Incident ที่เกี่ยวข้อง	• สอบทานรายงาน Loss Incident ที่สำคัญ ที่อาจกระทบต่อความถูกต้องเชื่อถือได้ของข้อมูล ระบบงาน เช่น การติดตั้งโปรแกรมผิดพลาดบน Production การเปลี่ยน Table/Parameter เกี่ยวกับอัตราดอกเบี้ยผิด การนำ Tape Backup ผิดมา install เป็นต้น

(3) ด้านความพร้อมใช้งาน (Availability)

ปัจจัยที่ใช้ประเมิน	วิธีการประเมิน
ความพร้อมของศูนย์คอมพิวเตอร์หลัก	• ประเมินความพร้อมของศูนย์คอมพิวเตอร์ โดยดูปัจจัย ได้แก่ ที่ตั้งศูนย์คอมพิวเตอร์ ลักษณะโครงสร้างอาคาร การบริหารจัดการศูนย์ [Refer to *ภาคผนวก ก* : 1 ศูนย์คอมพิวเตอร์ (Data Center)] • มาตรการด้านการรักษาความปลอดภัยที่สำคัญ ได้แก่ ผลการประเมินศูนย์เทียบมาตรฐานสากลได้ระดับ Tier ตามมาตรฐานของ TIA942 • ประเมินด้าน Physical Security ได้แก่ o Access Control o Guard o CCTV o Fire Protection o สภาพแวดล้อมอื่น ๆ เช่น ความเสี่ยงต่ออัคคีภัย หรือภัยธรรมชาติ o การยกพื้นห้องสูงและติดตั้งอุปกรณ์ป้องกันไฟฟ้าสถิต (High Pressure laminate: HPL) • ระบบไฟฟ้าและไฟฟ้าสำรอง ได้แก่ o Flow ของระบบไฟฟ้า o รายละเอียด UPS o รายละเอียด Generator และน้ ามันสำรอง • ระบบปรับอากาศ/ทำความเย็น • ระบบป้องกันไฟไหม้และน้ำรั่ว • ความพร้อมใช้ของระบบเครือข่ายสื่อสาร *[Refer to ภาคผนวก ก : 2.3 Network Availability Management]* o เครือข่ายสื่อสารระหว่างศูนย์หลัก และศูนย์สำรอง o เครือข่ายสื่อสารจากสาขาที่เชื่อมต่อเข้าสู่ศูนย์หลัก o มีการประเมิน Single Point of Failure เป็นระยะ และทุกครั้งที่มีการติดตั้งอุปกรณ์หรือเปลี่ยนแปลงโครงสร้างด้านเครือข่าย o การสำรองข้อมูลระหว่างศูนย์หลักและศูนย์สำรอง

ปัจจัยที่ใช้ประเมิน	วิธีการประเมิน
	○ การบำรุงรักษา Hardware อุปกรณ์ภายในศูนย์ และระบบ Facility ต่าง ๆ ○ การติดตามเฝ้าระวังที่สำคัญ และเครื่องมือที่ใช้ในการติดตาม Security Monitoring ○ มีแผนปฏิบัติการกรณีเหตุการณ์ฉุกเฉินครอบคลุมกรณีต่าง ๆ เช่น อุปกรณ์เครือข่ายสื่อสารตัวใดตัวหนึ่งขัดข้อง หรือระบบเครือข่ายสื่อสารขัดข้อง เป็นต้น โดยจัดทำแผนฯ เป็นลายลักษณ์อักษรและเป็นปัจจุบัน และครอบคลุมรายชื่อผู้ให้บริการระบบเครือข่ายสื่อสารและเบอร์ติดต่อ ○ มีการทดสอบแผน DRP กรณีระบบเครือข่ายสื่อสารขัดข้องร่วมกับผู้ให้บริการ ○ มีการประเมินประสิทธิภาพของผู้ให้บริการเครือข่ายสื่อสารและมีแผนรองรับกรณีผู้ให้บริการไม่สามารถให้บริการได้
ความพร้อมของศูนย์คอมพิวเตอร์สำรอง	● ข้อมูลศูนย์คอมพิวเตอร์สำรอง ในหัวข้อเช่นเดียวกันกับศูนย์หลัก ● วิธีการ/ขั้นตอนการสำรองข้อมูลประจำวันของระบบงานสำคัญ ประเมินความสอดคล้องกับนโยบาย DRP ● การแบ่งประเภทและจัดเตรียมความพร้อมใช้งานของระบบงานและข้อมูล ● กลยุทธ์การกู้คืน (Recovery Strategy) รูปแบบ วิธีการ เทคโนโลยี และความถี่ที่ใช้ในการสำรองข้อมูล
การติดตามดูแล Capacity ของเครื่องประมวลผลสำคัญ	● ประเมินการติดตามดูแล Utilization & Capacity Management ของศูนย์คอมพิวเตอร์หลักและสำรอง อุปกรณ์ Switching, Access Node และการเชื่อมต่อที่เกี่ยวข้องกับสมาชิกทั้งระบบหลักและสำรอง ในการให้บริการทั้งภาวะปกติและฉุกเฉิน รวมถึง stress volume โดยสอบทานจากรายงาน เช่น IT Dashboard, IT Service Management Monthly Report และการวัด Capacity ของอุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย, Database Utilization, CPU & Memory Usage และ Incident Report เป็นต้น *[Refer to ภาคผนวก ก : 1.2 การบริหารจัดการศูนย์ฯ (Facility Management) + ภาคผนวก ข : ตารางการควบคุมที่สำคัญ 6. Switching/Clearing ข้อ 6.6]* ● กระบวนการติดตามดูแลบำรุงรักษาอุปกรณ์ที่เกี่ยวข้องภายในศูนย์คอมพิวเตอร์หลักและสำรอง รวมถึงอุปกรณ์ที่เกี่ยวข้องและเชื่อมต่อ switching/clearing เพื่อให้มั่นใจว่ามีความพร้อมรองรับการให้บริการอย่างต่อเนื่อง *[Refer to ภาคผนวก ก : 1.2 การบริหารจัดการศูนย์ฯ (Facility Management) + ภาคผนวก ข : ตารางการควบคุมที่สำคัญ 6. Switching/Clearing ข้อ 6.7]*

ปัจจัยที่ใช้ประเมิน	วิธีการประเมิน
การบริหารจัดการทรัพย์สินด้าน IT	• มีมาตรฐานและระเบียนวิธีปฏิบัติการบริหารจัดการทรัพย์สินด้าน IT ครอบคลุมกระบวนการจัดการทรัพย์สินตั้งแต่ การจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การยกเลิกและเรียกคืนทรัพย์สิน • มีหน่วยงานผู้รับผิดชอบในการจัดทำ ปรับปรุงทะเบียนรายการทรัพย์สินด้าน IT และบำรุงรักษาทรัพย์สินด้าน IT • มีการจัดทำทะเบียนรายการทรัพย์สินด้าน IT อย่างครบถ้วนและเป็นลายลักษณ์อักษร • ปรับปรุงทะเบียนรายการทรัพย์สินด้าน IT ให้เป็นปัจจุบันอย่างต่อเนื่อง โดยมีการตรวจสอบทรัพย์สินด้าน IT ที่อยู่จริงกับทะเบียนรายการทรัพย์สินอย่างน้อยปีละ 1 ครั้ง • วางแผนรอบรับทรัพย์สินด้าน IT ที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (end of life) หรือ สิ้นสุดการให้บริการ (end of support) อย่างเหมาะสมทันการณ์ • กรณีใช้ทรัพย์สินด้าน IT ที่สิ้นสุดอายุการใช้งานหรือสิ้นสุดการให้บริการ ควรมีการประเมินความเสี่ยงจากการใช้งาน จัดหาการควบคุมแทน และควรใช้งานเพียงระยะสั้นตามระดับความเสี่ยงเท่านั้น รวมทั้งได้รับอนุมัติจากผู้บริหารที่ทำหน้าที่บริหารความเสี่ยง
Loss Incident ที่เกี่ยวข้อง	• สอบทาน Loss Incident ที่สำคัญ ที่อาจกระทบต่อความพร้อมใช้ของระบบงานและข้อมูล
การกำกับดูแลด้านการบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (DRP)	• บทบาทหน้าที่ของคณะกรรมการ/คณะกรรมการย่อย ผู้บริหารระดับสูง และฝ่ายงานที่เกี่ยวข้องในการกำกับดูแลการบริหารความต่อเนื่องทางธุรกิจตามสภาวะปกติ • การแต่งตั้งคณะกรรมการหรือทีมงานเฉพาะกิจเพื่อบริหารจัดการขณะเกิดเหตุวิกฤติพร้อมบทบาทหน้าที่ดังกล่าว
การกำหนดนโยบายการบริหารความต่อเนื่องทางธุรกิจ แผนฉุกเฉินด้าน IT (BCM Policy, BCP Policy, DR Policy)	• ความชัดเจนและความครอบคลุมของการจัดทำแผนฉุกเฉินด้าน IT ให้สอดคล้องกับนโยบาย BCM/BCP รวมถึงการประเมินการทดสอบระบบใน scenario ต่างๆ เพื่อให้มั่นใจได้ว่าระบบมีความพร้อมในการรองรับการให้บริการแก่สมาชิกภายใต้ สถานการณ์ฉุกเฉินต่าง ๆ *[Refer to ภาคผนวก ข : ตารางการควบคุมที่สำคัญ 6. Switching/Clearing ข้อ 6.6]*

การจัดทำแผน Disaster Recovery Plan (DRP) ของระบบงาน	• รายละเอียดแผน DRP ของระบบงานสำคัญ มีรายละเอียดครอบคลุมหัวข้อดังต่อไปนี้ ○ หน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง ○ การวิเคราะห์ผลกระทบต่อธุรกิจ (BIA) ○ การประเมินความเสี่ยง (Risk Assessment) และลดความเสี่ยง ○ การจัดลำดับระบบงานที่สำคัญและการจัดสรรทรัพยากร ○ การกำหนด trigger event และอำนาจการตัดสินใจที่ชัดเจน ○ Scenario ของการจัดทำแผน ควรครอบคลุม ■ ความรุนแรงน้อย เช่น กรณีเกิดความเสียหายเป็นบางเครื่อง/อุปกรณ์/ระบบงาน ■ ความรุนแรงปานกลาง เช่น กรณีระบบเครือข่ายสื่อสารขัดข้อง ■ ความรุนแรงสูง เช่น กรณีที่ต้องย้ายไปใช้งานศูนย์คอมพิวเตอร์สำรอง ○ Recovery Time Objective (RTO), Recovery Point Objective (RPO) ของระบบงาน ○ ขั้นตอนการปฏิบัติเพื่อกู้คืนระบบงานตั้งแต่เกิดเหตุจนถึงการกลับคืนสู่ภาวะปกติ ○ รายการอุปกรณ์ และเบอร์โทรศัพท์ของผู้ที่เกี่ยวข้อง (call tree) รวมถึง service providers คู่ค้า หรือ vendors ○ การทบทวนและปรับปรุงแผน ○ ความสอดคล้องและเป็นไปได้ของ DRP กับ BCP ของหน่วยงาน IT, service providers และฝ่ายงานที่เกี่ยวข้องอื่น ๆ
การทดสอบและการรายงานผลการทดสอบ Disaster Recovery Plan (DRP) ของระบบงานสำคัญ	• กระบวนการกำหนดแผนและการอนุมัติแผนการทดสอบประจำปี • รายละเอียดแผนการทดสอบ scenario ที่ใช้ และความครอบคลุมของระบบงานและเครือข่ายสื่อสารที่สำคัญ • การมีส่วนร่วมของผู้ที่เกี่ยวข้อง เช่น user, vendors/counterparties หรือ service providers • ผลการทดสอบ (actual RTO/target RTO) และข้อบกพร่องหรือปัญหาที่พบในการทดสอบ รวมถึง การดำเนินการแก้ไข • กระบวนการรายงานผลการทดสอบให้กรรมการหรือผู้บริหารระดับสูง • กระบวนการประเมินผลการทดสอบโดยหน่วยงานที่เป็นอิสระ
การทบทวนและปรับปรุงแผนฉุกเฉินด้าน IT	• การทบทวนและปรับปรุงแผน DRP ตามสภาพแวดล้อมที่เปลี่ยนแปลง / ตามข้อสังเกตจากผลการทดสอบครั้งล่าสุด

3.2.2 การประเมิน Oversight Functions (OF)

(1) คณะกรรมการธนาคาร (Board of Director : BOD)

หลักการ
1. เพื่อให้การบริหารจัดการ สง. มีความมั่นคง โปร่งใส มีธรรมาภิบาล และปฏิบัติตามกฎเกณฑ์ทางการ 2. ควบคุมและติดตามการบริหารจัดการ สง. ให้เป็นไปตามนโยบาย แผนงานด้าน IT และสอดคล้องกับเป้าหมายกลยุทธ์ทางธุรกิจที่กำหนด

ปัจจัยที่ใช้ประเมิน	วิธีการประเมิน
บทบาทหน้าที่ของคณะกรรมการธนาคารในการสนับสนุนการดำเนินกลยุทธ์	• คณะกรรมการมีการกำหนดเป้าหมาย วิสัยทัศน์ พันธกิจของ สง. อย่างชัดเจน และคำนึง Safety & Efficiency ของระบบ
ด้านเทคโนโลยีสารสนเทศ	• คณะกรรมการกำกับดูแลการดำเนินงานด้าน IT สอดคล้องกับธรรมาภิบาล และคำนึง Stakeholder ที่เกี่ยวข้อง ได้แก่ ธนาคารสมาชิก ลูกค้า ประชาชน และหน่วยงานทางการ • บทบาทหน้าที่ความรับผิดชอบและองค์ประกอบของคณะกรรมการมีความชัดเจน เหมาะสม ถ่วงดุล และตรวจสอบได้ ไม่มี Conflict of Interest • การกำหนดนโยบายและกรอบแนวทางการดำเนินงานด้าน IT ที่สอดคล้อง และสามารถสนับสนุนนโยบายของธุรกิจ • การกำหนดนโยบายและกรอบแนวทางด้านการบริหารจัดการความเสี่ยงให้ อยู่ในระดับที่ยอมรับได้ โดยคำนึงถึงเรื่องการดูแลผลกระทบต่อลูกค้าผู้บริโภค • บทบาทของคณะกรรมการที่เกี่ยวข้องกับการสนับสนุนและการบริหารจัดการด้าน IT โดยประเมินระดับการให้ความสำคัญและการสนับสนุนใน ด้านต่าง ๆ ในลักษณะ High level ดังนี้ ○ **การกำหนดกลยุทธ์และงบประมาณด้าน IT** : คณะกรรมการให้ความสำคัญกับการกำหนดกลยุทธ์ด้าน IT รวมทั้งมีการดูแลการจัดสรรงบประมาณด้าน IT ให้สอดคล้องกับเป้าหมายเชิงกลยุทธ์ เช่น การ Support Business การเพิ่ม Efficiency ของ Infrastructure และ Security เป็นต้น ○ **บุคลากร** : มีการกำหนดให้มีโครงสร้างหน่วยงานที่รับผิดชอบและมีแผนการจัดการบุคลากรด้าน IT อย่างเพียงพอและเหมาะสม ○ **กระบวนการทำงาน** : มีการจัดให้มีกระบวนการตรวจสอบและติดตามความเสี่ยงด้าน IT อย่างเพียงพอเหมาะสมตามหลักการ 3 Lines of Defense • รายละเอียดแผนกลยุทธ์และแผนงานประจำปีด้าน IT ที่สำคัญ • นโยบายและเป้าหมายด้าน IT ที่สำคัญ เช่น

	○ **นโยบายด้านการรักษาความปลอดภัย** : ควรกำหนดให้คณะกรรมการบริษัทจัดให้มีการประเมินประสิทธิภาพของนโยบายและกระบวนการรักษาความปลอดภัยอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่กระทบต่อการรักษาความปลอดภัยที่สำคัญ และนำเสนอคณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย ○ **นโยบาย 3rd Party Management/Outsourcing/Insourcing IT:** ควรกำหนดให้มีการประเมินความเสี่ยงก่อนการใช้บริการจากบุคคลภายนอกและ ครอบคลุมความเสี่ยงด้าน IT ที่สำคัญ รวมทั้ง มีการทบทวนความเสี่ยงเป็นประจำอย่างน้อยปีละครั้ง ○ **นโยบายการตรวจสอบด้าน IT** : ควรกำหนดให้มีการตรวจสอบศูนย์คอมพิวเตอร์อย่างน้อยทุกรอบ 12 เดือน ○ **นโยบาย BCM/BCP** : ควรจัดให้มีการประเมินและทบทวนแผน BCP จากหน่วยงานภายนอกที่มีความเชี่ยวชาญ หรือหน่วยงานภายในที่มีความรู้ความสามารถและมีความเป็นอิสระ และรายงานผลการประเมินต่อคณะกรรมการ นอกจากนี้ ควรปรับปรุงแผน BCP อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ควรทดสอบร่วมกับผู้ให้บริการและผู้ใช้บริการหลัก รวมทั้งปรับปรุงข้อมูลหรือเอกสารที่ได้เผยแพร่แก่พนักงานหรือบุคคลภายนอกให้มีความเป็นปัจจุบันและสอดคล้องกัน ○ สรุปการใช้บริการ 3rd Party ด้าน IT/Outsourcing/Insourcing ที่สำคัญ การติดตามประเมินผล และตรวจสอบการปฏิบัติงานของผู้ให้บริการภายนอก (Service Providers)

(2) ผู้บริหารระดับสูง (Senior Management) หมายถึง คณะกรรมการหรือหัวหน้าสายงาน ที่ทำหน้าที่รับนโยบาย เป้าหมาย ไปปฏิบัติให้เกิดผลสำเร็จตามที่กำหนด เช่น Executive Committee แต่ไม่รวมถึง Audit Committee และ Risk Management Committee

หลักการ
1. การบริหารจัดการอย่างมีประสิทธิภาพเพื่อให้ผลการดำเนินงานให้เป็นไปตามเป้าหมาย ภายใต้ระดับความเสี่ยงที่ยอมรับได้ 2. กำหนด Infrastructure ให้สอดรับกับนโยบายและกลยุทธ์ ได้แก่ กระบวนการทำงาน ระบบ IT และบุคลากร 3. กำหนด Framework ในการบริหารความเสี่ยง ได้แก่ ระบุ วัด ติดตาม ควบคุม 4. การควบคุมและติดตามการดำเนินงานให้เป็นไปตามเป้าหมาย รวมถึงสั่งการแก้ไขปัญหาอย่างทันกาล 5. การบริหารงานด้วยความโปร่งใส มีธรรมาภิบาล และควบคุมดูแลให้การปฏิบัติงานเป็นไปตามกฎเกณฑ์ทั้งของ สง. และทางการ

ปัจจัยที่ใช้ประเมิน	วิธีการประเมิน
บทบาทหน้าที่ของคณะกรรมการด้านเทคโนโลยีสารสนเทศในการกำกับดูแลงานด้านเทคโนโลยีสารสนเทศ	**(1) โครงสร้างสายงาน IT และบุคลากร** ● ประเมินความเหมาะสมของโครงสร้างการกำกับดูแลงานด้าน IT โครงสร้างองค์กรและสายการบังคับบัญชาในการสนับสนุนให้การดำเนินงาน IT สามารถสนับสนุนธุรกิจตามเป้าหมาย/แผนกลยุทธ์ ● บทบาทหน้าที่ความรับผิดชอบของผู้บริหารระดับสูงของสายงาน IT และที่เกี่ยวข้องมีกำหนดไว้อย่างชัดเจน โดยครอบคลุมกิจกรรมงานด้าน IT ต่าง ๆ ตามโครงสร้างองค์กรที่มีการแบ่งแยกหน้าที่ดีตามหลักการควบคุมงานด้าน IT ที่ดี โดยมีการถ่วงดุลอย่างเหมาะสม ● ผู้บริหารจัดให้มีการพัฒนาบุคลากรอย่างครอบคลุมและต่อเนื่อง รวมถึงการพัฒนาบุคลากรของธนาคารสมาชิกให้สามารถดูแลระบบในส่วนที่เกี่ยวข้องร่วมกัน **(2) กระบวนการและเครื่องมือ** ● ผู้บริหารจัดให้มีกระบวนการและช่องทางประสานงานร่วมกันเพื่อกำกับดูแลงานด้านต่าง ๆ รวมถึงกรณีเกิดเหตุการณ์ปัญหา/ความเสี่ยงที่เกิดขึ้น (ประเมินประสิทธิภาพของ Incident Escalation Process) ● มีกระบวนการ ระบบสารสนเทศ และเครื่องมือเพื่อการบริหารและปรับปรุงประสิทธิภาพของการดำเนินงานด้าน IT เพื่อให้ระบบ IT สามารถสนับสนุนธุรกิจได้ดียิ่งขึ้น ● ประเมินกระบวนการจัดทำและทบทวนแผนกลยุทธ์ด้าน IT การกำหนดแผนงาน/โครงการต่างๆ มีหน่วยงานธุรกิจเข้ามามีส่วนร่วม ● ประเมินแผนกลยุทธ์ด้าน IT ทั้งในระยะสั้นและระยะยาว เพื่อให้แผนกลยุทธ์ด้าน IT มีความสอดคล้องกับนโยบายและกลยุทธ์ของธุรกิจ ● มีกระบวนการและเครื่องมือในการติดตามดูแลแผนงาน/โครงการอย่างใกล้ชิดและต่อเนื่อง พร้อมทั้งมีกระบวนการ/เครื่องมือที่สามารถระบุและ

