ธนาคารแห่งประเทศไทย

แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices)

Phase 1: ธุรกรรมฝาก ถอน และโอนเงิน

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ
สายกำกับสถาบันการเงิน
พฤศจิกายน 2556

สารบัญ

Executive Summary

เหตุผลความจำเป็น

ปัจจุบันระบบเทคโนโลยีสารสนเทศ (IT) เป็นโครงสร้างพื้นฐานสำคัญที่ใช้รองรับกลยุทธ์และกระบวนการดำเนินธุรกิจด้านต่าง ๆ (Business Process) ของธนาคารพาณิชย์ (ธพ.) ซึ่งจุดอ่อนหรือช่องโหว่ของระบบ IT อาจมีผลต่อความปลอดภัย ความถูกต้อง ความต่อเนื่องต่อการให้บริการทางการเงินแก่ลูกค้าประชาชน และอาจส่งผลกระทบถึงภาพลักษณ์ความน่าเชื่อถือของ ธพ. ได้

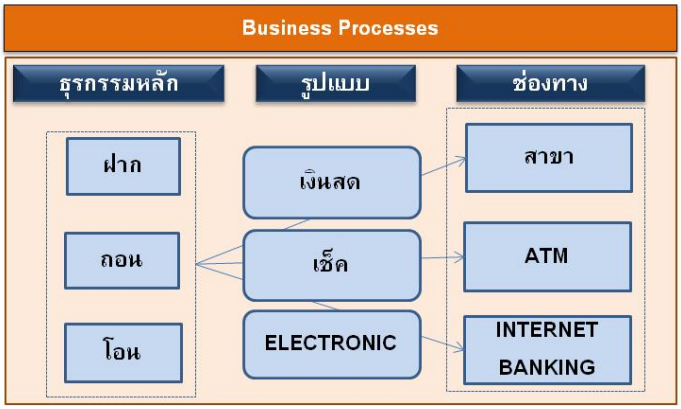
อย่างไรก็ตาม ระบบ IT ของ ธพ. แต่ละแห่งที่ใช้รองรับการให้บริการทางการเงินพื้นฐาน เช่น ธุรกรรมเงินฝาก ถอนและโอนเงิน ยังมีมาตรฐานการควบคุมภายในที่แตกต่างหลากหลาย ดังนั้น การมีมาตรฐานแนวปฏิบัติการควบคุมภายในที่ดีสอดคล้องกับมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป สำหรับใช้ในการควบคุมความเสี่ยงของระบบ IT จะช่วยให้การพัฒนาโครงสร้างพื้นฐานระบบ IT เอื้อต่อการสนับสนุนกลยุทธ์การขยายธุรกิจของ ธพ. ในอนาคต สร้างความมั่นใจในการใช้บริการของลูกค้าประชาชน ตลอดจนพัฒนาการกำกับดูแลสถาบันการเงินของ ธปท. ให้ทันกับวิวัฒนาการและความเสี่ยงที่เปลี่ยนแปลงด้วยเช่นกัน

ในปี 2556 ธปท. จึงจัดให้มีโครงการจัดทำแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยง (IT Best Practices) ด้าน Operational/ IT Risk Management ของ ธพ. เชื่อมโยงกับธุรกิจหลัก โดยใน Phase 1 ได้จัดทำแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงรองรับธุรกรรมด้านเงินฝาก ถอน และโอนเงิน ผ่านช่องทางสาขา ATM และ Internet Banking โดยมีบริษัท Deloitte Touche Tohmastsu (บริษัท Delloitte) เป็นที่ปรึกษาโครงการ เพื่อให้ IT Best Practices เป็นที่ยอมรับและสอดคล้องกับมาตรฐานสากลที่เกี่ยวข้อง

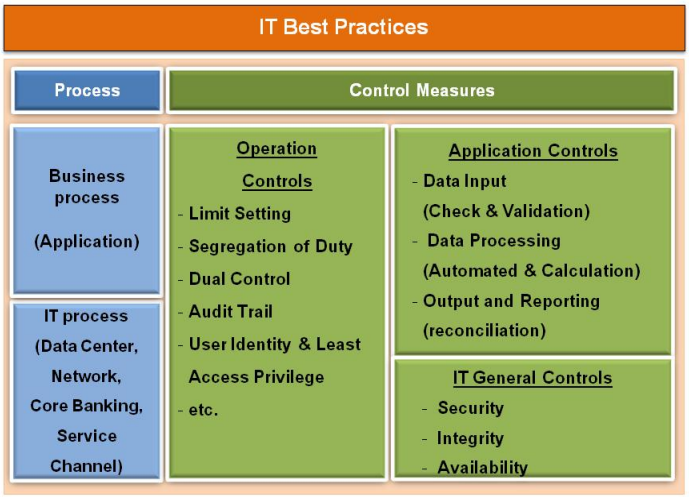
นอกจากนี้ ธพ. ไทยทุกแห่งเห็นด้วยและให้ความร่วมมือและความคิดเห็นที่เป็นประโยชน์อย่างยิ่ง ที่ช่วยให้แนวปฏิบัติที่ดีฉบับนี้มีความชัดเจน ยืดหยุ่น เป็นไปตามหลักสากลที่นำไปปฏิบัติได้และเหมาะสมกับระบบ ธพ. ไทย

สรุปสาระสำคัญของ IT Best Practices

การจัดทำ IT Best Practices ที่ดีต้องอาศัยพื้นฐานความเข้าใจในกระบวนการทางธุรกิจ (Business Process) ที่เกี่ยวข้องกับการทำธุรกรรมเงินฝาก ถอน และโอนเงิน โครงสร้างและกระบวนการของระบบ IT (IT Process) ที่สนับสนุนธุรกิจดังกล่าว เพื่อนำมาประเมินความเสี่ยงของกระบวนการทางธุรกิจ (Operational Risk) ตามมาตรฐาน Basel II และกำหนดแนวปฏิบัติการควบคุมภายในที่ดี



ดังนั้น สาระของ IT Best Practices จึงแบ่งออกเป็น 2 ส่วน คือ แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของกระบวนการทำธุรกิจหลัก และแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบ IT ที่ใช้รองรับธุรกรรมด้านเงินฝาก ถอน และโอนเงิน โดยกรอบในการจัดทำจะอ้างอิงหลักมาตรฐานสากล เกี่ยวกับการควบคุมภายในและระบบ IT เช่น กรอบแนวทางการตรวจสอบเทคโนโลยี Global Technology Audit Guide (GTAG) และกรอบการควบคุมด้านความปลอดภัยเทคโนโลยีสารสนเทศ ISO27001 เป็นต้น



1. แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของกระบวนการทำธุรกิจหลัก (ฝาก ถอน และโอนเงิน) จัดทำครอบคลุมกระบวนการเปิด/ปิดสาขา การเปิดบัญชีเงินฝาก และการทำธุรกรรมฝาก ถอนและโอนเงินผ่านช่องทางสาขา ATM และ Internet Banking โดยมีการควบคุมความเสี่ยงที่ดี เช่น การใช้เครื่องมือพิสูจน์ตัวตนลูกค้าจากบัตรประชาชนอิเล็กทรอนิกส์ การกำหนดสิทธิ์ให้แก่พนักงานเท่าที่จำเป็นตามบทบาทหน้าที่ การพิสูจน์ตัวตนของผู้อนุมัติรายการด้วยวิธีการที่ปลอดภัย เป็นต้น ซึ่งอาจเป็นได้ทั้งการควบคุมด้วยระบบ IT (Application Controls) และ/หรือ การควบคุมด้วยระเบียบวิธีปฏิบัติงาน (Operation Controls)

2. แนวปฏิบัติที่ดีสำหรับการควบคุมระบบ IT ที่สนับสนุนธุรกิจหลัก จะครอบคลุมโครงสร้างระบบ IT ที่สำคัญซึ่งประกอบด้วย Data Center ระบบเครือข่ายสื่อสาร (Network) ระบบ Core Banking และระบบช่องทางการให้บริการต่าง ๆ โดยการควบคุมระบบ IT ที่ดีจะครอบคลุมเรื่องสำคัญ 3 เรื่อง ได้แก่ (1) Access Control คือ การควบคุมระบบ IT เพื่อป้องกันการถูกบุกรุกและเข้าถึงโดยไม่ได้รับอนุญาต เช่น การพิสูจน์ตัวตนของผู้เข้าใช้งานระบบ IT การให้สิทธิ์แก่ผู้ใช้งานตามความจำเป็น (2) Security Management คือ การบริหารจัดการระบบ IT ให้มีความปลอดภัย เพื่อให้ระบบและข้อมูลมีความถูกต้อง เช่น การตั้งค่าความปลอดภัยระบบ IT การควบคุมการแก้ไขหรือเปลี่ยนแปลงระบบ IT และ (3) Availability Management คือ การบริหารจัดการระบบ IT ให้มีความพร้อมในการรองรับการทำธุรกรรมอย่างต่อเนื่อง เช่น การจัดเตรียมระบบ IT และข้อมูลชุดสำรอง เป็นต้น ซึ่งทั้ง 3 ด้าน สอดคล้องกับหลักการตรวจสอบ IT (Security Integrity Availability : SIA) ของ ธปท. ในปัจจุบัน

ประโยชน์ของการจัดทำ IT Best Practices

ธปท. มุ่งหวังให้ IT Best Practices นี้เกิดประโยชน์ในวงกว้าง โดย ธพ. สามารถนำแนวปฏิบัติที่ดีนี้ไปประเมินความเสี่ยงและการควบคุมด้วยตนเอง (Self Control System) ตลอดจนการนำไปใช้เป็น benchmark เพื่อการพัฒนาปรับปรุงระบบ IT ให้มีความปลอดภัย ความถูกต้อง และความพร้อมใช้งานเทียบเคียงแนวปฏิบัติที่เป็นมาตรฐานสากล นอกจากนี้ IT Best Practices จะช่วยยกระดับโครงสร้างพื้นฐานระบบ IT ของ ธพ. ไทย ทั้งระบบให้มีมาตรฐานที่ดียิ่งขึ้นในการรองรับการขยายธุรกิจและการเพิ่มประสิทธิภาพในการให้บริการทางการเงินแก่ลูกค้าประชาชน ตลอดจนเพิ่มศักยภาพทางการแข่งขันให้เทียบเคียงกับ ธพ. ต่างประเทศ

นอกจากนี้ IT Best Practices สามารถนำมาใช้พัฒนาแนวทางการตรวจสอบด้าน IT ของ ธปท. ให้มีความทันสมัยและช่วยผลักดันให้ ธพ. ปรับปรุงระบบ IT ให้สอดคล้องกับมาตรฐานสากลต่อไป **อย่างไรก็ดี ธปท. ตระหนักดีว่า ธพ. ไทยแต่ละแห่งมีความพร้อมในการพัฒนาด้าน IT แตกต่างกัน ซึ่งเป็นผลมาจากการมีนโยบายการทำธุรกิจ แผนการลงทุน ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน ดังนั้น การดำเนินโครงการใน Phase 2 ปี 2557 ธปท. จะศึกษาจัดทำแนวปฏิบัติที่ยอมรับได้ (Acceptable Practices) และประเมิน Gap ร่วมกับ ธพ. แต่ละแห่ง เพื่อเป็นแนวทางให้ ธปท. และ ธพ. ร่วมกันพิจารณาความเหมาะสมของการจัดทำแผนพัฒนาปรับปรุงระบบ IT ของตนเองให้ได้ตามมาตรฐานสากล ทั้งในระยะสั้นและระยะยาวต่อไป**

อนึ่ง แนวปฏิบัติการควบคุมภายในที่ดีฉบับนี้ได้จัดทำให้มีความเหมาะสมกับลักษณะธุรกิจและบริการของ ธพ. ไทย ซึ่งอาจมีความแตกต่างและยังไม่ครอบคลุมผลิตภัณฑ์และบริการการเงินของ ธพ. ในต่างประเทศ ดังนั้น จึงจำเป็นต้องปรับปรุง IT Best Practices ให้มีความทันสมัยต่อรูปแบบบริการทางการเงินใหม่ ๆ การเปลี่ยนแปลงของเทคโนโลยี และการทุจริตผ่านทางธนาคารอิเล็กทรอนิกส์ที่มีการพัฒนาอย่างรวดเร็วด้วยเช่นกัน