	ประเมินความเสี่ยงของแผนงาน/โครงการ เพื่อให้ผู้บริหารควบคุมดูแลได้ทันกาล **(3) คณะกรรมการเทคโนโลยีสารสนเทศ (IT Committee)** ● บทบาทหน้าที่ : กำหนดทิศทางและนโยบายการบริหารจัดการด้าน IT ตามแผนกลยุทธ์ทางธุรกิจของธนาคาร รวมถึงกำกับดูแลการดำเนินงานโครงการด้าน IT และการปฏิบัติงานของหน่วยงานด้าน IT โดยมีการประชุมอย่างน้อยเดือนละ 1 ครั้ง ● องค์ประกอบ : มีตัวแทน/กรรมการจากสายงานธุรกิจ ฝ่ายบริหารความเสี่ยงร่วมด้วย มีสมาชิกประกอบด้วยผู้เชี่ยวชาญที่ได้รับการแต่งตั้งโดยคณะกรรมการบริหาร หัวหน้าสายงานบริหารความเสี่ยง และหัวหน้าฝ่ายงานเทคโนโลยีสารสนเทศ ● ประเมินจากรายงานประชุมของคณะกรรมการชุดต่าง ๆ ว่าคณะกรรมการมีการกำกับดูแลและใส่ใจในงานด้าน IT อย่างเพียงพอ
บทบาทหน้าที่ของผู้บริหารระดับสูงในการกำหนดแผนกลยุทธ์ให้สอดคล้องกับเป้าหมายขององค์กร รวมทั้ง การกำกับดูแลการดำเนินงานด้านเทคโนโลยีสารสนเทศ	● การกำหนดทิศทางการดำเนินงาน แนวนโยบายเพื่อผลักดันให้แผนงานต่าง ๆ บรรลุวัตถุประสงค์ขององค์กร โดยพิจารณาจากกระบวนการจัดทำแผนกลยุทธ์โดยมีหน่วยงานธุรกิจเข้าร่วม มีการกำหนดแผนกลยุทธ์ด้าน IT (IT Roadmap) ทั้งในระยะสั้นและระยะยาว ● การติดตามแผนงาน Project Management มีการกำหนดให้มีหน่วยงานที่มีความเป็นอิสระทำหน้าที่ติดตามความคืบหน้าการดำเนินโครงการด้าน IT เพื่อเสนอต่อคณะกรรมการเทคโนโลยีสารสนเทศอย่างสม่ำเสมออย่างน้อยเดือนละครั้ง ● การกำหนด SLA เพื่อใช้ในการติดตามประสิทธิภาพของระบบ IT
บทบาทหน้าที่ของหน่วยงานด้าน IT และผู้บริหารระดับสูงในหน่วยงานด้าน IT	● การจัดโครงสร้างองค์กรและการแบ่งหน้าที่การทำงานในภาพรวม ● บทบาทหน้าที่ของแต่ละหน่วยงาน ชื่อหัวหน้าหน่วยงานพร้อมประวัติการศึกษาและประสบการณ์ทำงาน อัตรากำลัง และจำนวนพนักงานของสายงานที่เกี่ยวข้องต่าง ๆ ดังนี้ o สายงาน IT & IT Security o สายบริหารความเสี่ยง และบทบาทหน้าที่ เฉพาะหน่วยงานที่เกี่ยวข้องกับความเสี่ยงด้าน IT & ความเสี่ยงด้านปฏิบัติการ o สายกำกับการปฏิบัติงาน (Compliance) และบทบาทหน้าที่ เฉพาะหน่วยงานที่เกี่ยวข้องกับการกำกับความเสี่ยงด้าน IT & ความเสี่ยงด้านปฏิบัติการ o สายงานตรวจสอบภายใน และบทบาทหน้าที่ เฉพาะหน่วยงานตรวจสอบด้าน IT

ปัจจัยที่ใช้ประเมิน	วิธีการประเมิน
	• สอบทานการแบ่งแยกหน้าที่อย่างเหมาะสมทั้งระดับองค์กร (เช่น มีการแบ่งแยกการควบคุมด้าน IT ออกเป็น 3 Lines of Defense ประกอบด้วย การบริหารจัดการด้าน IT การบริหารความเสี่ยง การกำกับดูแลการปฏิบัติงาน และการสอบทานผลการปฏิบัติงาน และการแบ่งแยกหน้าที่ภายในสายงาน IT ว่าไม่มี Conflict of Interest • สอบทานความเป็นอิสระของหน่วยงาน Audit & Compliance โดยดูจากสายการบังคับบัญชา การรายงาน การประเมินผลงาน เป็นต้น
บทบาทหน้าที่ของผู้รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Head of IT Security)	• กำหนดนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด • กำหนดให้มีข้อกำหนดด้านความมั่นคงปลอดภัย (security specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT Security architecture) • บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงขององค์กร และนำเสนอความเสี่ยงดังกล่าวต่อคณะกรรมการของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจ หรือคณะกรรมการที่ได้รับมอบหมายเป็นวาระประจำ • ดูแลและดำเนินการให้มีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ • ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้ และความตระหนักรู้เรื่องความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์
บทบาทหน้าที่ของผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (CISO) กรณี ธนาคารพาณิชย์ที่มีนัยสำคัญต่อความเสี่ยงเชิงระบบในประเทศ (D-SIBs)	ธนาคารพาณิชย์ที่มีนัยสำคัญต่อความเสี่ยงเชิงระบบในประเทศ (Domestic Systemically Important Banks : D-SIBs) หรือสถาบันการเงินและสถาบันการเงินเฉพาะกิจที่มีความเสี่ยงตั้งต้นทางไซเบอร์ (cyber inherent risk) ในระดับสูง ตามกรอบการประเมินความพร้อมการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience Assessment Framework : CRAF) นอกจากต้องจำให้มีผู้บริหารที่ทำหน้าที่บริการจัดการความมั่นคงปลอดภัยด้าน IT แล้ว ต่อจัดให้มีผู้บริหารระดับสูงที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (Chief Information Security Officer : CISO) • รายงานปัญหาหรือเหตุการณ์ผิดปกติที่มีนัยสำคัญด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ต่อผู้บริหารสูงสุดหรือคณะกรรมการที่เกี่ยวข้อง หรือคณะกรรมการของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจโดยตรง • ให้ความเห็นในเรื่องการบริหารจัดการความเสี่ยงด้านความมั่งคงปลอดภัยด้าน

	เทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ต่อคณะกรรมของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจ หรือคณะกรรมการที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น IT steering หรือ IT risk committee รวมทั้ง ร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และภัยคุกคามทางไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ

(3) Risk Management หมายถึง ฝ่ายบริหารความเสี่ยง และคณะกรรมการบริหารความเสี่ยง (Risk Management Committee)

หลักการ
เพื่อให้ สง. มีการบริหารความเสี่ยงด้าน IT ที่เหมาะสมกับการทำธุรกรรม และความซับซ้อนของระบบงาน

ปัจจัยที่ใช้ประเมิน	**วิธีการประเมิน**
บทบาทหน้าที่ของหน่วยงานที่เกี่ยวข้องกับการบริหารความเสี่ยง	• โครงสร้างและบุคลากรในหน่วยงานบริหารความเสี่ยง (ด้าน IT และด้านการทุจริต) o โครงสร้างของหน่วยงานมีความเป็นอิสระและครอบคลุมให้สามารถเชื่อมโยงความเสี่ยงด้าน IT และความเสี่ยงด้านต่าง ๆ o การกำหนดบทบาทหน้าที่ความรับผิดชอบที่ชัดเจนเป็นลายลักษณ์อักษร o บุคลากรมีความเพียงพอสอดคล้องกับขนาดของธุรกิจ มีประสบการณ์ มีความเชี่ยวชาญและได้รับการฝึกอบรมเพิ่มความรู้อย่างต่อเนื่อง
นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการทุจริต (เชิง Preventive)	• นโยบาย/การประเมินความเสี่ยงด้าน IT และแนวทางการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ได้แก่ o ผลการประเมินความเสี่ยงด้าน IT ล่าสุด และการจัดลำดับความเสี่ยงด้าน IT o แผนการลดความเสี่ยงด้าน IT ให้อยู่ในระดับที่ยอมรับได้ o การดำเนินการตามแผนลดความเสี่ยงด้าน IT o การติดตามและรายงานความเสี่ยงด้าน IT • นโยบายการควบคุมการทุจริต เช่น มีนโยบายหรือแผนในการควบคุม Loss ที่เกิดจากการทุจริตทั้งปี ไม่ให้เกิน 0.03% ของรายได้
กระบวนการและเครื่องมือที่ใช้ในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการทุจริต (เชิง Detective)	• **กระบวนการ** • กระบวนการระบุ ประเมิน ควบคุมและติดตามความเสี่ยงด้าน IT และประสิทธิภาพของแนวทางการควบคุมความเสี่ยงเพื่อให้มั่นใจว่ามีการบริหารจัดการความเสี่ยงภายใต้ระดับที่ยอมรับได้ (Risk Tolerance Level) โดยกระบวนการดังกล่าวควรครอบคลุมระบบของบริษัทและที่เชื่อมโยงกับระบบของสมาชิก • ผลการประเมินความเสี่ยงด้าน IT ล่าสุด และการจัดลำดับความเสี่ยงด้าน IT • กระบวนการรายงานผลประเมินและการทดสอบความเสี่ยงในด้านต่าง ๆ ให้คณะกรรมการที่ได้รับมอบหมายรับทราบ เช่น Risk Assessment,

	ผลการทดสอบแผนฉุกเฉิน หรือรายงาน Loss/Incident เป็นต้น ● กรอบแนวทางในการจัดการความเสี่ยงด้าน IT ที่ชัดเจนเป็นลายลักษณ์อักษร มีการทบทวนความเหมาะสมอย่างต่อเนื่องเป็นประจำ เพื่อให้มั่นใจว่ามีการ ควบคุมความเสี่ยงสอดคล้องตามมาตรฐานที่กำหนด *[สำหรับผู้ให้บริการ Switching/Clearing Refer to ภาคผนวก ข : ตารางการควบคุมที่สำคัญ 6. Switching/ Clearing ข้อ 6.1-6.3, 6.14-6.15]* **(2) เครื่องมือ** ● เครื่องมือที่ใช้ ความเพียงพอและเหมาะสมของเครื่องมือหรือวิธีการที่ใช้ในระบุ ชี้วัด ติดตามและรายงานความเสี่ยงด้าน IT และปัญหาที่เกิดขึ้น เช่น RCSA, KRI, Loss Data หรือ Incident & Problem Report เป็นต้น ● เครื่องมือในการติดตามความปลอดภัยต่าง ๆ ● Fraud Monitoring มีกระบวนการหรือระบบที่ใช้ในการเฝ้าระวังและติดตามการทุจริต **(3) การใช้บริการ IT Outsourcing** ● แนวทางการบริหารความเสี่ยงจากการใช้บริการ IT Outsourcing สอดคล้องตามประกาศ ธปท. ● ขอบเขตงานหรือบริการที่มีการใช้ IT Outsourcing จาก Service Providers ● สอบทานความเพียงพอของรายงานการติดตาม ประเมินผล และตรวจสอบ ● การปฏิบัติงานของ Service
IT incident & Problem Management (เชิง Corrective)	● กระบวนการบริหารจัดการ Incident & Problem Management ครอบคลุมหน่วยงาน/ฝ่ายงานรับผิดชอบ คู่มือปฏิบัติงาน กระบวนการ และเครื่องมือรองรับการปฏิบัติงาน ตั้งแต่การรับแจ้งจนถึงการแก้ไข *[Refer to ภาคผนวก ข : ตารางการควบคุมที่สำคัญ 6. Switching/ Clearing ข้อ 6.4, 6.5, 6.7]* ● โครงสร้างการกำกับดูแลและควบคุมติดตาม Incident & Problem Management Process ตลอดจนการรายงานให้คณะกรรมการผู้บริหารระดับสูง และหน่วยงานบริหารความเสี่ยง
Loss Incident ที่เกี่ยวข้อง	● สอบทานรายงาน Loss Data, รายงาน Incident, รายงาน Problem จาก Help Desk (ถ้ามี) Loss Incident ที่สำคัญ ให้สรุปเรื่อง สาเหตุ และการแก้ไข หรือแนบไฟล์สรุปเรื่องของธนาคาร

(4) Compliance หมายถึง หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์

หลักการ
การดำเนินธุรกิจภายใต้กฎหมาย กฎเกณฑ์ ข้อบังคับ มาตรฐานและแนวปฏิบัติที่บังคับใช้กับธุรกรรมต่าง ๆ ของ สง.

ปัจจัยที่ใช้ประเมิน	วิธีการประเมิน
บทบาทหน้าที่ของหน่วยงานด้านการกำกับดูแลการปฏิบัติตามกฎเกณฑ์ทางการ	**(1) โครงสร้างและบุคลากร** หน่วยงาน Compliance ● สอบทานโครงสร้างองค์กรสายการบังคับบัญชาและการรายงานต่อผู้ที่เกี่ยวข้องโดยพิจารณาถึงความเป็นอิสระจากหน่วยงานธุรกิจ ● มีการกำหนดบทบาทหน้าที่ ความรับผิดชอบที่ชัดเจน เป็นลายลักษณ์อักษร และมีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่เป็น 1st line of defense ● บุคลากรมีความเพียงพอสอดคล้องกับขนาดของธุรกิจ มีประสบการณ์ มีความเชี่ยวชาญและได้รับการฝึกอบรบเพิ่มความรู้อย่างต่อเนื่อง **(2) กระบวนการ** ● สอบทานการปฏิบัติงานของหน่วยงานธุรกิจ (Business Unit) ว่ามีความสอดคล้องกับกฎหมาย กฎเกณฑ์ทางการและมาตรฐานสากลด้าน IT ที่เกี่ยวข้อง ● มีกระบวนการติดตามและรายงานความคืบหน้าข้อสังเกตที่ตรวจพบให้คณะกรรมการที่ได้รับมอบหมายรับทราบ ● มีการกำหนดแผนการบริหารความเสี่ยงด้านปฏิบัติการประจำปีครอบคลุมกฎหมายที่เกี่ยวข้อง สุ่มสอบทานการปฏิบัติตามกฎเกณฑ์และให้ความรู้แก่พนักงานในเรื่องกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง **(3) เครื่องมือ** ● สอบทานความเพียงพอและเหมาะสมของเครื่องมือที่ใช้ ● มีกระบวนการแจ้ง ธปท. ในเรื่องที่เกี่ยวข้องกับระบบงานสารสนเทศที่มีนัยสำคัญ เช่น การเปลี่ยนแปลงเทคโนโลยี การแจ้ง IT Incident ที่สำคัญ
ความคืบหน้าและการแก้ไขตามข้อสังเกตหรือคำแนะนำของ ธปท.	● สอบทานรายงานความคืบหน้าการแก้ไขข้อสังเกตของ ธปท. เฉพาะข้อสังเกตที่ยังแก้ไขไม่แล้วเสร็จ

(5) Internal Audit หมายถึง หน่วยงานตรวจสอบภายใน

หลักการ
1. การสอบทานและประเมินประสิทธิภาพการดำเนินงานขององค์กร เพื่อสนับสนุนให้ผู้ปฏิบัติงานทุกระดับขององค์กรสามารถปฏิบัติหน้าที่เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้องอย่างมีประสิทธิภาพยิ่งขึ้น รวมถึงการป้องกันไม่ให้เกิดการทุจริต 2. รายงานผลการตรวจสอบมีประโยชน์ต่อการตัดสินใจของผู้บริหาร รวมถึงสนับสนุนให้มีระบบการควบคุมภายในที่มีประสิทธิภาพ

ปัจจัยที่ใช้ประเมิน	วิธีการประเมิน
บทบาทหน้าที่ของหน่วยงานตรวจสอบภายใน	**โครงสร้างและบุคลากร** หน่วยงานตรวจสอบภายใน ● โครงสร้างของหน่วยงานและสายการบังคับบัญชามีความชัดเจนและเป็นอิสระ มีการกำหนดบทบาทหน้าที่ ความรับผิดชอบที่ชัดเจนเป็นลายลักษณ์อักษร ● บุคลากรมีความเพียงพอสอดคล้องกับขนาดของธุรกิจ มีประสบการณ์ มีความเชี่ยวชาญและได้รับการฝึกอบรบเพิ่มความรู้อย่างต่อเนื่อง
การสอบทานโดยผู้ตรวจสอบภายใน	● **ประเมินความเป็นอิสระ นโยบายและแผนการตรวจสอบ**ครอบคลุมเหมาะสม (ควรครอบคลุมกิจกรรมงาน IT ที่มีความเสี่ยง) เครื่องมือที่ใช้ตรวจ และประสิทธิภาพในการติดตามและปิดข้อสังเกต ● **กระบวนการ** มีกระบวนการตรวจสอบที่ครอบคลุมกิจกรรมงาน IT ที่สำคัญ ตั้งแต่การกำหนดนโยบาย การจัดทำแผนการตรวจสอบ การรายงานให้คณะกรรมการที่ได้รับมอบหมายให้รับทราบ รวมถึงการติดตามการแก้ไขประเด็นที่พบจากการตรวจสอบ ● **เครื่องมือ** ความเพียงพอและเหมาะสมของเครื่องมือที่ใช้ในการตรวจสอบและติดตามการแก้ไขข้อสังเกต ทั้งของหน่วยงานตรวจสอบภายใน ผู้ตรวจสอบภายนอก และ ธปท. และหน่วยงานกำกับดูแลอื่น ๆ ● ประเมินคุณภาพของการตรวจสอบ ข้อเสนอแนะ และการรายงานต่อคณะกรรมการตรวจสอบ รวมถึงการสั่งการและการติดตามการแก้ไขปัญหาของคณะกรรมการตรวจสอบ

ส่วนที่ 4 การประเมินความเสี่ยงสุทธิ (Net Risk)

Net Risk หมายถึง ความเสี่ยงสุทธิของระบบ IT ที่คงเหลืออยู่ ภายหลังบริหารจัดการ Inherent risk ด้วย QRM แล้ว หาก Net Risk อยู่ในระดับสูง สง. ควรดำเนินการแก้ไขปรับปรุง QRM ให้มีประสิทธิภาพมากขึ้น

การประเมิน Net Risk เริ่มจากประเมิน IR ตาม “ส่วนที่ 2 การประเมิน Inherent Risk (IR)” และประเมิน QRM ตาม “ส่วนที่ 3 การประเมิน Quality of Risk Management (QRM)” ว่าอยู่ในระดับใดตามตารางการให้ rating (ตารางที่ 1) ด้านล่างนี้

ตารางที่ 1 การให้ rating

Inherent Risk – Quality of Risk Management = Net Risk → Direction of Net Risk

Inherent Risk (IR)	Quality of Risk Management (QRM)	Net Risk	Direction of Risk
● ต่ำ ● ปานกลาง ● สูง	● ดี ● พอใช้ ● อ่อน	● ต่ำ ● ค่อนข้างต่ำ ● ปานกลาง ● ค่อนข้างสูง ● สูง	● เพิ่มขึ้น ● คงที่ ● ลดลง

และนำผลของระดับ IR และ QRM มาพิจารณา Net Risk ตามตารางที่ 2 SA risk matrix แบบ 5 x 5

ตารางที่ 2 SA risk matrix แบบ 5 x 5

QRM / IR	ดี	ดี + พอใช้	พอใช้	พอใช้ + อ่อน	อ่อน
ต่ำ	ต่ำ	ต่ำ	ค่อนข้างต่ำ	ค่อนข้างต่ำ	ปานกลาง
ต่ำ + กลาง	ต่ำ	ค่อนข้างต่ำ	ค่อนข้างต่ำ	ปานกลาง	ค่อนข้างสูง
ปานกลาง	ค่อนข้างต่ำ	ค่อนข้างต่ำ	ปานกลาง	ค่อนข้างสูง	ค่อนข้างสูง
กลาง + สูง	ค่อนข้างต่ำ	ปานกลาง	ปานกลาง	ค่อนข้างสูง	สูง
สูง	ค่อนข้างต่ำ	ปานกลาง	ค่อนข้างสูง	ค่อนข้างสูง	สูง

ทั้งนี้ SA แต่ละตัวมีปัจจัยที่ใช้ประเมิน IR และ QRM หลายด้าน ซึ่งอาจมีผลการประเมินที่แตกต่างกัน เช่น SA-IT มี IR ด้านกลยุทธ์ปลานกลาง แต่มี IR ด้านปฏิบัติการสูง ในขณะที่ QRM แต่ละด้านมีผลการประเมินอยู่ทั้งในระดับดี พอใช้และอ่อน จึงเป็นดุลยพินิจของทีมตรวจสอบที่ต้องพิจารณา ว่าควรใช้ rating ของ IR และ QRM ที่ระดับใด เพื่อประเมิน Net risk ของ SA นั้น ๆ ตาม SA risk matrix แบบ 5x5 (ตารางที่ 2) ข้างต้น โดยควรมีการระบุเหตุผลหรือความเห็นทีมตรวจที่ชัดเจนไว้

ส่วนที่ 5 การประเมินแนวโน้มความเสี่ยง (Direction of Net Risk)

5.1 คำจำกัดความ

แนวโน้มความเสี่ยง หมายถึง โอกาสที่ความเสี่ยงสุทธิของระบบ IT จะเปลี่ยนแปลงไปจากเดิมที่ได้ประเมินไว้ (ใน 1 ปีข้างหน้า) ซึ่งเกิดจากการเปลี่ยนแปลงของความเสี่ยงที่มีอยู่ของระบบ IT (Inherent Risk : IR) และ/หรือคุณภาพการบริหารจัดการความเสี่ยง (Quality of Risk Management : QRM)

5.2 หลักการพิจารณา

ปัจจัยที่ใช้ประเมิน	แนวโน้มความเสี่ยง		
	ลดลง	คงที่	เพิ่มขึ้น
ปัจจัยภายใน			
การเปลี่ยนแปลงเทคโนโลยี	โครงสร้างระบบ IT ที่สำคัญ ได้ผ่านการปรับปรุงในด้านการเพิ่มประสิทธิภาพ (S,I,A) และความทันสมัยต่อการรองรับการดำเนินธุรกิจ รวมถึงแนวโน้มธุรกิจในอนาคต	โครงสร้างระบบ IT ปัจจุบันเพียงพอรองรับการดำเนินธุรกิจตามแผนกลยุทธ์ อย่างไรก็ดี ธนาคารมีแผนจะดำเนินการเปลี่ยนแปลงด้าน IT เพื่อเพิ่มประสิทธิภาพและความทันสมัยในการรองรับแนวโน้มธุรกิจในอนาคต	โครงสร้างระบบ IT ที่สำคัญมีการใช้งานมานาน โดยยังไม่มีแผน / แนวทางจะปรับปรุงแก้ไข อีกทั้งมีสัญญาณบ่งชี้ว่าอาจมีความเสี่ยงที่ส่งผลกระทบต่อประสิทธิภาพในการปฏิบัติงานด้าน IT (S,I,A) ให้รองรับการดำเนินธุรกิจ รวมถึงแนวโน้มธุรกิจในอนาคต เช่น ผู้ผลิตยกเลิกการ support ระบบ IT สำคัญ