สรุปกระบวนการในการจัดทำแนวปฏิบัติที่ดี(IT Best Practices)

1. **การกำหนดขอบเขตการจัดทำแนวปฏิบัติที่ดี**

   ครอบคลุมการทำธุรกรรมฝาก ถอน และโอนเงิน ผ่านช่องทาง สาขา ATM และ Internet Banking ซึ่ง ธปท. ได้ว่าจ้างบริษัท Deloitte ทำหน้าที่ให้คำปรึกษาแก่ ธปท. ในทุกกระบวนการจัดทำแนวปฏิบัติที่ดี ฉบับนี้

2. **การเตรียมความพร้อมผู้ตรวจสอบ ธปท.**

   เตรียมความพร้อมผู้ตรวจสอบ ธปท. ให้เข้าใจแนวทางการรวบรวมข้อมูล การจัดทำ Business Process Flows IT Process Flows การระบุความเสี่ยง และแนวปฏิบัติที่ดี

3. **การรวบรวมข้อมูล เพื่อจัดทำแนวปฏิบัติที่ดี**

   ศึกษาและรวบรวมข้อมูลกระบวนการทางธุรกิจที่เกี่ยวข้องกับการทำธุรกรรมฝาก ถอน และโอนเงิน และโครงสร้างระบบ IT ที่เกี่ยวข้องกับการทำธุรกรรมดังกล่าวในลักษณะ End-to-End Process ของ ธพ. ไทย ทุกแห่ง

4. **การยกร่างแนวปฏิบัติที่ดี**

   การยกร่างแนวปฏิบัติที่ดีจัดทำโดยคณะทำงานภายใน ธปท. ประกอบด้วย ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ ฝ่ายตรวจสอบ 1 ฝ่ายตรวจสอบ 2 และฝ่ายเทคโนโลยีสารสนเทศ โดยมีการดำเนินงาน ดังนี้

   4.1 นำข้อมูลที่รวบรวมได้ในข้อ 3 มาประมวลผล และวิเคราะห์ เพื่อจัดทำ

   4.1.1 Business Process Flows และ IT Process Flows ที่เป็น Benchmark ของระบบ ธพ. ไทย

   4.1.2 ตารางระบุความเสี่ยงอ้างอิงประเภทความเสี่ยงด้านปฏิบัติการตามมาตรฐาน Basel II และร่างแนวปฏิบัติที่ดี ที่ควบคุมความเสี่ยง อ้างอิงตามกรอบมาตรฐานสากลเกี่ยวกับการควบคุมภายใน โดยแยกได้เป็น

   ด้าน Business Process อ้างอิงมาตรฐานดังนี้

   (1) มาตรฐานของ The Committee of Sponsoring Organizations of the Treadway Commission (COSO) ซึ่งเป็นคณะกรรมการที่จัดทำแนวปฏิบัติด้านการบริหารความเสี่ยงองค์กร (Enterprise Risk Management : ERM) การควบคุมภายใน และการป้องกันทุจริต ที่ได้รับการยอมรับในระดับสากล

   (2) Global Technology Audit Guide (GTAG) ซึ่งเป็นกรอบแนวทางการตรวจสอบเทคโนโลยีสารสนเทศของหน่วยงาน Institute of Internal Auditors (IIA) ซึ่งเป็นองค์กรวิชาชีพการตรวจสอบภายในซึ่งมีสมาชิกทั่วโลก

   ด้าน IT Process อ้างอิงมาตรฐานดังนี้

   (1) Control Objectives for Information and Related Technology (COBIT) หรือกรอบการบริหารจัดการด้านเทคโนโลยีสารสนเทศของหน่วยงาน The Information

Systems Audit and Control Association (ISACA) ซึ่งเป็นองค์กรระดับสากลที่มุ่งพัฒนาความรู้ และการปฏิบัติงานที่ดีด้านเทคโนโลยีสารสนเทศ

(2) ISO27001 (Information Security) ซึ่งเป็นกรอบการควบคุมด้านความปลอดภัยเทคโนโลยีสารสนเทศของหน่วยงาน International Organization for Standardization (ISO) หรือองค์กรมาตรฐานสากลซึ่งเป็นองค์กรระหว่างประเทศ ทำหน้าที่กำหนดมาตรฐานสากลต่างๆ ที่เกี่ยวข้องกับธุรกิจ และอุตสาหกรรม รวมทั้งมาตรฐานด้านเทคโนโลยีสารสนเทศด้วย

(3) มาตรฐานการตรวจสอบด้านเทคโนโลยีสารสนเทศของ Federal Financial Institutions Examination Council (FFIEC) ซึ่งเป็นองค์กรที่ออกมาตรฐานการตรวจสอบ เพื่อกำกับดูแลสถาบันการเงินในสหรัฐฯ

4.2 รับฟังความคิดเห็นต่อร่างแนวปฏิบัติที่ดีจาก ธพ. ไทย ทุกแห่ง พบว่า ธพ. ไทยทุกแห่งเห็นด้วยสูงถึงร้อยละ 94 ของข้อปฏิบัติของ IT Best Practices ทั้งหมด ส่วนที่เหลืออีกร้อยละ 6 มีข้อห่วงใยในบางเรื่องที่ต้องใช้เงินลงทุนสูง หรือมีทางเลือกอื่นช่วยชดเชยได้ (Manual Control) ซึ่ง ธปท. ได้ร่วมกับที่ปรึกษาได้ปรับปรุงให้มีความยืดหยุ่นมากขึ้นแล้ว

5. การ Finalize แนวปฏิบัติที่ดีฉบับนี้

ธปท. ได้ปรับปรุงร่างแนวปฏิบัติที่ดีตามความเห็นที่ได้รับจาก ธพ. เพื่อให้มีความชัดเจน ยืดหยุ่น สามารถนำไปปฏิบัติจริง และสอดคล้องกับมาตรฐานสากล โดยบริษัท Deloitte ได้สรุปความเห็นว่า แนวปฏิบัติที่ดีฉบับนี้ มีมาตรฐานสอดคล้องกับมาตรฐานสากล และ/หรือมาตรฐานของธนาคารชั้นนำในกลุ่มประเทศอาเซียน