	มีการกำกับดูแลและกระบวนการในการติดตามดูแลความเสี่ยง/ปัญหาต่าง ๆ ภายหลังการปรับปรุงโดยใกล้ชิด เพื่อให้สามารถรับทราบปัญหาและแก้ไขได้เร็วและมีประสิทธิภาพ	มีการกำหนดโครงสร้างการกำกับดูแล กระบวนการและแนวทางการควบคุมดูแลการปฏิบัติงานตามแผนและความเสี่ยงไว้ชัดเจนเพียงพอตามสมควร	ธนาคารยังไม่มีแนวทางแก้ไขปัญหาด้าน IT ที่ส่งผลกระทบต่อการให้บริการอย่างชัดเจน
ปัจจัยภายนอก			
ภัยคุกคามรูปแบบใหม่ ๆ ที่มีผลต่อระบบงานสำคัญ (New Technology Threat)	สง. ได้ดำเนินการปรับปรุงแก้ไข โดยปิดช่องโหว่ความเสี่ยงของภัยคุกคามรูปแบบใหม่ ๆ แล้ว	สง. ทราบถึงความเสี่ยงและมีแนวทางที่จะปรับปรุงแก้ไขที่สามารถป้องกันความเสี่ยงที่ชัดเจนแล้ว	สง. อาจยังไม่ทราบถึงความเสี่ยง หรือยังไม่มีแนวทางจะปรับปรุงแก้ไขช่องโหว่ในระบบงาน

ภาคผนวก ก แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบ IT ที่สนับสนุนธุรกิจหลัก

สรุปความหมายโดยย่อของคำศัพท์ที่สำคัญ

ศูนย์คอมพิวเตอร์ (Data Center)	ศูนย์รวมของเครื่องและอุปกรณ์คอมพิวเตอร์สำคัญของธนาคารที่ใช้ประมวลผลกลางรองรับการดำเนินธุรกิจและการให้บริการของธนาคาร เช่น ระบบ Core Banking เป็นต้น
ระบบเครือข่ายสื่อสาร (Network)	ระบบเครื่องมือสื่อสารที่ใช้รองรับการเชื่อมโยงเครื่องคอมพิวเตอร์ อุปกรณ์ ระบบงาน และช่องทางบริการจากที่ต่าง ๆ เข้าหากัน
ระบบ Core Banking	ระบบประมวลผลกลางที่มีความสำคัญอย่างยิ่งสำหรับรองรับการประมวลผลธุรกรรมหลักของธนาคาร เช่น ธุรกรรมฝากถอน และโอนเงิน เป็นต้น รวมทั้งสามารถรองรับการทำธุรกรรมจากช่องทางต่าง ๆ ของธนาคาร เช่น สาขา ATM และ Internet Banking เป็นต้น
ระบบงานการให้บริการแก่ลูกค้า	เครื่องคอมพิวเตอร์ อุปกรณ์ หรือระบบที่ใช้รับรายการธุรกรรมของลูกค้าเพื่อส่งไปประมวลผลที่ระบบประมวลผลกลาง เช่น เครื่องคอมพิวเตอร์ที่เจ้าหน้าที่สาขาใช้ปฏิบัติงาน ตู้ ATM ระบบ Internet Banking เป็นต้น
Hardware Security Module (HSM)	อุปกรณ์ที่ใช้ในการสร้างและตรวจสอบความถูกต้องของรหัสในการทำธุรกรรม
Network Time Protocol (NTP) Server	เครื่อง server ที่ใช้ปรับเทียบเวลา (Time Synchronization) กับเวลามาตรฐานสากล เพื่อให้เวลาของเครื่องและอุปกรณ์คอมพิวเตอร์ของธนาคารถูกต้องตรงกับเวลามาตรฐานของกรมอุทกศาสตร์
Secure Socket Layer (SSL)	ช่องทางการรับส่งข้อมูลที่มีความปลอดภัย
Two-Factor Authentication (2FA)	วิธีการพิสูจน์ตัวตนของผู้ทำรายการโดยใช้ข้อมูล 2 อย่างประกอบกัน ซึ่งข้อมูลดังกล่าวมี 3 ประเภท ได้แก่ 1) Something You Know เช่น User ID และ Password เป็นต้น 2) Something You Have เช่น บัตร ATM รหัสยืนยันการทำรายการที่ได้รับจากธนาคาร (One Time Password

	(OTP)) เป็นต้น และ 3) Something You Are เช่น ลายนิ้วมือ เป็นต้น ตัวอย่างการใช้ Two-Factor Authentication เช่น การใช้บัตร ATM คู่กับ รหัส PIN ในการทำรายการที่ตู้ ATM และการใช้ User ID และ Password ควบคู่กับรหัส OTP ในการทำรายการโอนเงินผ่าน Internet Banking เป็นต้น
One Time Password (OTP)	รหัสผ่านที่ใช้เพียงครั้งเดียวสำหรับยืนยันการทำธุรกรรมผ่าน Internet หรือ Mobile Banking ที่อาจส่งให้ลูกค้าทางมือถือก่อนอนุมัติทำรายการ
Token	อุปกรณ์สร้างและ/หรือรับรหัส OTP ที่มีความปลอดภัยสูง สำหรับใช้ในการยืนยันตัวตนของลูกค้าที่ทำธุรกรรมทางการเงินผ่าน Internet และ/หรือ Mobile Banking โดยสามารถป้องกันการถูกลักลอบโอนเงินออกจากบัญชีโดยกลุ่มมิจฉาชีพที่มีความเชี่ยวชาญด้านคอมพิวเตอร์ได้
Service Level Agreement (SLA)	สัญญาหรือข้อตกลงการให้บริการ ระหว่างผู้รับบริการและผู้ให้บริการ ซึ่งอาจเป็นสถาบันการเงินกับผู้ให้บริการภายนอกหรือหน่วยงานธุรกิจกับหน่วยงาน IT

หมายเหตุ : ความหมายของคำศัพท์นี้เป็นความหมายโดยย่อที่จัดทำขึ้นเพื่อมุ่งเน้นให้ผู้อ่านสามารถเข้าใจได้ง่ายและใช้อ้างอิงเฉพาะในแนวปฏิบัติฉบับนี้

ตารางการระบุความเสี่ยงขององค์ประกอบด้าน IT

ประเภทความเสี่ยง	**ศูนย์คอมพิวเตอร์ (Data Center)**	**ระบบเครือข่ายสื่อสาร (Network)**	**ระบบ Core Banking**	**ระบบงานการให้บริการแก่ลูกค้า**[1]
การฉ้อโกงโดยบุคคลภายใน (Internal Fraud) เช่น - การเข้าถึง การขโมย การเปลี่ยนแปลงแก้ไข หรือการทำลายข้อมูลระบบงาน/ ข้อมูลโดยไม่ได้รับอนุญาต (Hacking)	✓	✓	✓	✓
การฉ้อโกงโดยบุคคลภายนอก (External Fraud) เช่น - การเข้าถึง การขโมย การปลอมแปลงหรือการทำลายข้อมูลระบบงาน/	✓	✓	✓	✓

ข้อมูลโดยไม่ได้รับอนุญาต หรือภัยคุกคามรูปแบบต่าง ๆ (Hacking)				
ความเสียหายต่อทรัพย์สิน (Damage to Physical Assets) เช่น - ภัยพิบัติทางธรรมชาติ - การก่อการร้าย	✓	✓		
การที่ธุรกิจหยุดชะงักและระบบงานขัดข้องโดยไม่สามารถใช้งานได้ตามปกติ (Business Disruption and System Failures) เช่น - ระบบงานล้าสมัย - การปฏิบัติงานผิดพลาด (Human Error)	✓	✓	✓	

[1] *ระบบงานการให้บริการแก่ลูกค้า หมายถึง ระบบงานสาขาและเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงาน (PC Teller) ระบบและเครื่อง Automatic Teller Machine (ATM) และระบบ Internet Banking*

1 ศูนย์คอมพิวเตอร์ (Data Center)

1.1 การควบคุมการเข้าถึงศูนย์คอมพิวเตอร์ทางกายภาพ (Physical Access Control)

<u>วัตถุประสงค์</u> เพื่อป้องกันและเฝ้าระวังรักษาความปลอดภัยศูนย์คอมพิวเตอร์(ศูนย์ฯ) และพื้นที่สำคัญภายในศูนย์ฯ จากการเข้าถึงโดยไม่ได้รับอนุญาต การทำลายทรัพย์สิน ความเสียหาย และภัยคุกคามรูปแบบต่าง ๆ

<u>แนวปฏิบัติที่ดี</u>

- มีการควบคุมทางกายภาพและมีระบบควบคุมการเข้าถึงตัวอาคารศูนย์คอมพิวเตอร์หลัก (ศูนย์ฯ) และพื้นที่สำคัญ ต่าง ๆ ภายในศูนย์ฯ ได้แก่ ห้องจัดเก็บเครื่องประมวลผล ห้องจัดเก็บอุปกรณ์เครือข่าย ห้องจัดเก็บสื่อบันทึกข้อมูล ห้องจัดเก็บอุปกรณ์สาธารณูปโภค และห้องปฏิบัติงาน เป็นต้น (พื้นที่สำคัญฯ) ให้เข้าถึงได้เฉพาะบุคคลที่ได้รับ อนุญาตตามสิทธิ์ที่ได้รับมอบหมายเท่านั้น โดยระบบควบคุมควรมีความสามารถอื่น ๆ ดังต่อไปนี้
    - การใช้ Two-Factor Authentication ในการพิสูจน์ตัวตนของผู้เข้าออกพื้นที่สำคัญภายในศูนย์ฯ ได้แก่ ห้องจัดเก็บเครื่องประมวลผล ห้องจัดเก็บอุปกรณ์เครือข่าย ห้องจัดเก็บสื่อบันทึกข้อมูล เช่น Access Card Door + PIN รวมถึงระบบการควบคุมการเข้าออกสามารถป้องกันการหมุนเวียนบัตร (Pass Back) และการแอบลักลอบเข้ามาพร้อมผู้มีสิทธิ์ (Piggy Back)
    - สามารถบันทึกและจัดเก็บ Log Files ของการเข้าถึงศูนย์ฯ และพื้นที่สำคัญภายในศูนย์ฯ ได้อย่างถูกต้องแม่นยำ และมีรายละเอียดเพียงพอสำหรับใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้โดยเก็บย้อนหลังเป็นระยะเวลาอย่างน้อย 90 วัน ไว้ในสถานที่ที่มีความมั่นคง ปลอดภัย
    - สามารถแจ้งเตือนผู้เกี่ยวข้องเมื่อเกิดเหตุผิดปกติได้อย่างทันการณ์ตลอด 24x7 ชม. เช่น เมื่อพบการพยายามเข้าถึงพื้นที่สำคัญภายในศูนย์ฯ โดยผู้ไม่ได้รับอนุญาต การผ่านเข้า-ออก

ศูนย์ฯ ทางประตูหนี ไฟ การเปิดประตูค้างไว้ เป็นต้น

นอกจากนี้ มีการควบคุมการเข้าถึงทางกายภาพพื้นที่รอบนอกศูนย์ฯ ที่เหมาะสม เช่น มีกำแพงหรือรั้วที่มั่นคง มีเจ้าหน้าที่ตรวจสอบการผ่านเข้า-ออกและมีการตรวจสอบยานพาหนะ เป็นต้น อีกทั้งมีการแบ่งแยกพื้นที่ ลานจอดรถบุคคลภายนอก (Visitor Parking Area) รวมถึงพื้นที่/อุปกรณ์ที่ใช้ในการขนส่งสินค้า (Loading Docks) ออกจากบริเวณศูนย์ฯ

- มีการติดตั้งกล้องวงจรปิดบริเวณรอบนอกอาคารศูนย์ฯ ประตูทางเข้าศูนย์ฯ และภายในศูนย์ฯ อย่างทั่วถึง เพื่อใช้เป็นเครื่องมือสำคัญในการติดตามการเข้า-ออก และการกระทำต่างๆ ภายในศูนย์โดยเก็บบันทึกภาพจากกล้อง วงจรปิดไว้เป็นระยะเวลาอย่างน้อย 90 วัน และให้ภาพที่จัดเก็บมีความชัดเจนเพียงพอที่จะใช้ในการพิสูจน์หลักฐาน
- มีเจ้าหน้าที่ดูแลรักษาความปลอดภัยศูนย์ฯ เฝ้าระวังผ่านระบบกล้องวงจรปิด (CCTV) ตลอดเวลา (24x7)
- ห้ามไม่ให้นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่สามารถบันทึกภาพ/เสียงได้เข้ามาภายในพื้นที่สำคัญภายในศูนย์ฯ ได้แก่ ห้องจัดเก็บเครื่องประมวลผล ห้องจัดเก็บอุปกรณ์เครือข่าย ห้องจัดเก็บสื่อบันทึกข้อมูล เว้นแต่จะได้รับอนุญาตโดยผู้ที่มีอำนาจอนุมัติ
- เครื่องประมวลผลและอุปกรณ์เครือข่ายควรถูกจัดเก็บอยู่ในตู้Rack ที่มีการปิดล็อกอยู่ตลอดเวลา และการเข้าถึงต้องเป็นแบบ Dual Control
- มีกระบวนการจัดการสิทธิ์และหน่วยงานที่รับผิดชอบชัดเจนในการเข้าถึงศูนย์ฯ และพื้นที่สำคัญฯ ให้เป็นไปตามหลักความจำเป็น ถูกต้อง และเป็นปัจจุบัน ดังนี้
    - มีการจัดทำตารางการควบคุมการให้สิทธิ์ที่สอดคล้องกับตำแหน่งหน้าที่งานเพื่อใช้เป็นแนวทางการกำหนดสิทธิ์อย่างเป็นระบบและเป็นปัจจุบัน (Authorization Matrix) และมีการทบทวนตารางควบคุมการให้สิทธิ์(Authorization Matrix) ทุกครั้งที่มีการเปลี่ยนแปลงหรือเป็นประจำอย่างน้อยทุก 6 เดือน
    - การอนุมัติการเข้าถึงศูนย์ฯ และพื้นที่สำคัญต่าง ๆ ภายในศูนย์ฯ ต้องดำเนินการโดยผู้ที่มีอำนาจอนุมัติ และสอดคล้องตามตารางการควบคุมการให้สิทธิ์
    - มีการปรับปรุง/ ยกเลิกสิทธิ์การเข้า–ออกศูนย์ฯ ทันทีที่พนักงานลาออก โยกย้าย หรือเปลี่ยนหน้าที่ความรับผิดชอบ
    - มีการทบทวนสิทธิ์การเข้า-ออกศูนย์ฯ โดยผู้ที่มีอำนาจอนุมัติอย่างสม่ำเสมออย่างน้อยทุก 6 เดือน
- การเข้าถึงโดยพนักงานที่ไม่ได้มีหน้าที่ปฏิบัติงานประจำภายในศูนย์ฯ หรือบุคคลภายนอกมีกระบวนการในการควบคุมการเข้าถึงแบบชั่วคราว ดังนี้
    - มีการอนุมัติโดยผู้มีอำนาจอนุมัติก่อนทุกครั้ง
    - มีการมอบหมายให้มีเจ้าหน้าที่ศูนย์ฯ ติดตาม (Escort) ผู้เข้าถึงแบบชั่วคราวตลอดระยะเวลาที่เข้ามาปฏิบัติงานภายในศูนย์ฯ
    - มีเจ้าหน้าที่ควบคุมการลงบันทึกเข้า-ออกศูนย์ฯ โดยมีขั้นตอนและเครื่องมือที่สามารถระบุตัวตนของผู้ที่ได้รับอนุญาตให้เข้าถึงศูนย์ฯ แบบชั่วคราว พร้อมทั้งจัดทำทะเบียนคุมสำหรับลงบันทึกการเข้า-ออก ศูนย์ฯ ที่มีรายละเอียดเพียงพอสำหรับใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลได้
- มีกระบวนการสอบทาน Log Files ตลอดจนทะเบียนคุมการเข้า-ออกศูนย์ฯ โดยผู้ที่มีอำนาจอนุมัติอย่างสม่ำเสมออย่างน้อยทุก 30 วัน เพื่อติดตามการเข้าถึงศูนย์ฯ ที่ผิดปกติ เช่น ช่วงเวลาหรือ

ความถี่ที่ผิดปกติหรือการพยายาม เข้าถึงโดยบุคคลไม่เหมาะสม

1.2 การบริหารจัดการศูนย์ฯ (Facility Management)

วัตถุประสงค์ เพื่อให้ศูนย์คอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศมีความพร้อมใช้งานรองรับธุรกิจอย่างต่อเนื่อง

แนวปฏิบัติที่ดี

- จัดให้มีการประเมินความเสี่ยงของศูนย์ฯ ครอบคลุมปัจจัยเสี่ยงอย่างน้อยในเรื่องความปลอดภัยของพื้นที่รอบนอกศูนย์ฯ ตัวอาคารศูนย์ฯ และภายในศูนย์ฯ ความพร้อมใช้ของระบบสาธารณูปโภค ประสิทธิภาพระบบป้องกันภัยต่าง ๆ และความเพียงพอของการปฏิบัติงานภายในศูนย์ฯ การประเมินความเสี่ยงควรดำเนินการอย่างน้อยเป็นประจำทุกปี และเมื่อมีการเปลี่ยนแปลงที่สำคัญ โดยมีการบันทึกไว้เป็นลายลักษณ์อักษรและนำเสนอต่อคณะกรรมการที่ได้รับมอบหมายเพื่อรับทราบและ/ หรือขออนุมัติแผนปิด/ ลดความเสี่ยง
- ในการสร้างศูนย์ฯ สถานที่ตั้งไม่อยู่ในพื้นที่เสี่ยงภัย เช่น ตั้งอยู่ใกล้ปั๊มน้ำมัน ปั๊มแก๊ส หรือทางด่วน ควรกำหนดเป็นปัจจัยหนึ่งของการพิจารณาที่ตั้งของศูนย์ฯ สำหรับกรณีศูนย์ฯ ในปัจจุบันควรจัดให้มีมาตรการรองรับเหตุฉุกเฉินจากภัยพิบัติต่าง ๆ
- สถานที่ตั้งศูนย์ฯ อยู่แยกจากอาคารสานักงาน (Stand Alone) โดยมีการออกแบบโครงสร้างอาคาร สถานที่ และการติดตั้งระบบสาธารณูปโภคที่เหมาะสม
- โครงสร้างตัวอาคารศูนย์ฯ ถูกออกแบบให้สามารถรองรับภัยต่าง ๆ ในระดับที่เหมาะสม ปลอดภัย และยากต่อการทำลาย ดังนี้
    - การบุกรุก การทุบทำลาย และการรองรับแรงระเบิด
    - การป้องกันอัคคีภัย ผนังภายนอกศูนย์ฯ สามารถกันไฟได้อย่างน้อย 4 ชั่วโมง ผนังภายในที่กั้นพื้นที่สำคัญสามารถกันไฟได้อย่างน้อย 2 ชั่วโมง และผนังกั้นพื้นที่อื่น ๆ สามารถกันไฟได้อย่างน้อย 1 ชั่วโมง
- ระบบไฟฟ้าสำหรับศูนย์คอมพิวเตอร์
    - เส้นทางจ่ายไฟจากภายนอกมายังศูนย์ฯ มีจำนวนเส้นทางจ่ายไฟ (Feeders) จากสถานีจ่ายไฟของการไฟฟ้า (Substation) มายังศูนย์ฯ อย่างน้อย 2 เส้นทาง โดยมีการจ่ายไฟพร้อมกันทั้ง 2 เส้นทาง (Active/Active)
    - เส้นทางจ่ายไฟภายในศูนย์ฯ มีจำนวนเส้นทางจ่ายไฟภายในศูนย์ฯ ตั้งแต่อุปกรณ์รับไฟฟ้าแรงสูง (High Voltage), หม้อแปลงไฟฟ้า (Transformer), อุปกรณ์สลับการรับกระแสไฟฟ้า (Automatic Transfer Switch (ATS)) และอุปกรณ์ปรับแรงดันและสำรองไฟฟ้า (Uninterrupted Power Supply (UPS)) ไปจนถึงอุปกรณ์ภายในศูนย์ฯ อย่างน้อย 2 เส้นทาง โดยมีการจ่ายไฟพร้อมกันทั้ง 2 เส้นทาง (Active/Active)
    - อุปกรณ์คอมพิวเตอร์และอุปกรณ์สาธารณูปโภคภายในศูนย์ฯ ควรรองรับกระแสไฟฟ้าจากสองเส้นทาง (Dual Sources) แต่หากอุปกรณ์ใดไม่สามารถรับไฟจาก 2 เส้นทางได้ ต้องมีการติดตั้งอุปกรณ์ Static Transfer Switch (STS)[1]
    - มีการติดตั้งอุปกรณ์ระบบไฟฟ้า เช่น High Voltage , Transformer, ATS เพื่อรองรับการทำงานของอุปกรณ์สำคัญในศูนย์ฯ แบบ 2 ชุด โดยแต่ละชุดมีเส้นทางการเดินกระแสไฟแยกจากกันและตั้งอยู่คนละห้อง (Compartmentalization) หากอุปกรณ์ชุดใดชุดหนึ่งหยุดชะงัก/ บำรุงรักษา อีกชุดต้องสามารถจ่ายไฟแทนได้อย่างต่อเนื่อง ทั้งนี้แต่ละชุดควร