ส่วนที่ 1

แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยง

ของกระบวนการทำธุรกิจหลัก

Phase 1: ธุรกรรมฝาก ถอน และโอนเงิน

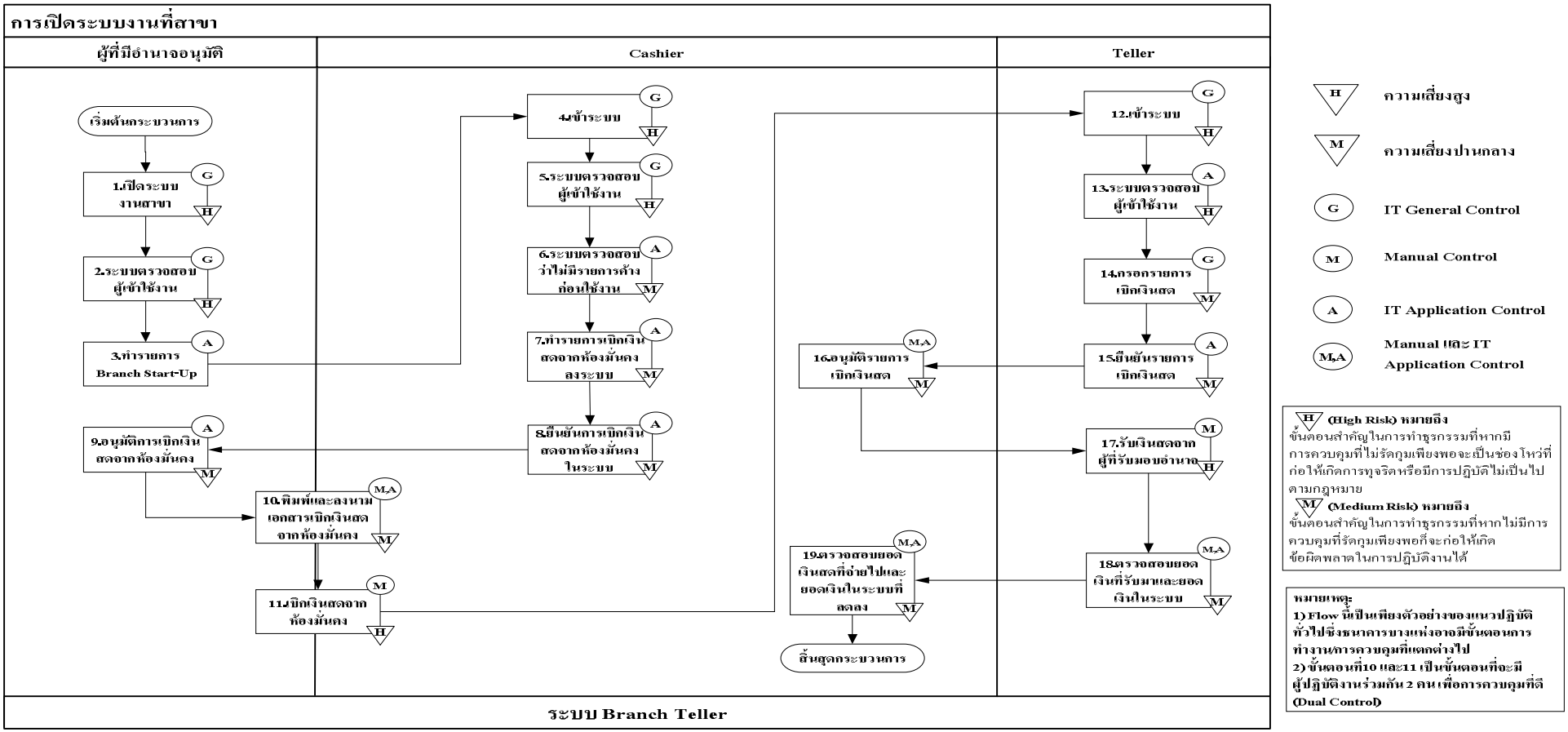
ตารางการระบุความเสี่ยงสำหรับกระบวนการทำธุรกิจหลัก (Business Process)

Risks	การเปิด/ปิด ระบบงานที่สาขา	การเปิดบัญชี เงินฝาก	การฝาก/ถอน/ โอนเงิน
การฉ้อโกงโดยบุคคลภายใน (Internal Fraud) เช่น - การทำธุรกรรมโดยไม่ได้รับอนุญาต - การปลอมแปลงต่าง ๆ - การบันทึกธุรกรรมไม่ถูกต้อง - การลักลอบใช้บัญชีของผู้อื่น การปลอมเป็นบุคคลอื่น	✓	✓	✓
การฉ้อโกงโดยบุคคลภายนอก (External Fraud) เช่น - การปลอมแปลงเป็นบุคคลอื่น - การโจรกรรมหรือการยักยอกทรัพย์ - การใช้ธนบัตรปลอม		✓	✓
ความเสียหายจากการปฏิบัติการ การส่งมอบ และการจัดกระบวนการ (Execution Delivery and Process Management) เช่น - ความผิดพลาดในการนำข้อมูลเข้าสู่ระบบการเก็บรักษา หรือการดึงข้อมูล - การปฏิบัติงานผิดพลาด (Human Error)	✓	✓	✓