ติดตั้งให้ครอบคลุมความเสี่ยงจากกรณีที่เครื่องใดเครื่องหนึ่งในชุดหยุดชะงัก/ บำรุงรักษา เครื่องที่เหลือต้องสามารถรองรับการให้บริการได้อย่างต่อเนื่อง (เป็นโครงสร้างแบบ 2(n+1))

- มีการติดตั้งอุปกรณ์ UPS และ Generator เพื่อรองรับการทำงานของอุปกรณ์สำคัญในศูนย์ฯ แบบ 2 ชุด โดยแต่ละชุดมีเส้นทางการเดินกระแสไฟแยกจากกันและตั้งอยู่คนละห้อง(Compartmentalization) หากอุปกรณ์ UPS/Generator ชุดใดชุดหนึ่งหยุดชะงัก/ บำรุงรักษา อีกชุดต้องสามารถจ่ายไฟแทนได้อย่างต่อเนื่อง ทั้งนี้แต่ละชุดควรติดตั้งให้ครอบคลุมความเสี่ยงจากกรณีที่เครื่องใดเครื่องหนึ่งในชุดหยุดชะงัก/ บำรุงรักษา เครื่องที่เหลือต้องสามารถรองรับการให้บริการได้อย่างต่อเนื่อง ทั้งนี้ควรมีการจัดการค่า Utilization ที่เหมาะสมเพื่อให้ระบบทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ
- เมื่อเกิดเหตุการณ์ไฟฟ้าขัดข้อง UPS ควรรองรับการให้บริการอย่างน้อย 15 นาที[2] และเพียงพอที่จะรองรับการให้บริการระหว่างที่รอการทำงานของเครื่องปั่นไฟ (Generator) (โครงสร้าง UPS และ Generator เป็นแบบ 2(n+1))
- มีการสำรองน้ำมันไว้ในระดับที่เพียงพอให้อุปกรณ์ Generator สามารถจ่ายไฟให้ศูนย์ฯ ได้อย่างต่อเนื่องเป็นระยะเวลาอย่างน้อย 4 วัน[3] และมีมาตรการในการดำเนินการเพื่อขนส่งน้ำมันมายังศูนย์ฯ เพิ่มเติมเพื่อการให้บริการอย่างต่อเนื่อง
- อุปกรณ์ระบบไฟฟ้า เช่น High Voltage, Transformer, ATS, UPS และ Generator ติดตั้งในห้องที่แยกจากห้องจัดเก็บอุปกรณ์อื่น ๆ โดยมีการควบคุมอุณหภูมิ ความชื้น และมีการระบายอากาศที่เหมาะสม

- ระบบทำความเย็นและควบคุมความชื้น
  - มีการติดตั้งระบบทำความเย็นและควบคุมความชื้น (ระบบทำความเย็นฯ) เช่น Precision Air Conditioner, Computer Room Air Conditioner (CRAC) เพื่อรองรับพื้นที่สำคัญฯ โดยมีเครื่องสำรองเพื่อรองรับการทำงานในกรณีที่เครื่องหลักชำรุดหรือหยุดชะงักหรือบำรุงรักษาเครื่องที่เหลือต้องสามารถรองรับการให้บริการได้อย่างต่อเนื่อง
  - ระบบไฟฟ้าและระบบท่อน้ำเย็น (Chiller System) ที่รองรับระบบทำความเย็นฯ ควรมีระบบสำรอง สามารถรองรับการให้บริการได้อย่างต่อเนื่อง โดยระบบทำความเย็นฯ ควรควบคุมอุณหภูมิให้อยู่ในระหว่าง 20-25 Co และความชื้นที่ 40-55%[4] สำหรับห้องที่ต้องการควบคุมความเย็นและความชื้นให้เหมาะสม เช่น ห้องจัดเก็บเครื่องประมวลผล ห้องจัดเก็บอุปกรณ์เครือข่าย ห้องจัดเก็บสื่อบันทึกข้อมูล เป็นต้น
  - มีการติดตั้งระบบตรวจวัดอุณหภูมิและความชื้น โดยติดตั้งให้ครอบคลุมพื้นที่สำคัญฯ และมีการเฝ้าระวังรักษาระดับอุณหภูมิและความชื้นให้อยู่ในระดับที่เหมาะสม
- ระบบป้องกัน/ ระงับอัคคีภัย และระบบตรวจจับน้ำรั่วซึม
  - มีการติดตั้งระบบป้องกัน/ ระงับอัคคีภัย (Fire Protection and Suppression System) ได้แก่ อุปกรณ์ตรวจจับควันและความร้อน (Smoke & Heat Detector) และระบบระงับอัคคีภัย โดยติดตั้งให้ครอบคลุมทุกพื้นที่
  - ถังดับเพลิงแบบมือถือ (Hand-held Fire Extinguisher) จะต้องติดตั้งให้ครอบคลุมพื้นที่ภายในศูนย์ฯ ในตำแหน่งที่เหมาะสม มองเห็นง่าย สะดวกในการใช้งาน และมีคำแนะนำวิธีการใช้งานอย่างชัดเจน
  - มีการติดตั้งระบบตรวจจับน้ำรั่วซึม (Water Leak Detection System) โดยติดตั้งให้

ครอบคลุมพื้นที่สำคัญฯ

- การบำรุงรักษา
  - มีกระบวนการ และเจ้าหน้าที่รับผิดชอบในการตรวจเช็คประจำวัน (Daily Checklist) ของระบบสาธารณูปโภคที่สำคัญในศูนย์ฯ ได้แก่ สภาพแวดล้อมของสถานที่จัดเก็บอุปกรณ์ และการทำงานของอุปกรณ์ต่าง ๆ ได้แก่ High Voltage, Transformer, UPS, Generator, ATS, Precision Air Conditioner, Chiller และอุปกรณ์สำคัญอื่นๆ
  - มีการจัดให้ผู้ผลิตหรือผู้เชี่ยวชาญมาทำการตรวจเช็ค บำรุงรักษา (Preventive Maintenance) และแก้ไขเมื่อเกิดปัญหา (Corrective Maintenance) ระบบสาธารณูปโภคที่สำคัญ เช่น อุปกรณ์ UPS แบตเตอรี่ของอุปกรณ์ UPS, อุปกรณ์ Generator, Chiller System, ระบบป้องกัน/ ระงับอัคคีภัย และระบบตรวจจับน้ำรั่วซึม ตามรอบระยะเวลาที่ผู้ผลิตแนะนำ
  - มีการทดสอบการใช้งานระบบสาธารณูปโภคอย่างสม่ำเสมอ โดยในการทดสอบควรพึงระวังไม่ให้การทดสอบนั้นกระทบต่อการดำเนินงานปกติของธนาคาร
  - มีระบบศูนย์กลางในการติดตามสถานะของระบบสาธารณูปโภคที่สำคัญภายในศูนย์ฯ เช่น อุปกรณ์ UPS, แบตเตอรี่ของอุปกรณ์ UPS, อุปกรณ์ Generator, Chiller System, ระบบป้องกัน/ ระงับอัคคีภัย และระบบตรวจจับน้ำรั่วซึม โดยมีเจ้าหน้าที่เฝ้าระวังระบบตลอด 24 ชม. และมีระบบแจ้งเตือนอัตโนมัติให้ผู้เกี่ยวข้องทราบทันทีเมื่อมีเหตุผิดปกติ

[1] *Static Transfer Switch คือ อุปกรณ์ที่ทำหน้าที่ให้อุปกรณ์อื่น ๆ ที่รับกระแสไฟฟ้าได้เพียงทางเดียว (Single Source) สามารถสลับไปรับไฟจากอีกทางได้ คล้ายอุปกรณ์ที่รับไฟได้แบบสองเส้นทาง (Dual Source)*

[2] *มาตรฐาน TIA-942 ในเรื่องการระยะเวลาการสำรองไฟฟ้าของแบตเตอรี่ใน UPS (Tier 4)*

[3] *มาตรฐาน TIA-942 ในเรื่องการสำรองน้ำมันของอุปกรณ์ generator สำหรับจ่ายไฟที่ full load*

[4] *มาตรฐาน TIA-942 ในเรื่องการควบคุมอุณหภูมิและความชื้น*

***ข้อสังเกต**: แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน ซึ่งต้องพิจารณาความเหมาะสมของแต่ละแห่ง*

2 ระบบเครือข่ายสื่อสาร

2.1 Network Access Control

วัตถุประสงค์เพื่อให้โครงสร้างของระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย โดยมีการออกแบบระบบเครือข่าย ที่เหมาะสมตามมาตรฐานสากล และมีการป้องกัน/เฝ้าระวังภัยบุกรุกหรือภัยคุกคามรูปแบบต่าง ๆ

<u>แนวปฏิบัติที่ดี</u>

- มีการแบ่งแยกเครือข่ายส่วนที่เป็น Private Network และ Public Network ออกจากกัน
- มีการจัดตั้งโซนเครือข่าย Demilitarized Zone (DMZ)[5] เพื่อรองรับระบบงานที่ต้องมีการให้บริการ ติดต่อสื่อสารหรือแลกเปลี่ยนข้อมูลกับภายนอก เช่น ระบบงาน Internet Banking ระบบงาน E-mail เป็นต้น โดยไม่จัดวาง Server ที่เป็นระบบฐานข้อมูลสำคัญไว้ในโซนดังกล่าว
- มีการจัดแบ่งเครือข่ายอย่างเหมาะสม โดยคำนึงถึงระดับความสำคัญของระบบงาน ระดับความสำคัญของข้อมูลที่ถูกประมวลผล รวมถึงความจำเป็นในการเชื่อมต่อจากระบบงานอื่น ๆ หรือจากภายนอกองค์กร และจัดให้มีการควบคุมการเชื่อมต่อจากระบบงานต่าง ๆ มายังระบบงานที่มีความสำคัญอย่างเข้มงวด
- ในจุดที่มีการแบ่งแยกเครือข่ายที่พิจารณาว่ามีความสำคัญและมีความเสี่ยง ควรติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่ายที่มีความสามารถในการควบคุมและคัดกรอง Traffic ที่ส่งผ่านระบบ

เครือข่าย การเฝ้าระวังการบุกรุก การป้องกันการบุกรุก และการตรวจจับไวรัส หรือมัลแวร์ต่าง ๆ ที่อาจบุกรุกเข้าสู่เครือข่าย

- มีการใช้อุปกรณ์รักษาความปลอดภัยเครือข่ายเพื่อคัดกรอง Traffic ในระดับ Application ในจุดที่มีการเชื่อมต่อกับ Internet เช่น การใช้ Web Application Firewall เป็นต้น
- กรณีมีการแบ่งแยกเครือข่ายเป็นหลายชั้น ควรใช้อุปกรณ์รักษาความปลอดภัยเครือข่ายที่ต่างยี่ห้อกันในแต่ละจุดเพื่อเพิ่มประสิทธิภาพในการคัดกรอง Traffic ที่ส่งผ่านระบบเครือข่าย
- มีการควบคุม และจำกัดให้เฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงระบบเครือข่ายได้ รวมถึงมีการระบุตัวตนของอุปกรณ์ที่มาเชื่อมต่อกับระบบเครือข่ายอย่างเหมาะสม
- มีการจำกัดให้เฉพาะบุคคลที่ได้รับมอบอำนาจเท่านั้นที่สามารถเข้าถึงระบบเครือข่าย โดยจำกัดสิทธิ์ในการเข้าถึงระบบเครือข่ายให้อยู่ในส่วนที่มีความจำเป็น และเหมาะสมตามหน้าที่การทำงานเท่านั้น
- การเข้าถึงอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเพื่อบริหารจัดการค่าต่าง ๆ ควรทำผ่านเครือข่ายเฉพาะที่แยกออกจากเครือข่ายปกติ เพื่อลดความเสี่ยงในการเปลี่ยนแปลงอุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่ายโดยบุคคลที่ไม่ได้รับอนุญาต
- กรณีที่ต้องมีการเชื่อมต่อมาจากเครือข่ายจากระยะไกล (Remote Access) เพื่อทำการแก้ไขและ/หรือตั้งค่าพารามิเตอร์ของเครื่องแม่ข่าย อุปกรณ์เครือข่าย หรือโปรแกรมระบบงาน ควรมีการระบุตัวตนและพิสูจน์ตัวตนของบุคคลในลักษณะ Two-Factors Authentication และกระทำผ่านช่องทางที่มีความปลอดภัย เช่น SSH, VPN หรือ SSL/TLS เป็นต้น
- มีการเปลี่ยน Default Password ของอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย ให้เป็นไปตามนโยบายรหัสผ่าน

[5] Demilitarized Zone (DMZ) คือ ระบบเครือข่ายสื่อสารที่เป็นส่วนที่เชื่อมต่อกับเครือข่ายสาธารณะภายนอก เช่น อินเทอร์เน็ต โดยจะมีการติดตั้งระบบรักษาความปลอดภัยเอาไว้เพื่อป้องกันการบุกรุกจากภายนอกเข้ามาสู่ระบบเครือข่ายภายใน

2.2 Network Security Management

วัตถุประสงค์ เพื่อให้อุปกรณ์ระบบเครือข่ายมีการรักษาความปลอดภัยและมีความถูกต้องเชื่อถือได้

<u>แนวปฏิบัติที่ดี</u>

- มีการตั้งค่าอุปกรณ์รักษาความปลอดภัยเครือข่ายเพื่อควบคุมให้ระบบงานติดต่อสื่อสารกันได้ตามความจำเป็น รวมถึงมีการปรับแต่งค่า (Tuning) เพื่อเพิ่มประสิทธิภาพในการดักจับภัยบุกรุกและมีการทบทวนการตั้งค่าอย่างสม่ำเสมอหรืออย่างน้อยปีละ 2 ครั้ง หรือเมื่อมีการบุกรุกรูปแบบใหม่ ๆ
- มีการใช้ระบบในการควบคุมค่าเวลาของเครื่องประมวลผล ให้ตรงกับเครื่องเซิร์ฟเวอร์ NTP (Clock Synchronization) เพื่อให้ค่าเวลาในการบันทึกเหตุการณ์ (Log) มีความถูกต้องในลักษณะ Real-Time ซึ่งเซิร์ฟเวอร์ NTP ต้องรับสัญญาณนาฬิกาจากสถาบันที่มีความน่าเชื่อถือ เช่น กรมอุทกศาสตร์ (กองทัพเรือ) หรือ สถาบันมาตรวิทยา (กระทรวงวิทยาศาสตร์และเทคโนโลยี)
- มีกระบวนการหรือเครื่องมือในการตรวจสอบการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นกับอุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่ายที่พิจารณาว่ามีความสำคัญหรือมีความเสี่ยง เช่น การเปลี่ยนแปลง Service การเปลี่ยนแปลง Port และมีการแจ้งเตือนไปยังผู้ที่ได้รับมอบอำนาจ
- มีกระบวนการบริหารจัดการการเปลี่ยนแปลงการตั้งค่าอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายอย่างเป็นขั้นตอน ซึ่งครอบคลุม
    - การประเมินผลกระทบที่เกี่ยวข้อง

- การทดสอบ
- แผนย้อนกลับ
- การอนุมัติโดยผู้ที่มีอำนาจอนุมัติ
- การติดตามผลหลังการติดตั้ง (Post Implementation Review)

- มีการจำกัดสิทธิ์ในการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย และการเข้าถึงหน้าจอการบริหารจัดการระบบเครือข่าย (Configuration Page) เฉพาะผู้ที่รับมอบอำนาจเท่านั้น
- มีกระบวนการประเมินช่องโหว่ (Vulnerability Assessment) ของอุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่ายที่พิจารณาว่ามีความสำคัญหรือมีความเสี่ยงอย่างน้อยทุก 6 เดือน และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญโดยผู้เชี่ยวชาญ และมีการรายงานไปยังผู้ที่รับมอบอำนาจเพื่อดำเนินการแก้ไข หรือปิดช่องโหว่
- สำหรับระบบงานที่ต้องมีการติดต่อสื่อสาร หรือแลกเปลี่ยนข้อมูลผ่านระบบ Internet ควรทดสอบเจาะระบบเครือข่าย (Network Penetration Test) โดยผู้เชี่ยวชาญ อย่างน้อยปีละครั้ง และ/หรือทุกครั้งที่มีการเปลี่ยนแปลงค่าความปลอดภัย หรือมีการเปลี่ยนแปลงความเสี่ยงทางเทคโนโลยีที่มีนัยสำคัญ รวมทั้งควรจะมีการพิจารณาความเหมาะสมของการเปลี่ยนผู้เชี่ยวชาญที่ทำการทดสอบด้วย เพื่อให้มีมุมมองที่แตกต่างในการบริหารจัดการความเสี่ยง
- มีการติดตั้ง Software Updates/ Patch ที่จำเป็นแก่ อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย ตามคำแนะนำของผู้ผลิต โดยการติดตั้งต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management) อย่างเป็นขั้นตอน

2.3 Network Availability Management

วัตถุประสงค์ เพื่อให้ระบบเครือข่ายมีความพร้อมใช้งานทั้งด้านประสิทธิภาพในการรองรับปริมาณ Traffic ของธนาคาร ทั้งในภาวะปกติและภาวะฉุกเฉิน

<u>แนวปฏิบัติที่ดี</u>

- มีการติดตามสถานะความพร้อมใช้งานของระบบเครือข่ายว่ายังอยู่ในระดับ Service Level Agreement (SLA) ที่กำหนด และจัดให้มีกระบวนการจัดการปัญหา และวิธีแก้ปัญหาเมื่อระบบเครือข่ายขัดข้อง
- มีการจัดเตรียมระบบเครือข่ายสื่อสาร และอุปกรณ์เครือข่ายชุดสำรองเอาไว้ทั้งที่ศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และศูนย์เครือข่ายภูมิภาคในลักษณะ High Availability หรือ Load Balancing เพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง
- ผู้ให้บริการระบบเครือข่ายสำรองควรเป็นคนละรายกับผู้ให้บริการระบบหลัก
- มีกระบวนการทดสอบอย่างสม่ำเสมอเพื่อให้แน่ใจว่าระบบเครือข่ายสื่อสาร และอุปกรณ์เครือข่ายชุดสำรองมีความพร้อมในการใช้งาน

***ข้อสังเกต**: แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน ซึ่งต้องพิจารณาความเหมาะสมของแต่ละแห่ง*

3 ระบบ Core Banking

3.1 Logical Access Control

วัตถุประสงค์ เพื่อให้การบริหารจัดการบัญชีและสิทธิ์ของผู้ใช้งานมีประสิทธิภาพเป็นไปตามหลักความจำเป็นของการใช้งานและสอดคล้องกับหลักการแบ่งแยกงาน IT ที่ดี โดยสามารถป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

<u>แนวปฏิบัติที่ดี</u>

- มีหน่วยงานและกระบวนการมาตรฐานในการเพิ่ม เปลี่ยนแปลง และลบบัญชีผู้ใช้ รวมถึงสิทธิ์ของผู้ใช้ และมีการใช้ระบบเพื่อสนับสนุนการจัดการสิทธิ์ให้มีประสิทธิภาพมากยิ่งขึ้น โดยกระบวนการจัดการสิทธิ์ต้องครอบคลุมอย่างน้อย
    - มีการจัดทำตารางควบคุมการให้สิทธิ์ (Authorization Matrix) ของบัญชีผู้ใช้ที่สอดคล้องกับตำแหน่งหน้าที่งานตามหลักการตามความจำเป็นของหน้าที่รับผิดชอบ เพื่อใช้เป็นแนวทางการกำหนดสิทธิ์อย่างเป็นระบบและเป็นปัจจุบัน และมีการทบทวนตารางควบคุมการให้สิทธิ์ (Authorization Matrix) ของบัญชีผู้ใช้ทุกครั้งที่มีการเปลี่ยนแปลงหรือเป็นประจำอย่างน้อยทุก 6 เดือน
    - มีการอนุมัติโดยผู้ที่มีอำนาจอนุมัติทุกครั้งที่มีการเพิ่ม ยกเลิก และ/หรือ เปลี่ยนแปลง
        - บัญชีผู้ใช้
        - สิทธิ์ของผู้ใช้
    - มีการปรับปรุง/ยกเลิกบัญชีผู้ใช้ทันทีที่ลาออกจากงานหรือเปลี่ยนหน้าที่ความรับผิดชอบ ทั้งนี้รวมถึงการยกเลิกหรือระงับบัญชีผู้ใช้ชั่วคราวและบัญชีผู้ใช้ฉุกเฉินทันทีหลังจากใช้งานเสร็จ
    - มีการสอบทานสิทธิ์โดยผู้มีอำนาจอนุมัติอย่างน้อยทุก 6 เดือนสำหรับบัญชีผู้ใช้งาน และทุก 3 เดือน สำหรับบัญชีผู้ใช้ดูแลระบบและบัญชีผู้ใช้ที่มีสิทธิ์เทียบเท่าสิทธิ์สูง
    - มีการสอบทานบัญชีผู้ใช้ที่ไม่ได้เข้าใช้ระบบมาเป็นระยะเวลาหนึ่งอย่างน้อยทุก 3 เดือน
- มีการแบ่งแยกหน้าที่ในการทำงานของผู้มีหน้าที่ดูแลระบบงานประมวลผลหลักตามความเหมาะสม เพื่อไม่ให้บุคคลใดบุคคลหนึ่งปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ โดยอย่างน้อยต้องครอบคลุมการ
    - แบ่งแยกบุคคลากรที่มีหน้าที่พัฒนาระบบงาน (Developer) ออกจากผู้ดูแลระบบ (System Administrator) และผู้ดูแลระบบฐานข้อมูล (Database Administrator)
    - แบ่งแยก System Administrator ออกจากผู้ดูแลด้านความปลอดภัย (Security Administrator)
    - แบ่งแยก System Administrator ออกจาก Computer Operator
    - แบ่งแยก Database Administrator (DBA) ออกจากหน้าที่การทำงานอื่น ๆ
    - แบ่งแยกบุคคลากรที่มีหน้าที่พัฒนาระบบงาน (Developer) ออกจาก คนที่ได้สิทธิ์ในการโอนย้ายระบบขึ้นสู่ Production (Migration)
- มีกระบวนการควบคุมดูแลการเบิกใช้บัญชีผู้ใช้งานที่มีสิทธิ์สูงสุด (Highest Privilege User) อย่างเหมาะสม โดยครอบคลุม
    - มีการจัดเก็บรหัสผ่านของบัญชีผู้ใช้ที่มีสิทธิ์สูงสุดโดยหน่วยงานที่มีความเป็นอิสระจากหน่วยงานของผู้ขอเบิกใช้
    - มีการจำกัดผู้ใช้งานที่มีสิทธิ์ในการเบิกใช้และช่วงเวลาในการเบิกใช้บัญชีผู้ใช้ที่มีสิทธิ์สูงสุด