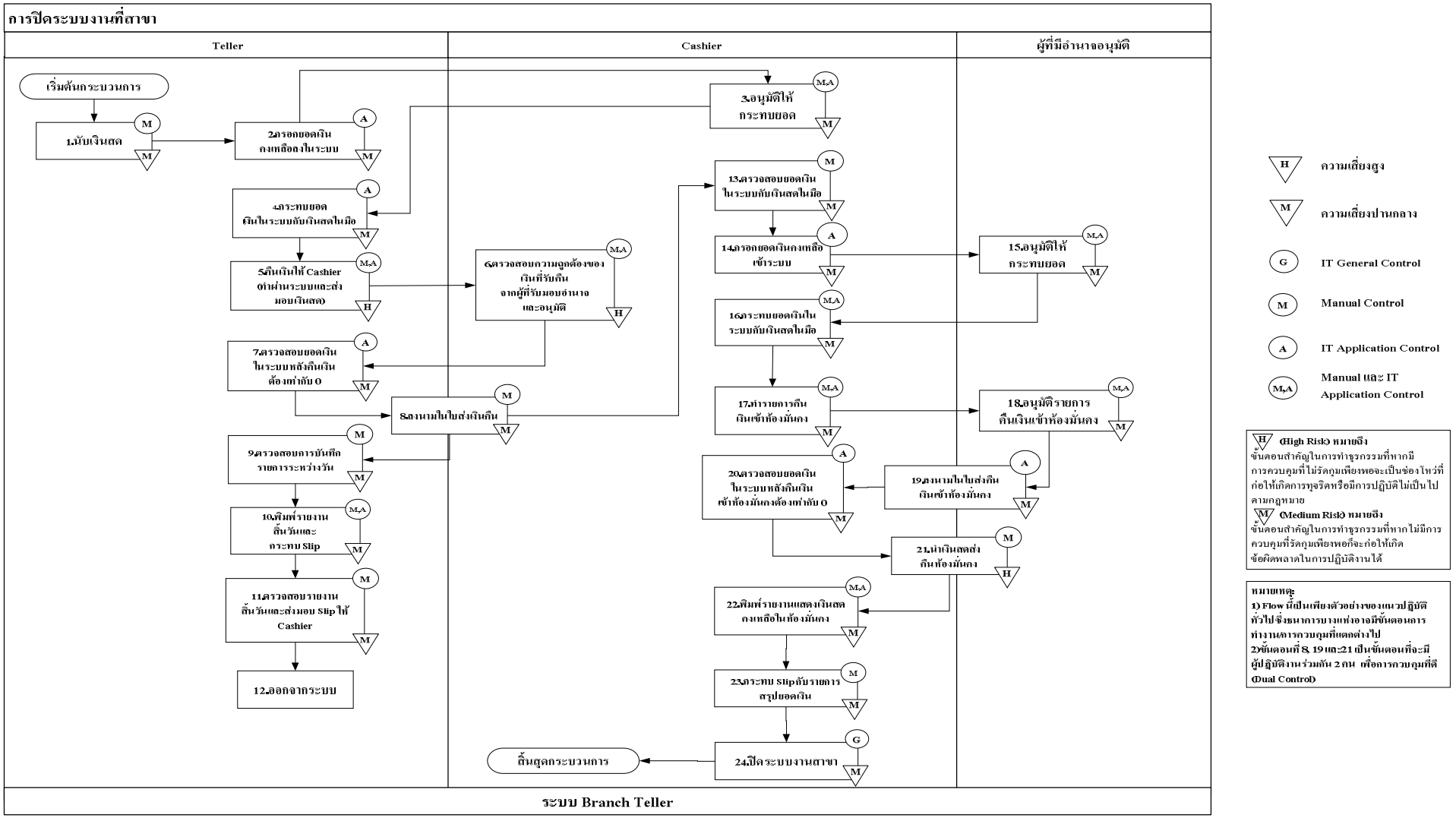
1.1 การเปิด/ปิดระบบงานที่สาขา

<u>ตัวอย่าง Flowchart กระบวนการทำงาน</u>

การเปิดระบบงานที่สาขา



การปิดระบบงานที่สาขา



ตารางการควบคุมที่สำคัญ

การเปิด/ปิดระบบงานที่สาขา	
วัตถุประสงค์ เพื่อให้การดำเนินงานของธนาคารเกี่ยวกับการเปิด/ปิดระบบงานที่สาขากระทำโดยเจ้าหน้าที่ที่รับมอบอำนาจ การปฏิบัติงานของสาขาในการให้บริการลูกค้ามีความปลอดภัยตามหลักมาตรฐานสากล มีความถูกต้องเชื่อถือได้ และสามารถให้บริการได้อย่างต่อเนื่อง	
ขั้นตอน	**แนวปฏิบัติที่ดี**
การเปิด/ปิดระบบ	มีระบบการควบคุมเอกสารสำคัญเกี่ยวกับบัญชีเงินฝาก เช่น
	- ยอดสมุดคู่ฝากคงเหลือ
	- ยอดบัตรอิเล็กทรอนิกส์คงเหลือ
	- Post Date Cheque ที่ครบกำหนดฝาก
	- อื่น ๆ
	ก่อนการปิดระบบจะต้องจัดการเรื่องดังต่อไปนี้ ให้แล้วเสร็จก่อน (หากไม่แล้วเสร็จระบบจะไม่อนุญาตให้ปิดระบบ)
	- จัดการให้ยอดเงินคงเหลือในระบบของผู้รักษาเงิน และผู้รับจ่ายเงินเท่ากับศูนย์
	- จัดการกรณีที่มีค่าความแตกต่างระหว่างระบบสาขาและระบบ Core Banking
	- ทำรายการส่งเงินสดทั้งหมดเข้าห้องมั่นคง
	- การกระทบ Slip ทั้งหมดกับยอดรวมที่บันทึกในระบบ
	มีการกำหนดสิทธิ์การเปิด/ปิดเครื่องแม่ข่ายสาขาแก่ผู้ที่มีอำนาจอนุมัติเท่านั้น
	มีการตั้งค่าระบบให้มีการแจ้งเตือนสถานะการส่งรายการบันทึกบัญชีจากสาขาไปสำนักงานใหญ่ทั้งในกรณีสำเร็จและไม่สำเร็จ
การทำรายการเบิกเงินสด	มีการกำหนดสิทธิ์เฉพาะ Teller ประจำสาขา ให้เบิกเงินสดจาก Cashier ได้เท่านั้น
	มีการกำหนดให้การเบิกเงินสดทำผ่านระบบเท่านั้น
	มีการตั้งค่าระบบให้แสดงยอดเงินสดคงเหลือของสาขา ซึ่งสามารถเรียกดูได้โดย Cashier และ/หรือ ผู้บริหารสาขา
	มีการตั้งค่าระบบให้แสดงยอดเงินสดคงเหลือของเครื่อง Teller
	มีการกำหนดสิทธิ์การเบิกเงินสดในระบบจากห้องมั่นคงแก่ Cashier เท่านั้น
การอนุมัติรายการเบิกเงินสด/การอนุมัติการคืนเงินสด	มีการตั้งค่าระบบบังคับให้มีการอนุมัติการทำรายการเบิก/คืนเงินสดก่อนที่ข้อมูลจะถูกบันทึกในระบบ (Teller เบิก/คืนเงินสดจาก Cashier และ Cashier เบิก/คืนเงินสดจากห้องมั่นคง)
	มีการพิสูจน์ตัวตนของผู้ที่มีอำนาจอนุมัติในระบบที่ปลอดภัย เช่น การใช้ Two-Factor Authentication หรือการสแกนลายนิ้วมือของผู้ที่มีอำนาจอนุมัติ
	มีการกำหนดสิทธิ์การอนุมัติการทำรายการในระบบให้แก่ผู้ที่มีอำนาจอนุมัติเท่านั้น
	มีการตั้งค่าระบบให้ปฏิเสธการทำรายการและอนุมัติรายการโดยใช้รหัสผู้ใช้งานเดียวกัน
	มีการแยกหน้าที่การทำงานระหว่าง Teller Cashier ผู้ที่มีอำนาจอนุมัติและผู้บริหารสาขาอย่างชัดเจน

ขั้นตอน	แนวปฏิบัติที่ดี
การจัดเก็บเงินสด	มีการจัดเก็บเงินสดไว้ในห้องมั่นคง และควบคุมการรับ - จ่ายโดยวิธี Dual Control โดยมีผู้บริหารสาขาหรือเทียบเท่าปฏิบัติงานร่วมกับ Cashier
การตรวจธนบัตรปลอม	มีเครื่องมือตรวจนับและตรวจสอบธนบัตรปลอม
การทำรายการคืนเงินสด	มีการตั้งค่าระบบให้ Teller ตรวจสอบการกระทบยอด ดังนี้
	- ยอดเงินสดของรายการที่เกิดขึ้นในระบบเปรียบเทียบกับยอดเงินสดที่นับได้ที่ Teller กรอกข้อมูล
	- ยอดเงินสดเกิน/เงินขาด
	มีการกำหนดให้การคืนเงินสดทำผ่านระบบเท่านั้น
	มีการตั้งค่าระบบให้แสดงยอดเงินสดคงเหลือของสาขา
	มีการตั้งค่าให้ Cashier จะทำการส่งเงินคืนเข้าห้องมั่นคงได้ ก็ต่อเมื่อ Teller ทุกคนทำรายการคืนเงินสด ณ สิ้นวันครบแล้วเท่านั้น
	มีการกำหนดสิทธิ์การคืนเงินสดในระบบ โดยแยกเป็น Teller คืนเงินให้ Cashier และ Cashier คืนเงินเข้าห้องมั่นคง
การเก็บหลักฐาน	มีการเก็บหลักฐานการเบิกเงินสด/ส่งเงินสดคืนห้องมั่นคงในระบบ และมีเอกสารที่มีการลงนามร่วมกันระหว่าง Cashier กับผู้บริหารสาขา
	มีการเก็บหลักฐานการเบิกเงินสด/คืนเงินสดระหว่าง Cashier และ Teller ในระบบ และมีเอกสารที่ลงนามร่วมกันระหว่าง Teller กับ Cashier

<u>หมายเหตุ</u>: 1) ผู้ที่มีอำนาจอนุมัติ หมายถึง เจ้าหน้าที่ที่รับมอบอำนาจจากธนาคาร และมีตำแหน่งสูงกว่า Teller

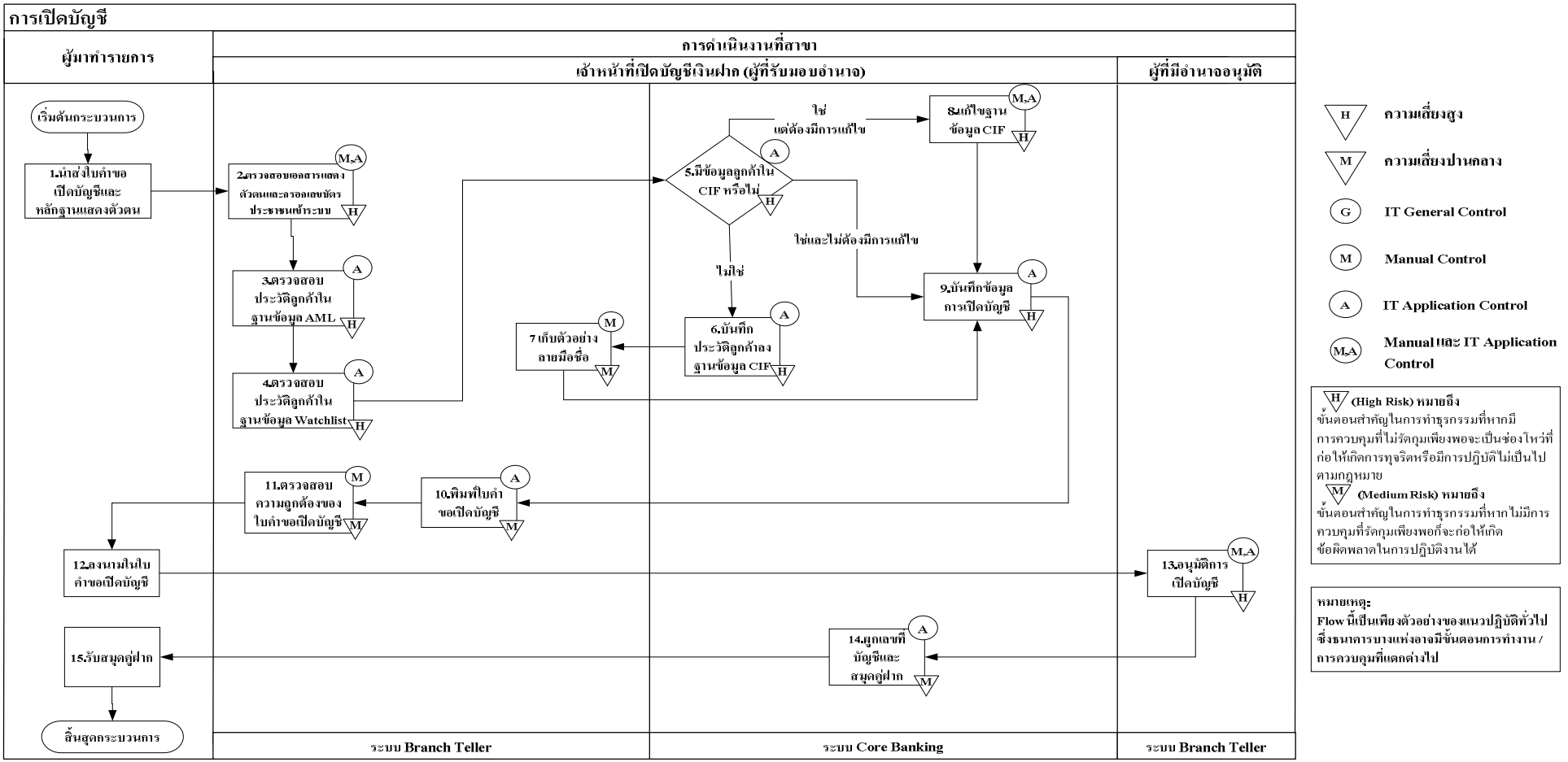
2) Two-Factor Authentication หมายถึง วิธีการพิสูจน์ตัวตนของผู้ทำรายการโดยใช้ข้อมูล 2 อย่าง ประกอบกัน ซึ่งข้อมูลดังกล่าวมี 3 ประเภท ได้แก่ 1) Something You Know เช่น User ID และ Password เป็นต้น 2) Something You Have เช่น บัตรอนุมัติรายการ เป็นต้น และ 3) Something You Are เช่น ลายนิ้วมือ เป็นต้น ตัวอย่างการใช้ Two-Factor Authentication เช่น การที่ผู้ที่มีอำนาจอนุมัติรูดบัตรอนุมัติรายการพร้อมการกรอก Password เพื่ออนุมัติรายการ เป็นต้น