ไว้สำหรับกรณีที่มีความจำเป็นเท่านั้น
    - มีขั้นตอนในการอนุมัติการเบิกใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูงสุดโดยหัวหน้างานของผู้ขอเบิกใช้และหัวหน้างานหน่วยงานผู้จัดเก็บบัญชีผู้ใช้ที่มีสิทธิ์สูงสุด
    - มีระบบหรือกระบวนการเฝ้าดู (Oversee) ระหว่างการใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูงสุด
    - มีการควบคุมไม่ให้มีการเบิกใช้งานบัญชีผู้ใช้ที่มีสิทธิ์สูงสุดในเวลาเดียวกัน หรือ อย่างน้อยระบบต้องสามารถ ระบุตัวตนของผู้เข้าใช้งานและบันทึกไว้เพื่อการตรวจสอบย้อนหลังได้
- มีการจำกัดสิทธิ์ในการเข้าถึงและการใช้งานโปรแกรมอรรถประโยชน์ (System Utility), Command Line และชุดคำสั่งที่สำคัญ (Command) ที่สำคัญของระบบปฏิบัติการไว้เฉพาะบุคคลที่มีอำนาจหน้าที่เหมาะสมเท่านั้น
- มีการจำกัด Command ที่สำคัญของระบบปฏิบัติการที่เกี่ยวข้องไว้เฉพาะกลุ่มบุคคลที่มีหน้าที่เหมาะสมเท่านั้น
- มีการกำหนดสิทธิ์ในการเข้าใช้ทรัพยากรสำคัญของระบบงานตามอำนาจหน้าที่อย่างเหมาะสม เช่น การเข้าถึง File, Folder, Library ที่สำคัญ โดยคำนึงถึงสิทธิ์ในการ Read, Write, Execute, Append และ Delete เป็นต้น
- มีการควบคุมให้ Application ทำงานด้วยสิทธิ์ที่เหมาะสม
- มีการควบคุมไม่ให้ Application สามารถ Save หรือ อ่าน File ที่อยู่นอกเหนือโครงสร้าง File หรือ Directory ที่ถูกกำหนดไว้ให้สามารถเข้าถึงได้ แม้ว่าผู้เข้าใช้จะเข้าผ่าน URL ของไฟล์เหล่านั้นโดยตรง หรือปรับเปลี่ยน URL ดังกล่าวเพื่อทำการเข้าถึง File หรือ Directory อื่น ๆ (การทำ Path Traversal)
- ในการเข้าใช้ระบบงานทุกครั้ง จะต้องมีการระบุตัวตนและพิสูจน์ตัวตนด้วยวิธีการที่เหมาะสม เช่น การใช้ User ID และ Password โดยจำกัดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงได้ ในกรณีที่เป็นการเข้าใช้ระบบงานด้วยบัญชีผู้ใช้ที่มีสิทธิ์เทียบเท่าสิทธิ์สูง ควรมีการพิสูจน์ตัวตนในลักษณะ Two-Factor Authentication
- User ID ต้องสามารถระบุตัวตนของผู้ใช้งานได้อย่างถูกต้อง โดยต้องมีกระบวนการหรือระบบที่สามารถควบคุมไม่ให้มีการใช้ User ID ร่วมกัน
- มีการระงับหรือยกเลิก Default Account ที่ไม่มีความจำเป็นในการใช้งานหรือไม่มีความจำเป็นต่อการทำงานของระบบ เช่น Guest Accounts เป็นต้น
- มีการกำหนดค่ารหัสผ่านบนระบบให้เป็นไปตามมาตรฐานหรือนโยบายรหัสผ่าน โดยอย่างน้อยต้องครอบคลุม
    - รหัสผ่านควรบังคับเปลี่ยนสำหรับการเข้าใช้งานครั้งแรกและควรเปลี่ยนเป็นประจำดังนี้
        - รหัสผ่านสำหรับบัญชีผู้ใช้งาน (End User) และ บัญชีผู้ใช้ดูแลระบบ (IT User) ควรถูกเปลี่ยนทุก 60 วัน
        - รหัสผ่านสำหรับบัญชีผู้ใช้ที่มีสิทธิ์เทียบเท่าสิทธิ์สูง (Equivalent Privilege User) ควรถูกเปลี่ยนทุก 30 วัน
        - บัญชีผู้ใช้งานที่มีสิทธิ์สูงสุด (Highest Privilege User) ควรถูกเปลี่ยนทุก 30 วัน และทุกครั้งหลังใช้งาน
    - รหัสผ่านควรมีความยาวไม่น้อยกว่า 8 ตัวอักษร
    - รหัสผ่านควรประกอบไปด้วยตัวเลข ตัวอักษร และตัวอักขระพิเศษ
    - รหัสผ่านถูกล๊อกเมื่อมีการใส่ผิด 3 ครั้งติดกัน

- รหัสผ่านไม่ควรซ้ำกับรหัสผ่านเดิมที่ใช้ 12 ครั้งที่ผ่านมา
- มีการอำพรางรหัสผ่านด้วยการใช้สัญลักษณ์ เช่น สัญลักษณ์ดอกจัน เป็นต้น

- มีการเปลี่ยน Default Password ของบัญชีผู้ใช้ที่มากับระบบงานให้เป็นไปตามมาตรฐานหรือนโยบายรหัสผ่าน หากกรณีจำเป็นต้องใช้จะต้องกำหนดให้มีการทบทวน Log การเข้าถึงและการเข้าใช้งานของบัญชีผู้ใช้ที่มากับระบบงานด้วย
- มีการใช้ระบบเพื่อช่วยสนับสนุนการบริหารจัดการรหัสผ่านของบัญชีผู้ใช้งานที่มีสิทธิ์สูงสุด โดยครอบคลุม
  - การจัดเก็บรหัสผ่าน
  - การเบิกใช้รหัสผ่าน
  - การเปลี่ยนรหัสผ่านโดยอัตโนมัติ

3.2 System Security Management
วัตถุประสงค์ เพื่อให้การประมวลผลข้อมูลเป็นไปอย่างถูกต้องครบถ้วนและไม่กระทบกับการให้บริการทางธุรกิจ

<u>แนวปฏิบัติที่ดี</u>
- มีกระบวนการตรวจสอบความถูกต้องและครบถ้วนของการประมวลผลข้อมูลโดยอย่างน้อยต้องครอบคลุมถึง
  - จัดให้มีการตรวจสอบความถูกต้องและครบถ้วนโดยผู้รับมอบอำนาจทันทีภายหลังขั้นตอนที่มีจุด Check Point ตามที่ธนาคารกำหนดเสร็จสิ้น
  - มีการสอบทานรายงานการปฏิบัติงานการประมวลผลสิ้นวันโดยหัวหน้างานในวันทำการถัดไป
  - มีกระบวนการแก้ไขปัญหาที่ชัดเจนในกรณีที่การประมวลผลข้อมูลไม่สำเร็จ และมีแนวทางในการรายงานให้ผู้บังคับบัญชาทราบตามลำดับชั้น ตั้งแต่เกิดปัญหาจนกระทั่งแก้ไขปัญหาแล้วเสร็จ

วัตถุประสงค์ เพื่อให้ระบบมีการควบคุมสภาพแวดล้อมที่มั่นคงปลอดภัย โดยสามารถป้องกันการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาตและกระทบกับความถูกต้องเชื่อถือได้

<u>แนวปฏิบัติที่ดี</u>
- มีการแบ่งแยก Environment ของระบบงานที่ใช้สำหรับการพัฒนา (Development) การทดสอบ (Testing) และระบบที่ให้บริการจริง (Production) ออกจากกันในเชิง Physical หรือ Logical
- มีการรักษาความถูกต้องของโปรแกรมระบบงาน โดยมีการ
  - ควบคุมการเข้าถึง Source Code โดยจำกัดสิทธิ์การเข้าถึงเฉพาะบุคคลที่เหมาะสมเท่านั้นซึ่งต้องไม่ขัดหลักการแบ่งแยกหน้าที่
  - ควบคุมไม่ให้มีการลง Development Tools[6] และ Compilers[7] ไว้บน Production Environment
  - ควบคุมไม่ให้ Developer ได้รับสิทธิ์ในการเข้าถึง Production Environment

วัตถุประสงค์ เพื่อให้การเปลี่ยนแปลงระบบ ตั้งแต่การตั้งค่าของระบบงาน การปรับปรุงแก้ไขระบบ ไปจนถึงการพัฒนาระบบ มีความถูกต้องเหมาะสม

<u>แนวปฏิบัติที่ดี</u>

- มีกระบวนการและเครื่องมือการบริหารจัดการการเปลี่ยนแปลงที่เกี่ยวข้องกับระบบอย่างเป็นขั้นตอนดังนี้
    - การประเมินผลกระทบที่เกี่ยวข้อง
    - การทดสอบ
    - การจัดเตรียมแผนย้อนกลับ (Roll Back Plan) หรือแผนสำรองฉุกเฉินกรณีที่ทำการเปลี่ยนแปลงไม่สำเร็จ (Fall Back Plan)
    - การอนุมัติโดยผู้ที่มีอำนาจอนุมัติ
    - การติดตามผลหลังจากติดตั้ง (Post Implementation Review)
- มีการจำกัดสิทธิ์ในการเปลี่ยนแปลงการตั้งค่าและการเข้าถึงหน้าการบริหารจัดการเครื่องแม่ข่ายไว้เฉพาะผู้ที่รับมอบอำนาจเท่านั้น
- มีการตั้งค่าความปลอดภัยของเครื่องประมวลผลตามแนวปฏิบัติขั้นต่ำด้านการรักษาความปลอดภัย (Security Baseline) และมีการสอบทานการตั้งค่าดังกล่าวโดยผู้มีหน้าที่ควบคุมดูแลความปลอดภัย หรือความเสี่ยงด้านเทคโนโลยีอย่างสม่ำเสมอ
- มีกระบวนการประเมินช่องโหว่ (Vulnerability Assessment) ของระบบงานประมวลผลหลักอย่างสม่ำเสมอโดยผู้เชี่ยวชาญ และมีการรายงานไปยังผู้ที่รับผิดชอบเพื่อดำเนินการแก้ไขหรือปิดช่องโหว่อย่างเหมาะสม
- มีการลบ ระงับ หรือยกเลิก Services Application หรือ Network Protocol ที่ไม่มีความจำเป็นในการใช้งาน (Hardening)
- มีการใช้ระบบในการควบคุมค่าเวลาของเครื่องประมวลผล ให้ตรงกับเครื่องเซิร์ฟเวอร์ Network Time Protocol:NTP (Clock Synchronization) เพื่อให้ค่าเวลาในการบันทึกเหตุการณ์ (Log) มีความถูกต้องในลักษณะ Real-Time ซึ่งเซิร์ฟเวอร์ NTP ต้องรับสัญญาณนาฬิกาจากสถาบันที่มีความน่าเชื่อถือ เช่น กรมอุทกศาสตร์ (กองทัพเรือ) หรือ สถาบันมาตรวิทยา (กระทรวงวิทยาศาสตร์และเทคโนโลยี)
- มีการติดตั้งโปรแกรมป้องกันภัยจากมัลแวร์บนระบบงานประมวลผลหลัก โดยต้องเป็นโปรแกรมที่ได้รับอนุมัติเท่านั้น และควรมีการอัพเดทซิกเนเจอร์ของโปรแกรมป้องกันมัลแวร์ให้เป็นปัจจุบัน
- มีการติดตั้ง Software Updates/ Patch ที่จำเป็นสำหรับระบบงานประมวลผลหลัก ตามคำแนะนำของผู้ผลิต โดยการติดตั้งต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงอย่างเป็นขั้นตอน

วัตถุประสงค์ เพื่อให้การบันทึกเหตุการณ์สามารถใช้ติดตามตรวจสอบการเข้าใช้งานระบบของผู้ใช้งานและการทำธุรกรรมที่เหมาะสม

<u>แนวปฏิบัติที่ดี</u>

- จัดให้มีการจัดเก็บบันทึกเหตุการณ์ดังต่อไปนี้อย่างมั่นคงปลอดภัย
    - บันทึกร่องรอยกิจกรรมการทำธุรกรรม (Transaction Log)
    - บันทึกการเข้าถึงระบบงาน (Access Log) โดยบัญชีผู้ใช้ทุกประเภท
    - บันทึกการดำเนินงาน (Activity Log) ที่สำคัญ โดยอย่างน้อยต้องครอบคลุม
        - การเปลี่ยนแปลงแก้ไขโครงสร้างฐานข้อมูล และการเปลี่ยนแปลงแก้ไขข้อมูล (Update/ Insert/ Delete) ในตารางที่สำคัญ

- การเปลี่ยนแปลงการตั้งค่าความปลอดภัยของระบบ
- การเข้าถึง Object ที่สำคัญของระบบ
- การเปลี่ยนแปลงแก้ไขบัญชีและสิทธิ์ของผู้ใช้งาน

โดยบันทึกดังกล่าวต้องถูกจัดเก็บเป็นระยะเวลาอย่างน้อย 90 วัน

- มีการควบคุมการเข้าถึงข้อมูลการบันทึกเหตุการณ์ (Log) เพื่อป้องกันการเปลี่ยนแปลง แก้ไข หรือทำลาย โดยข้อมูลการบันทึกเหตุการณ์ควรถูกจัดเก็บไว้ที่เครื่องแม่ข่ายที่แยกเฉพาะ
- มีการใช้เครื่องมือในการตรวจจับเหตุการณ์ผิดปกติที่เกิดขึ้นกับระบบและแจ้งเตือนผู้ที่รับมอบอำนาจอัตโนมัติเพื่อดำเนินการแก้ไขอย่างทันท่วงที

วัตถุประสงค์ เพื่อป้องกันการรั่วไหลของข้อมูลและการเปลี่ยนแปลงแก้ไขข้อมูลในฐานข้อมูลโดยไม่ได้รับอนุญาต

<u>แนวปฏิบัติที่ดี</u>

- มีมาตรฐานในการจัดชั้นข้อมูล (Classification of Data) โดยข้อมูลที่มีความสำคัญสูงสุด ควรครอบคลุม รหัสผ่าน ข้อมูลส่วนบุคคลของลูกค้า รวมถึงข้อมูลบัญชีของลูกค้า
- มีการจัดเก็บรหัสผ่านของลูกค้าให้อยู่ในรูปแบบที่ไม่สามารถเรียกดูได้ในแบบที่ไม่มีการเข้ารหัสข้อมูลหรือสามารถถูกดักจับและอ่านข้อมูลนั้นได้ง่าย (Clear-Text)
- มีการเข้ารหัสลับข้อมูลที่มีการจัดลำดับชั้นสูงสุดโดยเลือกใช้อัลกอริทึมในการเข้ารหัสลับที่มีความมั่นคงปลอดภัย
- มีการบันทึกการเข้าถึงข้อมูลที่ถูกจัดชั้นที่มีความสำคัญสูงสุดให้สามารถตรวจสอบย้อนหลังได้ (Audit Trail)
- ในกรณีที่ต้องมีการนำข้อมูลจริงที่จัดอยู่ในระดับชั้นความสำคัญสูงสุดมาใช้เพื่อทำการทดสอบหรือแก้ไขปัญหาระบบงาน ต้องมีการควบคุมไม่ให้เปิดเผยข้อมูลที่แท้จริง (Data Masking)
- มีการควบคุมการเข้าถึง เรียกดู เปลี่ยนแปลงแก้ไข ลบข้อมูลในฐานข้อมูลลูกค้าให้ดำเนินการผ่านโปรแกรมระบบงานที่มีขั้นตอนการพิสูจน์ตัวตนของผู้ได้รับอนุญาตตามสิทธิ์ที่ได้รับมอบหมาย ก่อนเข้าถึงทุกครั้ง

2.3.3 System Availability Management

วัตถุประสงค์ เพื่อให้ระบบงานประมวลผลหลักมีความพร้อมใช้อยู่เสมอ ทั้งในภาวะปกติและภาวะฉุกเฉิน

<u>แนวปฏิบัติที่ดี</u>

- มีหน่วยงานและกระบวนการในการติดตาม Capacity ของเครื่องประมวลผล เพื่อให้ทรัพยากรของระบบ ได้แก่ CPU Utilization และ Disk Usage มีความเพียงพอรองรับปริมาณงานประมวลผลทั้งในช่วงปกติ และช่วง Peak
- มีการวางแผนที่ชัดเจนและเป็นลายลักษณ์อักษร ในการขยาย Resource ของเครื่อง เพื่อให้รองรับความต้องการในอนาคต โดยสอดคล้องกับการเติบโตของธุรกิจ (Resource Planning)
- นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรกำหนดให้ระบบ Core Banking อยู่ในกลุ่มระบบงานที่มีความสำคัญสูงสุด

- สำหรับระบบงานที่จัดอยู่ในกลุ่มระบบที่มีความสำคัญและสำคัญสูงสุด ควรมีการจัดเตรียมเครื่องอุปกรณ์ ระบบและข้อมูลสำรองพร้อมทำงานโดยอัตโนมัติเมื่อเกิดเหตุฉุกเฉินในลักษณะ High Availability
- มีการจัดเตรียมเครื่อง อุปกรณ์ ระบบ ข้อมูลสำรอง ไว้ที่ศูนย์ฯ สำรอง โดยมีกระบวนการที่ทำให้มั่นใจได้ว่าโปรแกรมระบบงาน รวมถึงการตั้งค่าและการปรับแต่งค่าบนระบบสำรองถูกต้องเป็นปัจจุบัน สำหรับพร้อมรองรับการทำธุรกรรม หากเกิดเหตุขัดข้องและระบบงานหลักไม่สามารถให้บริการได้ตามปกติ
- มีกระบวนการทดสอบเพื่อให้แน่ใจว่าระบบงานสำรองมีความพร้อมในการใช้งาน

หมายเหตุ: *ธพ. สามารถนำแนวปฏิบัติของระบบ Core Banking ไปประยุกต์ใช้ตามความเหมาะสมกับเครื่องประมวลผลอื่น เช่น เครื่องประมวลผลสาขา (Branch Server) เครื่องประมวลผล ATM เป็นต้น*

ข้อสังเกต: *แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน ซึ่งต้องพิจารณาความเหมาะสมของแต่ละแห่ง*

4 ระบบงานการให้บริการแก่ลูกค้า

4.1 เครื่องคอมพิวเตอร์ส่วนบุคคลที่สาขา

4.1.1 PC Security Control

วัตถุประสงค์ เพื่อให้เครื่องคอมพิวเตอร์ที่ใช้ในการปฏิบัติงาน/ทำธุรกรรม มีความมั่นคงปลอดภัย และไม่เป็นช่องทางที่ทำให้ข้อมูลสำคัญของลูกค้ารั่วไหลหรือมีการเข้าใช้งานโดยไม่ได้รับอนุญาต

<u>แนวปฏิบัติที่ดี</u>

- มีการระบุตัวตนและพิสูจน์ตัวตนของผู้เข้าใช้เครื่องคอมพิวเตอร์สาขาและระบบงานอย่างเหมาะสมและจำกัดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงได้
- มีการจำกัดการเข้าถึง Shared Drive/ Folder ตามความจำเป็นของหน้าที่การทำงานเท่านั้น
- มีการควบคุมการใช้ฟังก์ชัน Print Screen และ มีการกำหนดระยะเวลาที่เหมาะสมในการบังคับระบบให้มีการ Lock หน้าจอการทำงานเมื่อไม่มีการเคลื่อนไหว
- มีการควบคุมไม่ให้มีการจัดเก็บข้อมูลที่จัดชั้นเป็นระดับความสำคัญสูงสุดในเครื่องคอมพิวเตอร์ของผู้ใช้งาน หากมีความจำเป็นต้องจัดเก็บ ต้องมีการรักษาความปลอดภัยที่เหมาะสม เช่น การเข้ารหัส
- ควรมีกระบวนการบริหารจัดการหรือมาตราการป้องกันการรั่วไหลของข้อมูล (Data Leakage Prevention) ผ่านช่องทางต่าง ๆ เช่น Portable Thumb Drive, External Hard disk และ Internet เป็นต้น
- มีการลงโปรแกรมป้องกันภัยจากมัลแวร์ที่เครื่องคอมพิวเตอร์สาขา และควรมีการอัพเดทซิกเนเจอร์ของโปรแกรมป้องกันมัลแวร์ให้เป็นปัจจุบัน
- มีการควบคุมการการเข้าใช้บริการเครือข่าย Internet โดยคำนึงถึง
    - การจำกัด Website ที่เข้าถึงได้
    - การจำกัดการดาวน์โหลด/ อัพโหลดข้อมูลจากอินเตอร์เน็ต
- มีการกำหนดทะเบียนโปรแกรมที่ได้รับอนุญาตให้สามารถติดตั้งบนเครื่องคอมพิวเตอร์สาขาตามความจำเป็นในการใช้งาน โดยจัดให้มีกระบวนการในการขออนุญาตติดตั้งโปรแกรม และมีหน่วยงานควบคุมดูแลการติดตั้ง การใช้งานโปรแกรม รวมถึงการตั้งค่าต่าง ๆ ของคอมพิวเตอร์
- มีการตั้งค่าความปลอดภัยของเครื่องคอมพิวเตอร์อย่างเหมาะสมและมีการควบคุมไม่ให้ผู้ใช้งานได้รับสิทธิ์ในการติดตั้งโปรแกรมหรือเปลี่ยนแปลงแก้ไขค่าต่างๆ ที่เกี่ยวข้องกับการรักษาความ