<u>ข้อสังเกต</u>: แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน โดยโครงการใน Phase 2 ปี 2557 ธปท. จะศึกษาจัดทำแนวปฏิบัติที่ยอมรับได้ (Acceptable Practices) และประเมิน Gap ร่วมกับ ธพ. แต่ละแห่ง เพื่อเป็นแนวทางให้ ธปท. และ ธพ. ร่วมกันพิจารณาความเหมาะสมของการจัดทำแผนพัฒนาปรับปรุงระบบ IT ของตนเองให้ได้ตามมาตรฐานสากล ทั้งในระยะสั้นและระยะยาวต่อไป

1.2 การเปิดบัญชีเงินฝาก

<u>ตัวอย่าง Flowchart กระบวนการทำงาน</u>

การเปิดบัญชี



ตารางการควบคุมที่สำคัญ

การเปิดบัญชี	
วัตถุประสงค์ เพื่อให้การดำเนินงานของธนาคารเกี่ยวกับการเปิดบัญชีเงินฝากของลูกค้ากระทำโดยเจ้าหน้าที่ที่ได้รับมอบอำนาจ มีกระบวนการพิสูจน์ตัวตนของผู้เปิดบัญชีจากหลักฐานที่เชื่อถือได้ตามหลักมาตรฐานสากล มีการป้องกันการทุจริตจากการเปิดบัญชี และมีการควบคุมเพื่อป้องกันความผิดพลาดจากการปฏิบัติงาน	
ขั้นตอน	**แนวปฏิบัติที่ดี**
การพิสูจน์ตัวตนของเจ้าของบัญชี	**การตรวจสอบเอกสารแสดงตัวตน และข้อมูลในเอกสารแสดงตัวตนที่ลูกค้านำมาเปิดบัญชีเพื่อให้แน่ใจว่าเอกสารมีความถูกต้อง และระบุตัวตนลูกค้าได้อย่างถูกต้องตามความเป็นจริง**
	มีการตั้งค่าระบบให้ตรวจสอบจากบัตรประชาชนที่เป็นบัตรอิเล็กทรอนิกส์ (ในกรณีที่ลูกค้ามีบัตรประชาชนแบบอิเล็กทรอนิกส์เท่านั้น)
	มีการตรวจสอบเอกสารเพิ่มเติมกรณีนำบัตรประชาชนที่ไม่เป็นอิเล็กทรอนิกส์มาพิสูจน์ตัวตนเพื่อเปิดบัญชี เช่น บัตรข้าราชการ บัตรพนักงานรัฐวิสาหกิจ บัตรพนักงานองค์การของรัฐ ใบอนุญาตขับรถ กรณีเป็นลูกค้าเดิมให้ตรวจสอบสมุดคู่ฝาก ลายมือชื่อและรูปถ่ายในระบบฐานข้อมูลของธนาคาร
	การตรวจสอบฐานข้อมูลต่าง ๆ ก่อนการเปิดบัญชี เพื่อให้เป็นไปตามข้อกฎหมายที่กำหนด
	มีการตั้งค่าระบบให้ตรวจสอบฐานข้อมูล AML โดยอัตโนมัติ
	มีการตั้งค่าระบบให้ตรวจสอบฐานข้อมูล Watchlist โดยอัตโนมัติ
	การปฏิเสธการเปิดบัญชี
	มีการตั้งค่าระบบให้ปฏิเสธการทำรายการให้กับผู้ที่ถูกขึ้นบัญชีเป็นผู้ก่อการร้าย หรือผู้ต้องห้ามตามกฎหมาย
	การควบคุมอื่นๆที่เกี่ยวข้องกับการพิสูจน์ตัวตน
	มีการตั้งค่าระบบให้จัดทำ KYC จากข้อมูลที่ได้จากลูกค้า เพื่อจัดระดับความเสี่ยงของลูกค้าโดยอัตโนมัติ
การทำรายการ	มีการกำหนดสิทธิ์การทำรายการเปิดบัญชีในระบบให้แก่เจ้าหน้าที่เปิดบัญชี (ผู้ที่รับมอบอำนาจ) เท่านั้น
	ความถูกต้องและครบถ้วนของข้อมูลที่ Input
	มีการตั้งค่าระบบให้ดึงข้อมูลที่ใช้เปิดบัญชีจากบัตรอิเล็กทรอนิกส์ที่ออกโดยราชการเป็นฐานข้อมูลในการทำรายการ
	มีการตั้งค่าระบบให้บังคับกรอกข้อมูลสำคัญให้ครบถ้วน
	มีการตั้งค่าระบบให้ตรวจสอบความถูกต้องของข้อมูลที่กรอก
	ระบบ Generate เลขที่บัญชีที่เปิดใหม่ให้โดยอัตโนมัติ
	การเก็บตัวอย่างลายมือชื่อ
	มีการเก็บข้อมูลลายมือชื่อในรูปแบบอิเล็กทรอนิกส์ เพื่อลดความเสี่ยงการปลอมแปลงลายมือชื่อ