ปลอดภัยของเครื่องคอมพิวเตอร์ด้วยตนเอง

***ข้อสังเกต**: แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน ซึ่งต้องพิจารณาความเหมาะสมของแต่ละแห่ง*

4.2 ATM Application Control

4.2.1 การควบคุมการบันทึกข้อมูลเข้าสู่ระบบ (Input Validation)

วัตถุประสงค์ เพื่อให้ข้อมูลเข้าสู่ระบบมีความครบถ้วนถูกต้อง

แนวปฏิบัติที่ดี

- มีการตรวจสอบข้อมูลที่เข้าสู่ระบบ (Input Validation) โดยอนุญาตเฉพาะข้อมูลที่อยู่ในรูปแบบที่กำหนดเท่านั้น เพื่อป้องกันข้อมูลผิดลักษณะ/รูปแบบ ไม่สมเหตุผล หรือผิด Logic เข้าสู่ระบบ
- มีการตรวจสอบความครบถ้วนของข้อมูล ก่อนที่จะทำการประมวลผลในขั้นตอนต่อไป เช่น จำนวนหลักของหมายเลข PIN หรือหมายเลขบัญชีเป็นต้น
- มีข้อความแจ้งเตือนผู้ใช้บริการ ในกรณีที่ผู้ใช้บริการกรอกข้อมูลไม่ถูกต้องครบถ้วน และไม่อนุญาตให้ผู้ใช้บริการข้ามขั้นตอนจนกว่าจะกรอกข้อมูลที่ถูกต้อง

4.2.2 การควบคุมข้อมูลขณะประมวลผล (Processing Control)

วัตถุประสงค์ เพื่อให้การประมวลผลข้อมูลมีความครบถ้วนถูกต้อง

แนวปฏิบัติที่ดี

- มีการตรวจสอบเงื่อนไขการทำธุรกรรม เช่น ยอดคงเหลือ Limit จำนวนเงินต่อครั้ง Limit จำนวนเงินต่อวัน ค่าธรรมเนียม เป็นต้น ก่อนที่จะดำเนินรายการตามขั้นตอนที่กำหนดไว้
- ระบบสามารถดึงข้อมูลบัญชีลูกค้ามาจากระบบฐานข้อมูลได้อย่างถูกต้องและครบถ้วนโดยมีกระบวนการที่ทำให้มั่นใจว่าข้อมูลในฐานข้อมูลของระบบงานเป็นปัจจุบัน
- ระบบมีการสรุปรายการเพื่อให้ลูกค้าทำการตรวจสอบความถูกต้องอีกครั้งก่อนยืนยันการทำรายการจริง เช่น การโอนเงิน การชำระค่าสินค้าและบริการ เป็นต้น
- หากเกิดความผิดพลาดระหว่างที่ระบบประมวลผลข้อมูล ระบบจะต้องมีการแจ้งลูกค้าและต้องสามารถตรวจสอบความถูกต้องของข้อมูล (Data Integrity) เพื่อกลับไปสู่สถานะก่อนการทำรายการอย่างถูกต้อง

4.2.3 การควบคุมการนำข้อมูลออกจากระบบ (Output Control)

วัตถุประสงค์ เพื่อให้ข้อมูลออกจากระบบมีความครบถ้วนถูกต้อง

แนวปฏิบัติที่ดี

- กรณีที่มีการแจ้งข้อมูลสำคัญของลูกค้า เช่น ชื่อบัญชี หมายเลขบัญชี เป็นต้น ควรทำการปิดบังบางส่วนของข้อมูล
- ระบบพิมพ์หลักฐานการทำรายการให้แก่ลูกค้าอย่างครบถ้วนและถูกต้องภายหลังจากการทำรายการเสร็จสิ้นสมบูรณ์ตามขั้นตอนที่กำหนดไว้ โดยต้องครอบคลุมรายละเอียดตามที่ สนส. 26/2551 เอกสารแนบ 4 กำหนด
- มีการควบคุมไม่ให้ข้อความแจ้งเตือน (Error Message) แสดงข้อมูลเกินความจำเป็น หรือแสดงข้อมูลที่เป็นการบ่งชี้อย่างเฉพาะเจาะจงว่าข้อมูลส่วนใดส่วนหนึ่งผิดพลาด เช่นการแจ้งเตือนว่ารหัสผ่านไม่ถูกต้อง เป็นต้น
- มีการควบคุมให้ข้อความแจ้งเตือน (Error Message) เป็นหน้ากลางที่มีรูปแบบเดียวกันทั้งหมด

โดยข้อความจะต้องสื่อสารให้ลูกค้าเกิดความเข้าใจที่ถูกต้อง และจะต้องไม่แสดงข้อมูลภายในของระบบ เช่น ยี่ห้อ และ version ของระบบงาน, Debug Message, Stack Trace, IP Address และ Path เป็นต้น และควรแสดงรหัสที่บอกถึงสาเหตุของการทำงานที่ผิดพลาด ที่สามารถเข้าใจได้เฉพาะบุคลากรที่รับมอบอำนาจเท่านั้น

***ข้อสังเกต**: แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน ซึ่งต้องพิจารณาความเหมาะสมของแต่ละแห่ง*

4.3 ตู้ Automatic Teller Machine (ATM)

4.3.1 ATM Security Control

วัตถุประสงค์ เพื่อให้ตู้ ATM ที่ใช้ในการทำธุรกรรม มีความมั่นคงปลอดภัย และไม่เป็นช่องทางการทำทุจริตหรือมีการทำธุรกรรมที่ไม่เหมาะสม

<u>แนวปฏิบัติที่ดี</u>

- มีการป้องกันการแอบลักลอบติดตั้งอุปกรณ์แปลกปลอมที่ตู้ ATM เพื่อให้สามารถป้องกันภัยคุกคามอย่างน้อยดังนี้
    - การทำให้บัตรหรือเงินสดค้างไว้ที่ช่องเสียบบัตรโดยตั้งใจ (Card /Cash Trapping)
    - การคัดลอกข้อมูลจากแถบแม่เหล็กของบัตร (Magnetic Stripe) หรือ Chip ของบัตร
    - การแอบดูและขโมย PIN ของลูกค้า
- มีการติดตั้งกล้องที่ตู้ ATM หรือในบริเวณที่จัดตั้งตู้ ATM โดยจับภาพ ผู้ที่มาทำรายการ และบริเวณช่องจ่ายเงิน โดยมีการจัดเก็บภาพจากกล้องวงจรปิดไว้เป็นหลักฐานเป็นระยะเวลาอย่างน้อย 90 วัน และมีการสอบทานคุณภาพของการบันทึกภาพจากกล้องวงจรปิดอย่างสม่ำเสมอโดยบุคคลที่รับมอบอำนาจ
- มีหน่วยงานกลางและเครื่องมือในการติดตามการทุจริตที่เกิดจากช่องทาง ATM (Fraud Monitoring System) โดยสามารถตรวจพบพฤติกรรมที่น่าสงสัย เพื่อเจ้าหน้าที่ตรวจสอบได้ในทันที และมีการตรวจสอบ การติดตั้งอุปกรณ์แปลกปลอมที่ตู้ ATM อย่างครอบคลุมและสม่ำเสมอ
- มีหน่วยงานกลางและเครื่องมือในการติดตามสถานะการทำงานของตู้ ATM (ATM Monitoring) แบบ Real-Time โดยอย่างน้อยครอบคลุมเหตุการณ์ ดังต่อไปนี้
    - สถานะการทำงานของตู้ ATM
    - ระบบเครือข่ายสื่อสารขัดข้อง
    - สถานะเงินสดในตู้ ATM
- ในการปฏิบัติงานที่ตู้ ATM ควรมีการควบคุมการปฏิบัติงานที่เกี่ยวข้องกับส่วนสำคัญต่าง ๆ ของตู้อย่างรัดกุมเพียงพอและเป็นไปตามหลัก Dual Control โดยจำกัดเฉพาะผู้ที่ได้รับอนุญาตเท่านั้นโดยครอบคลุม
    - การเข้าถึงและปฏิบัติงานผ่านหน้าจอ Console ของตู้ ATM
    - การเข้าถึงกล่องเงินสด กล่องรับบัตร Reject อุปกรณ์เครือข่ายสื่อสาร สายไฟ อุปกรณ์ UPS (ถ้ามี)
    - การบำรุงรักษาและซ่อมแซมตู้ทางกายภาพ
- มีการแบ่งแยกหน้าที่ต่างๆของบุคคลากรที่มีหน้าที่ในการดูแลรักษาระบบ โดยครอบคลุมหน้าที่ดังต่อไปนี้
    - การดำเนินงานทั่วไป ได้แก่ การเติมเงินหรือเอาเงินออกจากตู้ ,การเติมกระดาษ ,การเก็บ

บัตรคงค้างในตู้ ATM
    - การบำรุงรักษาและซ่อมแซมตู้ทางกายภาพ
    - การตั้งค่าต่างๆของโปรแกรม
    - การบริหารจัดการ key
    - การตรวจสอบการกระทบยอดเงินคงเหลือที่ตู้ ATM
- มีการควบคุมไม่ให้มีการเชื่อมต่ออุปกรณ์สื่อที่เคลื่อนย้ายได้ เช่น USB, CD/DVD และ External HDD เป็นต้น โดยไม่ได้รับอนุญาต
- มีการควบคุมให้หยุดให้บริการตู้ ATM ที่อยู่ระหว่างการบำรุงรักษาระบบ
- มีการจัดเก็บบันทึกเหตุการณ์ (Electronic Journal Log) ของตู้ ATM ดังต่อไปนี้อย่างมั่นคงปลอดภัย และสามารถนำมาวิเคราะห์ตรวจสอบได้ทันทีอย่างน้อย 90 วันย้อนหลัง
    - รายการการทำธุรกรรม (Transaction Log)
    - การบำรุงรักษา ซึ่งรวมถึงการซ่อมแซม ปรับปรุงแก้ไขต่าง ๆ ได้แก่
        - การเข้าถึงและการปฏิบัติงานผ่านหน้าจอหลักของตู้ ATM
        - การเข้าถึงและปฏิบัติงานกับตู้ทางกายภาพ เช่น การเปิด/ปิดตู้
        - การเปลี่ยนกล่องเงิน การเปลี่ยนกล่องรับบัตร Reject เป็นต้น

  โดยมีการ Upload Log ของตู้ ATM ไปเก็บยังระบบจัดเก็บ Log ส่วนกลางเป็นระยะเวลาอย่างน้อย 1 ปี ซึ่ง สง. สามารถกำหนดระยะเวลาในการ Upload Log ของตู้ ATM ตามความเหมาะสม
- มีการควบคุมไม่ให้มีการจัดเก็บข้อมูล PIN ในบันทึกเหตุการณ์ (Log) ของระบบงานของตู้ ATM แม้ว่าจะอยู่ในรูปแบบที่เข้ารหัสแล้วก็ตาม

ข้อสังเกต: *แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน ซึ่งต้องพิจารณาความเหมาะสมของแต่ละแห่ง*

4.4 อุปกรณ์ Hardware Security Machine (HSM)

4.4.1 HSM Security Control

วัตถุประสงค์ เพื่อให้การปฏิบัติงานกับเครื่อง HSM ซึ่งใช้เป็นส่วนสำคัญในการพิสูจน์ตัวตนของลูกค้ามีความรัดกุมปลอดภัยสูงสุด

<u>แนวปฏิบัติที่ดี</u>

- มีการระบุตัวตนและพิสูจน์ตัวตนของผู้เข้าใช้ระบบ HSM โดยอาศัยหลักการ Dual Control และ Split Knowledge โดยจำกัดให้เฉพาะบุคคลที่ได้รับมอบอำนาจเท่านั้นที่สามารถเข้าถึงได้โดยการพิสูจน์ตัวตน จะต้องทำหน้าที่ Console ของ HSM เท่านั้น
- มีการควบคุมและจำกัดให้เฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้นที่สามารถเชื่อมต่อ กับระบบ HSM ได้ โดยมีการระบุตัวตนของอุปกรณ์ที่มาเชื่อมต่ออย่างเหมาะสม
- มีกระบวนการควบคุมกุญแจหรือ Key Card ที่ใช้ในการเข้าถึงเครื่อง HSM ทางกายภาพ โดยครอบคลุม
    - การจัดเก็บกุญแจหรือ Key Card ให้มีความมั่นคงปลอดภัยโดยหน่วยงานที่เหมาะสม
    - การจำกัดผู้ใช้งานที่สามารถเบิกใช้กุญแจหรือ Key Card ได้
    - การอนุมัติการขอเบิกใช้กุญแจหรือ Key Card จากผู้ที่ได้รับมอบอำนาจเหมาะสม
    - การจัดทำทะเบียนคุมการเบิกใช้กุญแจและหรือ Key Card
    - การสอบทานการเบิกใช้กุญแจหรือ Key Card อย่างสม่ำเสมอ

- มีการตรวจสอบกระบวนการควบคุมการเข้าถึงเครื่อง HSM และการบริหารจัดการ Key โดยหน่วยงานที่เป็นอิสระอย่างสม่ำเสมอ
- มีการใช้ชนิดของอัลกอริทึมที่มีความแข็งแรงในการเข้ารหัส/ถอดรหัสข้อมูล PIN และมีการประเมินความแข็งแรงของอัลกอริทึ่มที่ใช้อย่างสม่ำเสมอ
- มีการรักษาความปลอดภัยของสื่อที่ใช้ในการจัดเก็บข้อมูล PIN หรือ Key ที่ใช้ในการเข้ารหัส/ถอดรหัสข้อมูลอย่างเหมาะสม เช่น กระดาษคาร์บอน ซอง PIN ที่ไม่ได้ใช้งาน และ Smart Card เป็นต้น
- มีการจัดวาง Printer ที่ใช้ในการพิมพ์ PIN หรือ Key ในที่ที่มีความมั่นคงปลอดภัยและมีการควบคุมการเข้าถึงอย่างเหมาะสม

ข้อสังเกต: *แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน ซึ่งต้องพิจารณาความเหมาะสมของแต่ละแห่ง*

4.5 Internet Banking Application Control

4.5.1 การควบคุมการบันทึกข้อมูลเข้าสู่ระบบ (Input Validation)

วัตถุประสงค์ เพื่อให้ข้อมูลเข้าสู่ระบบมีความครบถ้วนถูกต้อง

แนวปฏิบัติที่ดี

- อนุญาตเฉพาะข้อมูลที่อยู่ในรูปแบบที่กำหนดเท่านั้น เพื่อป้องกันข้อมูลที่ไม่ประสงค์ดี (เช่น ชุดคำสั่ง) ข้อมูลผิดลักษณะ/รูปแบบ ไม่สมเหตุผล หรือผิด Logic เข้าสู่ระบบ
- มีการตรวจสอบความครบถ้วนของข้อมูล ก่อนที่จะทำการประมวลผลในขั้นตอนต่อไป เช่น จำนวนหลักของหมายเลขบัญชี ความครบถ้วนของ Mandatory Fields เป็นต้น
- มีข้อความแจ้งเตือนผู้ใช้บริการ ในกรณีที่ผู้ใช้บริการกรอกข้อมูลไม่ถูกต้องครบถ้วน และไม่อนุญาตให้ผู้ใช้บริการข้ามขั้นตอนจนกว่าจะกรอกข้อมูลที่ถูกต้อง

4.5.2 การควบคุมข้อมูลขณะประมวลผล (Processing Control)

วัตถุประสงค์ เพื่อให้การประมวลผลข้อมูลมีความครบถ้วนถูกต้อง

แนวปฏิบัติที่ดี

- มีการตรวจสอบเงื่อนไขการทำธุรกรรม เช่น ยอดคงเหลือ, Limit จำนวนเงินต่อครั้ง, Limit จำนวนเงินต่อวัน และค่าธรรมเนียม เป็นต้น ก่อนที่จะดำเนินรายการตามขั้นตอนที่กำหนดไว้
- ระบบสามารถดึงข้อมูลบัญชีของลูกค้ามาจากระบบฐานข้อมูลได้อย่างถูกต้องและครบถ้วน โดยมีกระบวนการที่ทำให้มั่นใจว่าข้อมูลในฐานข้อมูลของระบบงานเป็นปัจจุบัน
- ระบบมีการสรุปรายการเพื่อให้ลูกค้าทำการตรวจสอบความถูกต้องอีกครั้งก่อนยืนยันการทำรายการจริง
- หากเกิดความผิดพลาดระหว่างที่ระบบประมวลผลข้อมูล ระบบจะต้องมีการแจ้งลูกค้าและต้องสามารถตรวจสอบความถูกต้องของข้อมูล (Data Integrity) เพื่อกลับไปสู่สถานะก่อนการทำรายการอย่างถูกต้อง

4.5.3 การควบคุมการนำข้อมูลออกจากระบบ (Output Control)

วัตถุประสงค์ เพื่อให้ข้อมูลออกจากระบบมีความครบถ้วนถูกต้อง

แนวปฏิบัติที่ดี

- กรณีที่มีการแจ้งข้อมูลสำคัญของลูกค้า เช่น ชื่อบัญชี และหมายเลขบัญชี เป็นต้น ควรทำการปิดบังบางส่วนของข้อมูล

- ระบบจัดทำใบบันทึกรายการให้แก่ลูกค้าอย่างครบถ้วนและถูกต้องภายหลังจากการทำรายการเสร็จสมบูรณ์ตามขั้นตอนที่กำหนดไว้ โดยต้องครอบคลุมรายละเอียดตามที่ สนส. 26/2551 เอกสารแนบ 4 กำหนด
- มีการควบคุมไม่ให้ข้อความแจ้งเตือน (Error Message) แสดงข้อมูลเกินความจำเป็น หรือแสดงข้อมูลที่เป็นการบ่งชี้อย่างเฉพาะเจาะจงว่าข้อมูลส่วนใดส่วนหนึ่งผิดพลาด เช่นการแจ้งเตือนว่ารหัสผ่านไม่ถูกต้อง เป็นต้น
- มีการควบคุมให้ข้อความแจ้งเตือน (Error Message) เป็นหน้ากลางที่มีรูปแบบเดียวกันทั้งหมด โดยข้อความจะต้องสื่อสารให้ลูกค้าเกิดความเข้าใจที่ถูกต้อง และจะต้องไม่แสดงข้อมูลภายในของระบบ เช่น ยี่ห้อ และ Version ของ Web Application, Debug Message, Stack Trace, IP Address, Path เป็นต้น และควรแสดงรหัสที่บอกถึงสาเหตุของการทำงานที่ผิดพลาด ที่สามารถเข้าใจได้เฉพาะบุคลากรที่รับมอบอำนาจเท่านั้น

ข้อสังเกต: *แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน ซึ่งต้องพิจารณาความเหมาะสมของแต่ละแห่ง*

4.6 Internet Banking Security

4.6.1 System Security

วัตถุประสงค์ เพื่อให้การทำธุรกรรมการเงินของลูกค้าผ่านช่องทาง Internet Banking มีความถูกต้องครบถ้วนและมั่นคงปลอดภัยจากการบุกรุกหรือภัยคุกคามรูปแบบต่าง ๆ

<u>แนวปฏิบัติที่ดี</u>

- มีการควบคุมให้ช่องทางในการทำธุรกรรมมีความปลอดภัยโดยการใช้ Protocol ที่เข้ารหัสลับในการรับส่งข้อมูลระหว่างผู้ใช้บริการ กับ Web Server เช่น HTTPs เป็นต้น โดยคำนึงถึงความปลอดภัยของช่องทางตั้งแต่จุดที่เริ่มป้อนข้อมูล ไปจนถึงเครื่องแม่ข่าย ในระบบเครือข่ายภายในที่ทำการประมวลผล (End-to-End Encryption)
- มีการทำ End-to-End Encryption ที่ระดับ Application Layer เพื่อรักษาความลับและความปลอดภัยข้อมูลผู้ใช้บริการ เช่น รหัสผ่านของผู้ใช้บริการ,ข้อมูลบัญชีของผู้ใช้บริการ เป็นต้น
- มีการรักษาความปลอดภัยของ Key ที่ใช้ในการเข้ารหัส/ถอดรหัส โดยการใช้ Hardware Security Module (HSM)
- การพิสูจน์ตัวตน ควรทำที่เครื่องแม่ข่ายสำหรับการพิสูจน์ตัวตนโดยเฉพาะซึ่งถูกแยกทางกายภาพ (Physical) กับ Database Server ที่ใช้ในการให้บริการ Internet Banking
- มีการเข้ารหัสข้อมูลรหัสผ่านของผู้ใช้บริการ ที่จัดเก็บในฐานข้อมูลที่ใช้ในการพิสูจน์ตัวตน (Authentication Database) ด้วยมาตรฐานการเข้ารหัสที่เป็นที่ยอมรับสากล โดยเลือกใช้อัลกอริทึมในการเข้ารหัสลับแบบย้อนกลับไม่ได้ (Irreversible Encryption หรือ Hashing) และมีความมั่นคงปลอดภัย ยกตัวอย่างเช่น SHA-256 แบบมี Salt เป็นอย่างน้อย
- ในขั้นตอนการออกแบบและพัฒนา Web Application ควรคำนึงถึงความปลอดภัยของระบบงานให้ครอบคลุมความเสี่ยงของ OWASP[8] TOP 10 ปีล่าสุด
- มีการทดสอบเจาะระบบงาน (Application Penetration Test) โดยผู้เชี่ยวชาญ อย่างน้อยปีละครั้ง และ/หรือทุกครั้งที่มีการเปลี่ยนแปลงค่าความปลอดภัย หรือมีการเปลี่ยนแปลงความเสี่ยงทางเทคโนโลยีที่มีนัยสำคัญ รวมทั้งควรจะมีการพิจารณาเปลี่ยนผู้เชี่ยวชาญที่ทำการทดสอบตามความเหมาะสม โดยการทดสอบต้องครอบคลุม
    - ฟังก์ชั่นการทำงานของโปรแกรมทั้งหมด (Business Logic)

- OWASP top 10 ของปีล่าสุด
- มีการทบทวนรหัสต้นฉบับเพื่อตรวจหาช่องโหว่ (Security Source Code Review) ทุกครั้งที่มีการเปลี่ยนแปลงระบบงานที่มีนัยสำคัญ เพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากการพัฒนาแอพพลิเคชั่นอย่างไม่ปลอดภัย
- มีการประเมินความเสี่ยงและช่องโหว่ ของ Internet Banking Application อย่างสม่ำเสมอ หรือเมื่อมีภัยใหม่ๆและมีการปรับปรุงแก้ไข Application หรือเพิ่มการควบคุมที่จำเป็นอย่างทันท่วงที
- มีการตั้งค่าความปลอดภัยของเครื่องคอมพิวเตอร์อย่างเหมาะสมและมีการควบคุมไม่ให้ผู้ใช้งานได้รับสิทธิ์ในการติดตั้งโปรแกรมหรือเปลี่ยนแปลงแก้ไขค่าต่าง ๆ ที่เกี่ยวข้องกับการรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ด้วยตนเอง

[8] *OWASP หรือ The Open Web Application Security Project เป็นองค์กรที่จัดตั้งโดยไม่แสวงหาผลกำไรเพื่อศึกษาและเก็บข้อมูลภัยคุกคามที่เกิดขึ้นทาง Internet รูปแบบใหม่ ๆ*

4.6.2 Access Control

วัตถุประสงค์ เพื่อให้มั่นใจว่าระบบงาน Internet Banking มีการป้องกันการเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต

<u>แนวปฏิบัติที่ดี</u>

- มีการระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้บริการ โดยการใช้ Two-Factor Authentication ในขั้นตอนการเข้าใช้ระบบงานและควบคุมไม่ให้ User ID เดียวกันเข้าใช้งานระบบพร้อมกัน (Concurrent Session)
- มีการควบคุมให้ระบบล็อกบัญชีผู้ใช้ของผู้ใช้บริการเมื่อมีการใส่ข้อมูลการพิสูจน์ตัวตน ผิดเกินจำนวน 3-5 ครั้ง โดยระบบต้องไม่เปิดเผยข้อความแจ้งเตือนที่เป็นการบ่งชี้ว่าข้อมูลพิสูจน์ตัวตนส่วนใดที่ไม่ถูกต้อง
- กำหนดให้ผู้ใช้บริการตั้งค่ารหัสผ่านให้มีความซับซ้อนและยากต่อการคาดเดา โดยรหัสผ่านต้องประกอบไปด้วย ตัวอักษร ตัวอักขระพิเศษและตัวเลข
- มีการบังคับให้ผู้ใช้บริการเปลี่ยนรหัสผ่านเมื่อเข้าใช้ระบบงานครั้งแรก หรือได้รับรหัสผ่านใหม่
- หากลูกค้าลืมรหัสผู้ใช้งาน หรือรหัสผ่านต้องมีการพิสูจน์ตัวตนของลูกค้าโดยวิธี Two-Factor Authentication ก่อนให้ลูกค้าทำการ Reset รหัสผ่าน

4.6.3 Application Security

วัตถุประสงค์ เพื่อให้ระบบงาน Internet Banking มีระบบการควบคุมและรักษาความปลอดภัยอย่างเหมาะสม

<u>แนวปฏิบัติที่ดี</u>

- มีการแสดงวันที่ และเวลาที่เข้าระบบครั้งล่าสุดเมื่อเข้าสู่ระบบ Internet Banking สำเร็จ เพื่อให้ลูกค้าได้ตรวจสอบความถูกต้องของเวลาที่มีกิจกรรมครั้งล่าสุด
- มีการควบคุมไม่ให้มีการจัดเก็บข้อมูลที่ใช้ในการระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้บริการ เช่น Session ID, User ID หรือ รหัสผ่าน ไว้ใน Cookie หรือ ใน Web Browser
- มีการตรวจสอบสิทธิ์ของผู้ใช้บริการใหม่เมื่อมีการเข้าใช้งานฟังก์ชันที่สำคัญของระบบงาน เพื่อป้องกันการยกระดับสิทธิ์โดยไม่ได้รับอนุญาต
- มีการบริหารจัดการ Session การใช้งานอย่างเหมาะสม โดยอย่างน้อยให้มีการควบคุมที่ลดความ

เสี่ยงจาก Man-in-the-Middle Attack และ Man-in-the-Browser Attack

- มีการควบคุมไม่ให้มีการเก็บข้อมูลที่สำคัญของลูกค้าไว้ใน Session และมีการสร้าง Session Key ใหม่เมื่อมีการเปลี่ยนหน้า/ขั้นตอนการทำรายการ
- มีการตรวจสอบลำดับของขั้นตอนการทำธุรกรรมอย่างเหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีสามารถข้ามขั้นตอนใดขั้นตอนหนึ่งได้ หากพบว่ามีการกระทาดังกล่าว จะต้องมีกระบวนการในการยับยั้งการทำธุรกรรม เช่น ทำให้ Session หมดอายุ หรือ Logout ผู้ใช้บริการออกจากระบบ
- มีการกำหนด Time-Out ของ Session ให้ไม่เกิน 10 นาที
- มีการพิสูจน์ตัวตนของผู้ใช้บริการอีกครั้งสำหรับการทำกิจกรรมและ/หรือการทำรายการธุรกรรมที่มีความเสี่ยงสูง โดยการใช้ Hardware Token ที่สามารถทำ Transaction Signing ได้ โดยอย่างน้อยต้องครอบคลุมกิจกรรมดังนี้
    - การเปลี่ยน Profile เช่น เปลี่ยนที่อยู่ เบอร์โทร E-mail เป็นต้น
    - การผูกบัญชีบุคคลที่สามสำหรับทำธุรกรรมโอนเงิน การโอนเงินไปยังบุคคลที่สาม
    - การเปลี่ยนแปลงวงเงินการทำธุรกรรมโอนเงิน
- ในกรณีที่มีการใช้ One-Time-Password (OTP)[9] เพื่อยืนยันตัวตนผู้ใช้บริการ ควรกำหนดอายุการใช้งาน OTP ให้มีระยะเวลาไม่เกิน 5 นาที ซึ่ง OTP ที่ถูกสร้างขึ้นมาต้องใช้สำหรับการทำธุรกรรมรายการใดรายการหนึ่งเท่านั้น โดยไม่สามารถใช้กับรายการธุรกรรมอื่น ๆ ได้ โดยในการสร้าง OTP ควรมีการใช้ข้อมูลเกี่ยวกับธุรกรรม เช่น หลายเลขบัญชี จำนวนเงินที่ทำธุรกรรม เป็นต้น มาเป็นส่วนประกอบหนึ่งของการสร้าง OTP ด้วย (Transaction Signing)
- หน้าเวปไซต์ (Browser) ควรออกแบบให้สามารถป้องกันการ Key เดาสุ่มข้อมูลสำคัญ เช่น User ID / Password การสืบค้นข้อมูลบัญชีของลูกค้า เป็นต้น
- มีการแจ้งเตือนไปยังผู้ใช้งานผ่านอุปกรณ์หรือช่องทางอื่นที่ไม่ได้ใช้ทำรายการ เช่น E-mail และ SMS เป็นต้น เมื่อผู้ใช้บริการดำเนินกิจกรรมและ/หรือธุรกรรมที่มีความเสี่ยงสูงแล้วเสร็จ เช่น การ Login เข้าสู่ระบบ การเปลี่ยนแปลง Profile การเปลี่ยน Password การผูกบัญชี การโอนเงินไปยังบุคคลที่สาม เป็นต้น

ข้อสังเกต: *แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน ซึ่งต้องพิจารณาความเหมาะสมของแต่ละแห่ง*

ภาคผนวก ข การควบคุมที่สำคัญของบริการ Payment Gateway/Switching/ Clearing

(ที่มา : แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices) Phase 2 : ธุรกรรม E-Banking และ E-Payment)

5. การรับชำระการซื้อสินค้าและบริการผ่านร้านค้า e-Commerce (Payment Gateway)		
วัตถุประสงค์ เพื่อให้การดำเนินการของผู้ให้บริการ Payment Gateway มีความรัดกุมปลอดภัย น่าเชื่อถือและพร้อมใช้งาน สอดคล้องกับมาตรฐานสากลและเป็นไปตามกฎหมายหลักเกณฑ์ที่เกี่ยวข้อง		
ขั้นตอน	**แนวปฏิบัติที่ดี**	
การส่ง/รับคำสั่งชำระสินค้าและบริการ	5.1	มีระบบตรวจสอบความถูกต้องของข้อมูลรายการชำระเงินที่รับจากร้านค้าสมาชิก ตัวอย่าง เช่น ■ รหัสร้านค้าที่เป็นสมาชิกและ Issuer ■ ประเภทบัตร เช่น Visa, Master Card เป็นต้น ■ รูปแบบของ Message ตามมาตรฐานที่กำหนดร่วมกัน ■ ลายเซ็นอิเล็กทรอนิกส์ของร้านค้าและ Issuer
	5.2	มีการตรวจสอบข้อมูลที่เข้าสู่ระบบ (Input Validation) โดยอนุญาตเฉพาะข้อมูลที่อยู่ในรูปแบบที่กำหนดเท่านั้น เพื่อป้องกันข้อมูลผิดลักษณะ/รูปแบบ ไม่สมเหตุผล หรือผิด Logic และระบบต้องไม่อนุญาตให้ผู้ใช้บริการข้ามขั้นตอนจนกว่าจะกรอกข้อมูลถูกต้อง
	5.3	มีการตรวจสอบความครบถ้วนของข้อมูลก่อนที่จะทำการประมวลผลในขั้นตอนต่อไป เช่น จำนวนหลักของเลขที่บัตร ความครบถ้วนของ Mandatory Fields เป็นต้น หากข้อมูลใน Mandatory Field ไม่ถูกต้องครบถ้วน ควรมีข้อความแจ้งผู้ใช้บริการทราบ และระบบต้องไม่อนุญาตให้ผู้ใช้บริการข้ามขั้นตอนจนกว่าจะกรอกข้อมูลถูกต้อง
	5.4	มีการกำหนดมาตรฐานของช่วงเวลาในการส่งและรับ Message ระหว่างระบบงาน ให้ครอบคลุมเหตุการณ์กรณีต่าง ๆ ที่อาจทำให้เกิดข้อผิดพลาดในการรับส่ง message ระหว่างระบบ (Time out) เช่น Network Connection Loss, Message Loss เป็นต้น
	5.5	ในกรณีที่การส่งและรับ Message ระหว่างระบบเกินเวลาที่กำหนด (Time out message) ให้ระบบมีการแจ้งสถานะของการไม่ได้รับ Message ให้ระบบต้นทางและปลายทางได้รับทราบ เพื่อให้สามารถดำเนินการในขั้นตอนต่อไปได้อย่างถูกต้อง
การบันทึกและแจ้งผลการทำรายการ	5.6	มีการแสดงผลและรายละเอียดการทำรายการให้ผู้ใช้บริการทราบทันที หลังจากที่ระบบประมวลผลแล้วเสร็จ และมีการจัดเก็บข้อมูลประวัติการทำรายการ (Transaction History) เพื่อให้ผู้ใช้บริการสามารถตรวจสอบย้อนหลังได้

6. บริการ Switching และการหักบัญชีเพื่อชำระดุล (Switching/ Clearing)		
วัตถุประสงค์ เพื่อให้การดำเนินงานของผู้ให้บริการ Switching/ Clearing มีความรัดกุมปลอดภัย น่าเชื่อถือ และพร้อมใช้งาน สอดคล้องกับมาตรฐานสากลและเป็นไปตามกฎหมายหลักเกณฑ์ที่เกี่ยวข้อง		
ขั้นตอน	**แนวปฏิบัติที่ดี**	
การ Switching	6.1	มีการกำหนดข้อตกลงร่วมกันกับสมาชิกเกี่ยวกับ บทบาทหน้าที่ความรับผิดชอบ, ข้อตกลงระดับในการบริการ (Service Level Agreement: SLA), การบริหารจัดการระบบ, การเชื่อมต่อเชิงเทคนิค, และกระบวนการทางธุรกิจที่เป็นมาตรฐานสอดคล้องกัน อย่างชัดเจนเป็นลายลักษณ์อักษร โดยมีการลงนามร่วมกันระหว่างผู้ให้บริการและสมาชิก ข้อตกลงข้างต้นควรมีการทบทวนให้มีความเหมาะสมอย่างสม่ำเสมอ
	6.2	มีการกำหนดรูปแบบ Message ที่เป็นมาตรฐานร่วมกันระหว่างสมาชิก และมีระบบการตรวจสอบความถูกต้องของรูปแบบ Message ซึ่งหากพบว่า Message อยู่ในรูปแบบที่ไม่ถูกต้อง ควรมีการแจ้งกลับ และปฏิเสธการรับ Message ก่อนประมวลผลในขั้นตอนต่อไป
	6.3	มีการกำหนดมาตรฐานของช่วงเวลา (time out) ในการส่งและรับ Message ระหว่างระบบงาน ให้ครอบคลุมเหตุการณ์กรณีต่าง ๆ ที่อาจทำให้เกิดข้อผิดพลาดในการรับส่ง Message ระหว่างระบบ
	6.4	มีการกำหนดแนวปฏิบัติร่วมกันกับสมาชิก เพื่อให้รองรับเหตุขัดข้องต่าง ๆ ที่อาจเกิดขึ้น และสามารถทำงานต่อไปได้อย่างถูกต้องและสอดคล้องกันทั้งระบบ เช่น ▪ กรณีที่การส่งและรับ Message ระหว่างระบบเกินเวลาที่กำหนด (Time out message) ระบบจะต้องแจ้งสถานะของการไม่ได้รับ Message ตอบกลับ ให้ทั้งระบบต้นทางและปลายทางได้รับทราบ เพื่อให้สามารถดำเนินการตามแนวปฏิบัติที่ได้ตกลงไว้ร่วมกัน เพื่อแก้ไขข้อผิดพลาด (เช่นการ reverse รายการ) และดำเนินการในขั้นตอนต่อไปได้อย่างถูกต้อง
	6.5	มีระบบการจัดเก็บข้อมูลการรับส่ง message อย่างเพียงพอสำหรับใช้ในการพิสูจน์การทำรายการระหว่างสมาชิกย้อนหลัง โดยจัดเก็บเป็นไปตามระยะเวลาไม่ต่ำกว่าที่กฎหมายกำหนด และมีการควบคุมการเข้าถึงข้อมูลดังกล่าว
	6.6	มีกระบวนการในการควบคุมดูแลระบบอย่างต่อเนื่อง และทำให้มั่นใจว่าระบบมีความพร้อมและเหมาะสมกับการใช้งานใน

		ปัจจุบัน เช่น ▪ การตรวจสอบความพร้อมใช้งานของระบบ (System Health Checking) ที่ครอบคลุมถึง ○ การตรวจสอบการตั้งค่าระบบ (System Configuration) ของอุปกรณ์ที่มีความสำคัญทั้งของผู้ให้บริการ Switching และของสมาชิก ให้เหมาะสมกับการใช้งานในปัจจุบัน ○ การทบทวนความเพียงพอของทรัพยากรระบบ (System Capacity) ▪ การทดสอบขีดความสามารถในการรับภาระของระบบร่วมกันทั้งวง Switching (Industry Load Test) โดยควรมีเครื่องมือในการจำลองธุรกรรมปริมาณมากเพื่อใช้ในการทดสอบ โดยกระบวนการข้างต้น ควรดำเนินการตามรอบระยะเวลาที่เหมาะสมอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่อาจส่งผลกระทบต่อระบบ
	6.7	มีกระบวนการและ/หรือเครื่องมือในการติดตามและเฝ้าระวังไม่ให้เกิดปัญหาในการให้บริการ และมีแนวปฏิบัติในการตอบสนองและจัดการกับปัญหาที่เกิดขึ้นร่วมกับสมาชิกอย่างชัดเจน รวมถึงกำหนดช่องทางการติดต่อสื่อสารและรายชื่อผู้ประสานงานทั้งผู้ให้บริการและสมาชิกที่เหมาะสม ชัดเจน และมีประสิทธิภาพ
	6.8	มีกระบวนการในการจัดการการเปลี่ยนแปลงอย่างเหมาะสมสำหรับทุกระบบงานที่เกี่ยวข้อง รวมถึงระบบงานภายในของสมาชิกแต่ละรายที่อาจส่งผลกระทบต่อการให้บริการ Switching โดยรวม โดยควรมีการดำเนินการดังต่อไปนี้ เป็นอย่างน้อย 1. มีการวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลงที่จะดำเนินการ 2. มีช่องทาง วิธีการ และกระบวนการในการสื่อสาร ชี้แจ้งข้อมูลการเปลี่ยนแปลงและทาความเข้าใจร่วมกันระหว่างผู้เกี่ยวข้องรวมถึง ธปท. อย่างชัดเจนและเป็นทางการ โดยมีการบันทึกเป็นความตกลงร่วมกันเป็นลายลักษณ์อักษร 3. มีการทดสอบระบบที่เกี่ยวข้องร่วมกัน ซึ่งอาจพิจารณาให้มีการทดสอบร่วมกันทั้งวง Switching (Industry-Wide Test) ในกรณีการเปลี่ยนแปลงมีนัยสำคัญ หรืออาจกระทบต่อระบบโดยรวม โดยมีขั้นตอนการลงนามรับรองผลการทดสอบ และจัดเก็บเอกสารประกอบการทดสอบอย่างเป็นระบบ 4. มีการจัดเตรียมแผนย้อนกลับ (Roll Back Plan) และแผน

		สำรองฉุกเฉินกรณีที่ทาการเปลี่ยนแปลงไม่สำเร็จ (Fall Back Plan) เพื่อรองรับกรณีเกิดปัญหาในระหว่างการเปลี่ยนแปลง โดยมีกระบวนการในการพิจารณาความเสี่ยง, ผลกระทบ, และแนวทางการแก้ปัญหา ที่เห็นชอบร่วมกันกับสมาชิก
การ Clearing	6.9	มีการกำหนดข้อตกลงและกระบวนการ Clearing ที่เป็นมาตรฐานเป็นลายลักษณ์อักษรอย่างชัดเจน โดยมีการลงนามร่วมกันกับสมาชิกและผู้ให้บริการชำระดุล (Settlement Agent) เช่น ■ รูปแบบ Clearing File ที่ส่งให้ Settlement Agent ■ การตรวจสอบความถูกต้องของรูปแบบ Clearing File ■ รอบระยะเวลาในการ Clearing ระหว่างกัน และกำหนดเวลา cut-off time ของแต่ละรอบให้ชัดเจน
	6.10	มีระบบตรวจสอบความถูกต้องของข้อมูล Clearing File ที่จะส่งให้ Settlement Agent เพื่อชำระดุล ดังนี้ ■ รูปแบบ Clearing File ■ รหัสสมาชิกผู้รับและผู้ส่ง ■ จำนวนรายการต่อไฟล์ ■ ยอดรวมของมูลค่ารายการ Clearing ทั้งหมดในไฟล์ ■ ยอดรวมสุทธิของรายการฝั่ง Debit และฝั่ง Credit ต้องมีค่าเป็น 0
	6.11	มีระบบในการจัดทำรายงานที่แสดงรายการ Unmatched เพื่อให้สมาชิกสามารถตรวจสอบความถูกต้องและมีกระบวนการในการให้สมาชิกส่งรายการเพื่อปรับปรุงแก้ไข (Adjust) รายการ Unmatched ตามรอบระยะเวลาที่เหมาะสม ทั้งนี้ขึ้นกับจำนวนสมาชิกและปริมาณธุรกรรม
	6.12	มีระบบในการสรุปยอดดุลสุทธิของสมาชิก (Netting) และมีกระบวนการตรวจสอบความถูกต้องของยอดได้ดุล/เสียดุลของสมาชิกในแต่ละรอบการชำระดุล และ/หรือทุกสิ้นวัน
	6.13	มีระบบการจัดเก็บข้อมูลการ Clearing อย่างเพียงพอสำหรับใช้ในการพิสูจน์การทำรายการระหว่างสมาชิกย้อนหลัง โดยจัดเก็บเป็นระยะเวลาไม่ต่ำกว่าที่กฎหมายกำหนด และมีการควบคุมการเข้าถึงข้อมูลดังกล่าว
	6.14	มีช่องทางและระบบให้สมาชิกสามารถเรียกดูข้อมูลที่เกี่ยวข้องและสามารถนาออกไปใช้ประมวลผลในระบบงานของสมาชิกได้ ได้แก่ ■ ยอดดุลระหว่างวันแบบ Real-time เพื่อให้สมาชิกสามารถใช้บริหารจัดการสภาพคล่อง

		▪ สรุปยอดดุลในแต่ละรอบ Clearing และหรือแต่ละวัน
	6.15	มีการกำหนดนโยบาย/ปฏิบัติ ให้ครอบคลุมเหตุติดขัดต่าง ๆ ที่อาจเกิดขึ้น เพื่อให้มั่นใจว่าการชำระดุลจะดำเนินต่อไปได้ เช่น เมื่อมีสมาชิกบางรายไม่สามารถชำระดุลได้ ผู้ให้บริการอาจดำเนินการ Unwind (การหักยอดของสมาชิกรายที่มีปัญหาออกแล้วคำนวณ Netting Position ของสมาชิกที่เหลือใหม่) และส่งชำระดุลด้วยยอดใหม่ หรือผู้ให้บริการอาจจะให้สมาชิกดังกล่าวกู้เพื่อให้สามารถชำระดุลได้สำเร็จ

ภาคผนวก ค แนวนโยบาย เรื่องการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) สำหรับสถาบันการเงิน

ธนาคารแห่งประเทศไทย

27 ธันวาคม 2562

เรียน ผู้จัดการ

สถาบันการเงินทุกธนาคาร

ที่ ธปท.ฝตท.(01) ว.1922/2562 เรื่อง นำส่งแนวนโยบาย เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security)

ปัจจุบันสถาบันการเงิน และผู้ให้บริการการชำระเงินให้บริการทางการเงินผ่านช่องทางอุปกรณ์เคลื่อนที่เป็นช่องทางหลัก และการใช้บริการผ่านช่องทางดังกล่าวมีปริมาณเพิ่มขึ้นอย่างรวดเร็วและขยายตัวอย่างต่อเนื่อง ขณะเดียวกันการให้บริการผ่านช่องทางดังกล่าวทำให้ต้องเผชิญกับภัยคุกคามทางไซเบอร์ (cyber threat) ที่ปัจจุบันมีความหลากหลายและซับซ้อนมากขึ้น อาจก่อให้เกิดความเสียหายต่อลูกค้าผู้ใช้บริการได้ ธนาคารแห่งประเทศไทย (ธปท.) ได้ดูแลเรื่องดังกล่าวมาอย่างต่อเนื่องโดยได้ออกแนวนโยบายว่าด้วยการเสริมสร้างความเชื่อมั่นการชำระเงินโดยอุปกรณ์เคลื่อนที่ (Guiding Principles for Trusted Mobile Payments) ลงวันที่ 24 มีนาคม 2560 อย่างไรก็ตาม เพื่อยกระดับความมั่นคงปลอดภัยในการให้บริการทางการเงินผ่านช่องทางอุปกรณ์เคลื่อนที่ ป้องกันและควบคุมความเสี่ยงจากภัยคุกคามสำคัญได้อย่างรัดกุมเพียงพอตามมาตรฐานสากลให้ประชาชนเกิดความเชื่อมั่นในการใช้บริการ ธปท. จึงได้ออกแนวนโยบายการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) ที่ให้บริการแก่ลูกค้ารายย่อย ซึ่งประกอบด้วยมาตรการ 2 ระดับ คือ (1) มาตรการขั้นต่ำที่จำเป็นต้องดำเนินการเพื่อความรัดกุมด้านความมั่นคงปลอดภัยในการให้บริการ (2) มาตรการเพิ่มเติมที่อาจพิจารณาดำเนินการเพื่อให้เกิดความรัดกุมปลอดภัยยิ่งขึ้น

ทั้งนี้ ธปท. กำหนดให้สถาบันการเงิน ที่ให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ (Mobile Banking Application) แก่ผู้ใช้บริการลูกค้ารายย่อย ดำเนินการตามแนวนโยบายนี้ และขอให้หน่วยงานบริหารความเสี่ยงหน่วยงานกำกับการปฏิบัติตามหลักเกณฑ์ และหน่วยงานตรวจสอบภายในของสถาบันการเงิน กำกับดูแลการปฏิบัติตามแนวนโยบายดังกล่าว ให้เกิดการถ่วงดุลตามหลัก three lines of defense

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นายรณดล นุ่มนนท์)
รองผู้ว่าการ ด้านเสถียรภาพสถาบันการเงิน
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย แนวนโยบายการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security)

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 6347, 0 2283 6574
E-Mail ITSupervision@bot.or.th

หมายเหตุ [X] ธนาคารได้จัดประชุมชี้แจง ในวันที่ 16 ตุลาคม 2562 ณ ธนาคารแห่งประเทศไทย
[ ] ไม่มีการประชุมชี้แจง

แนวนโยบาย
เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงิน
บนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security)
สำหรับสถาบันการเงิน

---

1. เหตุผลในการออกแนวนโยบาย

ปัจจุบันสถาบันการเงินให้บริการทางการเงินผ่านช่องทางอุปกรณ์เคลื่อนที่เป็นช่องทางหลัก และการใช้บริการผ่านช่องทางดังกล่าวมีปริมาณเพิ่มขึ้นอย่างรวดเร็วและขยายตัวอย่างต่อเนื่อง ขณะเดียวกัน การให้บริการผ่านช่องทางดังกล่าวทำให้ต้องเผชิญกับภัยคุกคามทางไซเบอร์ (cyber threat) ที่ปัจจุบันมีความหลากหลายและซับซ้อนมากขึ้น อาจก่อให้เกิดความเสียหายต่อลูกค้าผู้ใช้บริการได้ ธนาคารแห่งประเทศไทย (ธปท.) ได้ดูแลเรื่องดังกล่าวมาอย่างต่อเนื่องโดยได้ออกแนวนโยบายว่าด้วยการเสริมสร้างความเชื่อมั่นการชำระเงินโดยอุปกรณ์เคลื่อนที่ (Guiding Principles for Trusted Mobile Payments) ลงวันที่ 24 มีนาคม 2560 อย่างไรก็ตาม เพื่อยกระดับความมั่นคงปลอดภัย ในการให้บริการทางการเงินผ่านช่องทางอุปกรณ์เคลื่อนที่ให้มั่นใจว่าสามารถป้องกัน และควบคุมความเสี่ยงจากภัยคุกคามสำคัญได้อย่างรัดกุม เพียงพอตามมาตรฐานสากล ให้ประชาชนเกิดความเชื่อมั่นในการใช้บริการ ธปท. จึงได้ออกแนวนโยบายการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) ที่ให้บริการแก่กลุ่มลูกค้ารายย่อย ซึ่งประกอบด้วยมาตรการ 2 ระดับ คือ

1. มาตรการขั้นต่ำที่จำเป็นต้องดำเนินการเพื่อความรัดกุมด้านความมั่นคงปลอดภัยในการให้บริการ

2. มาตรการเพิ่มเติมที่อาจพิจารณาดำเนินการเพื่อให้เกิดความรัดกุมปลอดภัยยิ่งขึ้น

ทั้งนี้ แนวนโยบายฉบับนี้ครอบคลุมด้านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ ด้านอุปกรณ์เคลื่อนที่ของลูกค้า ด้านระบบเครือข่ายที่เชื่อมต่อกับผู้ใช้บริการหรือผู้ให้บริการภายนอก ด้านระบบประมวลผล และด้านการวางแอปพลิเคชันบนแพลตฟอร์มอิเล็กทรอนิกส์ (e-Marketplace) โดยอ้างอิงตามมาตรฐานการทดสอบที่เป็นสากล เช่น OWASP Mobile Top 10 เป็นต้น

2. ขอบเขตของการถือปฏิบัติ

แนวนโยบายฉบับนี้ใช้กับสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินที่ให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ แก่ผู้ใช้บริการกลุ่มลูกค้ารายย่อย

3. เนื้อหา

3.1 คำจำกัดความ

"อุปกรณ์เคลื่อนที่" หมายความว่า อุปกรณ์อิเล็กทรอนิกส์แบบพกพา ซึ่งมีความสามารถในการเชื่อมต่อกับอุปกรณ์อื่น เพื่อรับหรือส่งข้อมูลทางการเงิน การชำระเงิน หรือคำสั่งการชำระเงินผ่านระบบเครือข่ายโทรคมนาคมไร้สายหรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้าเป็นสื่อกลาง

"ผู้ให้บริการ" หมายความว่า สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินที่ให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่แก่ผู้ใช้บริการกลุ่มลูกค้ารายย่อย

"ผู้ใช้บริการ" หมายความว่า ผู้ใช้บริการทางการเงินและการชำระเงินโดยช่องทางการให้บริการผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่กับผู้ให้บริการ

3.2 มาตรการการรักษาความมั่นคงปลอดภัย

แนวนโยบายการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ฉบับนี้ ประกอบด้วยมาตรการ 2 ระดับ คือ 1. มาตรการขั้นต่ำ ที่จำเป็นต้องดำเนินการเพื่อความรัดกุมด้านความมั่นคงปลอดภัยในการให้บริการ และ 2. มาตรการเพิ่มเติมที่อาจพิจารณาดำเนินการเพื่อให้เกิดความรัดกุมปลอดภัยยิ่งขึ้น ดังนี้

1. มาตรการขั้นต่ำ เป็นมาตรการที่ป้องกันความเสี่ยงจากภัยคุกคามไซเบอร์ที่ส่งผลกระทบต่อผู้ใช้บริการและความเชื่อมั่นในวงกว้าง โดยผู้ให้บริการต้องดำเนินการปรับปรุงการรักษาความมั่นคงปลอดภัยของแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ให้เป็นไปตามมาตรการขั้นต่ำ ดังนี้

ด้านระบบ

(1) ไม่อนุญาตให้ใช้อุปกรณ์เคลื่อนที่ที่เปิดสิทธิ์ให้เข้าถึงระบบปฏิบัติการ (rooted/jailbroken) เข้าใช้งานแอปพลิเคชัน เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลสำคัญของผู้ใช้บริการ และละเมิดหรือหลีกเลี่ยงมาตรการการรักษาความมั่นคงปลอดภัยที่ผู้ให้บริการกำหนดไว้

(2) ไม่อนุญาตให้อุปกรณ์เคลื่อนที่ที่ใช้ระบบปฏิบัติการล้าสมัย (obsolete Operating System : OS) มีช่องโหว่ร้ายแรงที่ประกาศจากหน่วยงานด้านความมั่นคงปลอดภัยที่เป็นสากลและกระทบการใช้งานของผู้ใช้บริการในวงกว้างเข้าใช้งานแอปพลิเคชัน ทั้งนี้ ในกรณีที่ obsolete OS มีช่องโหว่อื่นที่ไม่กระทบผู้ใช้บริการในวงกว้าง ควรมีมาตรการรองรับเพื่อลดความเสี่ยงของผู้ให้บริการและผู้ใช้บริการตามความเหมาะสม เช่น การแจ้งเตือนผู้ใช้บริการ การจำกัดวงเงินธุรกรรม และการเพิ่มมาตรการยืนยันตัวตน

(3) ขอสิทธิ์เข้าถึงทรัพยากรหรือบริการโดยแอปพลิเคชัน (application permission) บนอุปกรณ์เคลื่อนที่ของผู้ใช้บริการเท่าที่จำเป็น และมีกระบวนการทบทวนการขอสิทธิ์ดังกล่าวอย่างเป็นประจำ เพื่อป้องกันการละเมิดสิทธิ์ความเป็นส่วนตัวของผู้ใช้บริการ

(4) ป้องกัน source code ส่วนสำคัญ เช่น การโอนเงิน การพิสูจน์ตัวตน ไม่ให้รั่วไหลจากแอปพลิเคชัน เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีทำการแก้ไข เปลี่ยนแปลง source code ดังกล่าว

(5) ป้องกันการฝังข้อมูลสำคัญ หรือ code ที่ไม่พึงประสงค์ (malicious code) บนแอปพลิเคชัน

(6) เข้ารหัสไฟล์ข้อมูล (files encryption) ที่จัดเก็บข้อมูลสำคัญบนอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ เพื่อป้องกันข้อมูลสำคัญของผู้ใช้บริการรั่วไหล

(7) ไม่อนุญาตให้ผู้ใช้บริการใช้แอปพลิเคชันเวอร์ชั่นต่ำกว่าที่ผู้ให้บริการกำหนด เพื่อให้แอปพลิเคชันมีการรักษาความมั่นคงปลอดภัยเป็นไปตามมาตรฐานของผู้ให้บริการ

(8) ป้องกันการโจมตีในลักษณะ Distributed denial-of-service (DDoS Attack) ในระดับเครือข่าย (network layer) เพื่อป้องกันระบบจากการถูกโจมตีจนไม่สามารถให้บริการได้

(9) ป้องกันภัยจากการถูกดักจับหรือแก้ไขเปลี่ยนแปลงข้อมูลระหว่างการรับส่ง (Man in the Middle Attack) โดยยืนยันตัวตนด้วยเทคนิค Certificate Pinning หรือวิธีอื่นที่เทียบเท่า และการใช้ช่องทางสื่อสารที่ปลอดภัย (secure protocol) ในการรับส่งข้อมูล

(10) ป้องกันการสวมรอยการเข้าใช้งานของลูกค้า (Session Hijacking)

(11) ป้องกันการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (server) โดยไม่ได้รับอนุญาต เช่น การเข้าถึงโดยอาศัยวิธี SQL Injection, Local File Inclusion หรือ Directory Traversal เพื่อลดความเสี่ยงจากข้อมูลรั่วไหลและระบบถูกโจมตี

(12) ตรวจสอบและรับมือแอปพลิเคชันปลอมบนแพลตฟอร์มอิเล็กทรอนิกส์ที่เป็นที่ยอมรับและน่าเชื่อถือ (official e-Marketplace) เช่น Google Play Store, App Store เพื่อลดความเสี่ยงจากการที่ลูกค้า download และติดตั้งแอปพลิเคชันปลอม

ด้านการดูแลลูกค้าผู้ใช้บริการ

(1) ผู้ให้บริการต้องจัดให้มีการเสริมสร้างความรู้ความเข้าใจการใช้บริการเทคโนโลยีทางการเงินให้แก่ประชาชน ทั้งความรู้เกี่ยวกับภัยคุกคามใหม่ ๆ และวิธีการปฏิบัติตนให้ปลอดภัยในการใช้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ในเชิงรุกและต่อเนื่อง

(2) จัดให้มีแนวปฏิบัติการให้บริการลูกค้าในการใช้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่แก่พนักงานของสถาบันการเงิน และดูแลให้พนักงาน

ถือปฏิบัติอย่างรัดกุมเข้มงวด และระมัดระวังไม่ดำเนินการในลักษณะที่ก่อให้เกิดความเสี่ยง เช่น กรณีพนักงานสาขาติดตั้งแอปพลิเคชันให้ลูกค้า ควรดำเนินการเท่าที่จำเป็น ไม่เข้าถึงข้อมูลสำคัญของลูกค้าและไม่ใส่รหัสผ่านแทนลูกค้า เป็นต้น ซึ่งอาจนำไปสู่การก่อทุจริตได้

2. มาตรการเพิ่มเติม เพื่อให้การให้บริการผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่มีการรักษาความมั่นคงปลอดภัยเข้มแข็งมากยิ่งขึ้น ผู้ให้บริการควรพิจารณาดำเนินการเพิ่มเติม ดังนี้

(1) ตรวจสอบการเปลี่ยนแปลงแก้ไขแอปพลิเคชัน เมื่อผู้ใช้บริการเข้าใช้งานในทันที (Anti-Tampering) เพื่อป้องกันไม่ให้ข้อมูลผู้ใช้บริการรั่วไหลหรือเกิดความเสียหาย จากแอปพลิเคชันที่มีการดัดแปลงแก้ไขโดยฝัง malicious code ไว้

(2) กำหนดให้ตั้งค่า PIN หรือ รหัสผ่านที่ซับซ้อน (PIN / password complexity) ในการเข้าใช้งานแอปพลิเคชันเพื่อให้ยากต่อการคาดเดา

(3) แสดงผลข้อมูลผู้ใช้บริการบนแอปพลิเคชันอย่างรัดกุม เช่น การปิดบังข้อมูลสำคัญของลูกค้า (sensitive data masking) การปิดบังหน้าจอเมื่อย่อแอปพลิเคชัน (Application Blurring) เพื่อลดความเสี่ยงที่ข้อมูลสำคัญของผู้ใช้บริการจะรั่วไหล

(4) ป้องกันภัยคุกคามในระดับแอปพลิเคชัน (application layer) เช่น การเข้ารหัสข้อมูลสำคัญระหว่างรับ/ส่ง การป้องกัน DDoS Attack เพื่อยกระดับการป้องกันข้อมูลรั่วไหลระหว่างรับ/ส่ง หรือป้องกันระบบถูกโจมตีจนไม่สามารถให้บริการได้

(5) ตรวจสอบและรับมือแอปพลิเคชันปลอมบน website อื่น นอกเหนือจากแพลตฟอร์มอิเล็กทรอนิกส์ที่เป็นที่ยอมรับและน่าเชื่อถือ (official e-Marketplace) เช่น บน darkweb เป็นต้น

4. วันที่ประกาศให้ทราบ

แนวนโยบายฉบับนี้ให้ใช้บังคับตั้งแต่วันที่ 1 พฤษภาคม 2563 เป็นต้นไป

คำถาม – คำตอบแนบท้ายแนวนโยบาย

เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงิน บนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security)

ลำดับ	คำถาม	คำตอบ
1	ธปท. จะมีการกำหนดหรือไม่ว่า จะต้องดำเนินการภายในระยะเวลาเท่าไหร่ หลังจากที่ผู้ให้บริการประกาศรายชื่อ obsolete OS	สถาบันการเงินต้องปรับปรุงระบบและเตรียมการสื่อสารแก่ลูกค้า สำหรับกรณีผู้พัฒนาระบบปฏิบัติการประกาศ obsolete OS และพบช่องโหว่ร้ายแรง ธปท. เห็นว่าควรดำเนินการภายในระยะเวลา 3 เดือน ส่วนกรณีผู้พัฒนาระบบปฏิบัติการประกาศ obsolete OS แต่ยังไม่พบช่องโหว่ร้ายแรง ควรดำเนินการ ภายในระยะเวลา 6 เดือน
2	ธปท. จะมีประกาศไหมว่า OS รุ่นไหนจะไม่ให้เข้าใช้งาน จะได้ปฏิบัติได้ตรงกันทุกสถาบันการเงิน	สถาบันการเงินควรมีกระบวนการติดตามการประกาศ obsolete OS และช่องโหว่ร้ายแรงจากผู้พัฒนาระบบปฏิบัติการอย่างสม่ำเสมอ รวมทั้งควรกำหนดเป็นนโยบาย มาตรฐานหรือแนวปฏิบัติว่าระบบปฏิบัติการใดที่สถาบันการเงินไม่สามารถยอมรับความเสี่ยงได้ ทั้งนี้ สถาบันการเงินอาจหารือร่วมกับสมาชิกในกลุ่ม TB-CERT เพื่อกำหนดมาตรฐานร่วมกัน
3	ปัจจุบันสถาบันการเงินพบปัญหาเครื่องมือถือใหม่ที่มาจากบางแหล่งผลิต แต่ระบบมองว่าเป็นการ rooted เป็นไปได้หรือไม่ ให้มีการรับรองจาก กสทช. ก่อน	ธปท. อยู่ระหว่างการหารือร่วมกับ กสทช. ถึงการยกระดับความปลอดภัยของเครื่องมือถือที่นำเข้ามาใช้งานในประเทศไทย
4.	ธปท. มีรายชื่อ list โปรแกรม bypass การทำ rooted/jailbreak และการทำ Certificate Pinning ไหม ที่จะต้องสามารถป้องกันได้เป็นขั้นต่ำ	โปรแกรม bypass ขั้นต่ำจะเป็นโปรแกรมลักษณะ off-the-self คือสามารถดาวน์โหลดมาใช้งานได้ทันที โดยไม่ต้องใช้ความรู้เชิงลึก เช่น โปรแกรม RootCloak, Magisk, tsProtector สำหรับการ rooted/jailbreak และโปรแกรม SSLUnpinning, SSL Kill Switch สำหรับ Certificate Pinning เป็นต้น อย่างไรก็ดี โปรแกรมข้างต้น เป็นเพียงโปรแกรมตัวอย่างในระดับพื้นฐาน สถาบันการเงินควรพิจารณาโปรแกรมหรือเทคนิคในการ bypass อื่นเพิ่มเติมด้วย

5.	ธปท. จะมีข้อความการสื่อสารต่อผู้ใช้บริการในภาพรวมเดียวกัน เพื่อให้เกิดความชัดเจนและสื่อสารไปในทิศทางเดียวกันไหม ทั้งกรณี Rooted/Jailbroken และ Obsolete OS	สถาบันการเงินสามารถตกลงร่วมกันเพื่อกำหนดข้อความการสื่อสารให้กับประชาชนผู้ใช้บริการเพื่อให้เกิดความชัดเจนและสื่อสารไปในทิศทางเดียวกัน โดยเมื่อตกลงร่วมกันแล้ว สถาบันการเงินอาจนำข้อความที่ตกลงร่วมกันหารือกับ ธปท. ได้
6.	การป้องกัน Anti-tampering ของ 3rd party เป็นการลงทุนที่ค่อนข้างสูงของสถาบันการเงิน เป็นไปได้หรือไม่ที่จะกำหนดวิธีการที่เทียบเคียงให้ทางสถาบันการเงินปฏิบัติตาม	สถาบันการเงินสามารถใช้เทคนิคอื่นในการตรวจสอบได้ เช่น ตรวจสอบจากค่า Hashing หรือ ตรวจสอบจาก Certificate โดยเทคนิคดังกล่าวต้องสามารถป้องกันแอปพลิเคชันที่มีการดัดแปลงแก้ไขและยังสามารถเข้าใช้งานได้
7.	ธปท. ควรประกาศฟิลด์ข้อมูล sensitive data ให้ชัดเจน เพื่อให้เป็นมาตรฐานเดียวกันกับทุกสถาบันการเงิน	สถาบันการเงินแต่ละแห่งกำหนดข้อมูล sensitive ไม่เหมือนกัน ขึ้นอยู่กับปัจจัยต่าง ๆ เช่น ประเภทธุรกิจ กลุ่มลูกค้าเป้าหมาย เป็นต้น อย่างไรก็ตามทุกแห่งมีเกณฑ์การจัดชั้นความลับของข้อมูล (data classification) ที่ประกาศใช้อย่างเป็นทางการ ดังนั้นการกำหนดข้อมูล sensitive สถาบันการเงินจึงควรอ้างอิงตามหลักเกณฑ์ดังกล่าว
8.	กรณี fake app ขอทราบความเหตุผลที่ ธปท. กำหนดเรื่องนี้	เนื่องด้วย fake app เป็นวิธีการที่ใช้ในการล่อล่วงให้ใช้งานเพื่อโจรกรรมข้อมูลลูกค้า ซึ่งนำไปสู่การทุจริตทำให้เกิดความเสียหายต่อลูกค้าและอาจส่งผลกระทบต่อเนื่องมายังความเชื่อมั่นที่มีต่อสถาบันการเงิน การที่สถาบันการเงินสามารถตรวจจับและควบคุม fake app ได้รวดเร็ว จะช่วยลดความเสี่ยงดังกล่าว