ขั้นตอน	แนวปฏิบัติที่ดี
	มีการจำกัดการเข้าถึงข้อมูลลายมือชื่อโดยผู้ที่รับมอบอำนาจเท่านั้น
	การเก็บเอกสารคำขอเปิดบัญชี
	มีการเก็บคำขอเปิดบัญชีในรูปแบบอิเล็กทรอนิกส์และจำกัดการเข้าถึงข้อมูลโดยผู้ที่รับมอบอำนาจเท่านั้น เพื่อลดความเสี่ยงการปลอมแปลงลายมือชื่อ
	มีขั้นตอนให้ลูกค้าตรวจสอบความถูกต้องและลงนามเอกสารคำขอเปิดบัญชี
	การผูกเลขที่บัญชีกับสมุดคู่ฝาก
	มีการตั้งค่าระบบให้ปฏิเสธทุกครั้งที่มีการผูกบัญชีกับสมุดคู่ฝากผิดประเภท เช่น เปิดบัญชีออมทรัพย์ แต่ใช้สมุดบัญชีฝากประจำ
	มีการตั้งค่าระบบให้ปฏิเสธทุกครั้งที่มีการผูกบัญชีกับสมุดคู่ฝากที่ไม่มีในทะเบียนสมุดคู่ฝากของสาขาที่ทำการเปิดบัญชีเงินฝาก
	มีการผูกเลขที่บัญชีและสมุดคู่ฝากโดยการใช้เครื่องมือช่วยในการ Input เลขที่บัญชี เช่น การใช้แถบแม่เหล็กหลังสมุดคู่ฝาก
การอนุมัติรายการ	มีการตั้งค่าระบบบังคับให้มีการอนุมัติการทำรายการก่อนที่รายการเปิดบัญชีจะถูกบันทึกในระบบ
	มีการพิสูจน์ตัวตนของผู้ที่มีอำนาจอนุมัติในระบบที่ปลอดภัย เช่น การใช้ Two-Factor Authentication หรือการสแกนลายนิ้วมือของผู้มีอำนาจอนุมัติ
	ระบบกำหนดสิทธิ์การอนุมัติการทำรายการให้กับผู้ที่มีอำนาจอนุมัติเท่านั้น
	ระบบปฏิเสธการทำรายการและอนุมัติรายการโดยใช้รหัสผู้ใช้งานเดียวกัน
	มีการตรวจสอบความถูกต้อง และความครบถ้วนของการทำรายการทุก ๆ สิ้นวันโดยผู้ที่มีอำนาจอนุมัติ (ไม่เป็นคนเดียวกับผู้เปิดบัญชี และผู้อนุมัติการเปิดบัญชี)
การตรวจสอบความถูกต้องและครบถ้วนก่อนให้หลักฐานแก่ผู้มาทำรายการ	มีการตรวจสอบความถูกต้องก่อนให้หลักฐานแก่ผู้มาทำรายการ และความครบถ้วนของการจ่ายสมุดคู่ฝากทุก ๆ สิ้นวันโดย ผู้ที่มีอำนาจอนุมัติ
	สมุดคู่ฝากมีข้อความแสดงประเภทของบัญชี เลขที่บัญชี ชื่อบัญชี ชื่อสาขา ให้เจ้าของบัญชีรับทราบอย่างชัดเจน
	มีขั้นตอนให้ลูกค้าลงนามในการรับสมุดคู่ฝาก
การแก้ไขรายการเปิดบัญชี	มีการตั้งค่าระบบให้บังคับให้มีการอนุมัติการแก้ไขรายการ ก่อนข้อมูลถูกบันทึกในระบบ
	มีการพิสูจน์ตัวตนของผู้ที่มีอำนาจอนุมัติในระบบที่ปลอดภัย เช่น การใช้ Two-Factor Authentication หรือการสแกนลายนิ้วมือของผู้มีอำนาจอนุมัติ
	มีการกำหนดสิทธิ์การอนุมัติการทำรายการในระบบให้แก่ผู้ที่มีอำนาจอนุมัติเท่านั้น
	มีการตั้งค่าระบบให้ปฏิเสธการทำรายการและอนุมัติรายการโดยใช้รหัสผู้ใช้งานเดียวกัน
	การแก้ไขต้องทำโดยความเห็นชอบพร้อมกันของผู้ทำรายการ ผู้ที่มีอำนาจอนุมัติ และเจ้าของบัญชี
	มีการตรวจสอบความถูกต้อง และความครบถ้วนของการทำรายการทุก ๆ สิ้นวันโดยผู้ที่มีอำนาจอนุมัติ

ขั้นตอน	แนวปฏิบัติที่ดี
การแก้ไขฐานข้อมูล CIF กรณีเคยเป็นลูกค้าธนาคารแล้วมาเปิดบัญชีใหม่	ถ้าข้อมูลลูกค้าไม่ตรงกับฐานข้อมูลเดิมของธนาคาร ให้ผู้ที่รับมอบอำนาจระมัดระวังในการตรวจสอบข้อมูลสำคัญ เช่น ที่อยู่ หมายเลขโทรศัพท์ และหากลูกค้าต้องการแก้ไข มีการตั้งค่าระบบให้อนุมัติรายการแก้ไขข้อมูลลูกค้าโดยผู้ที่มีอำนาจอนุมัติ

<u>หมายเหตุ</u>: 1) ผู้ที่มีอำนาจอนุมัติ หมายถึง เจ้าหน้าที่ที่รับมอบอำนาจจากธนาคาร และมีตำแหน่งสูงกว่า เจ้าหน้าที่เปิดบัญชีเงินฝาก

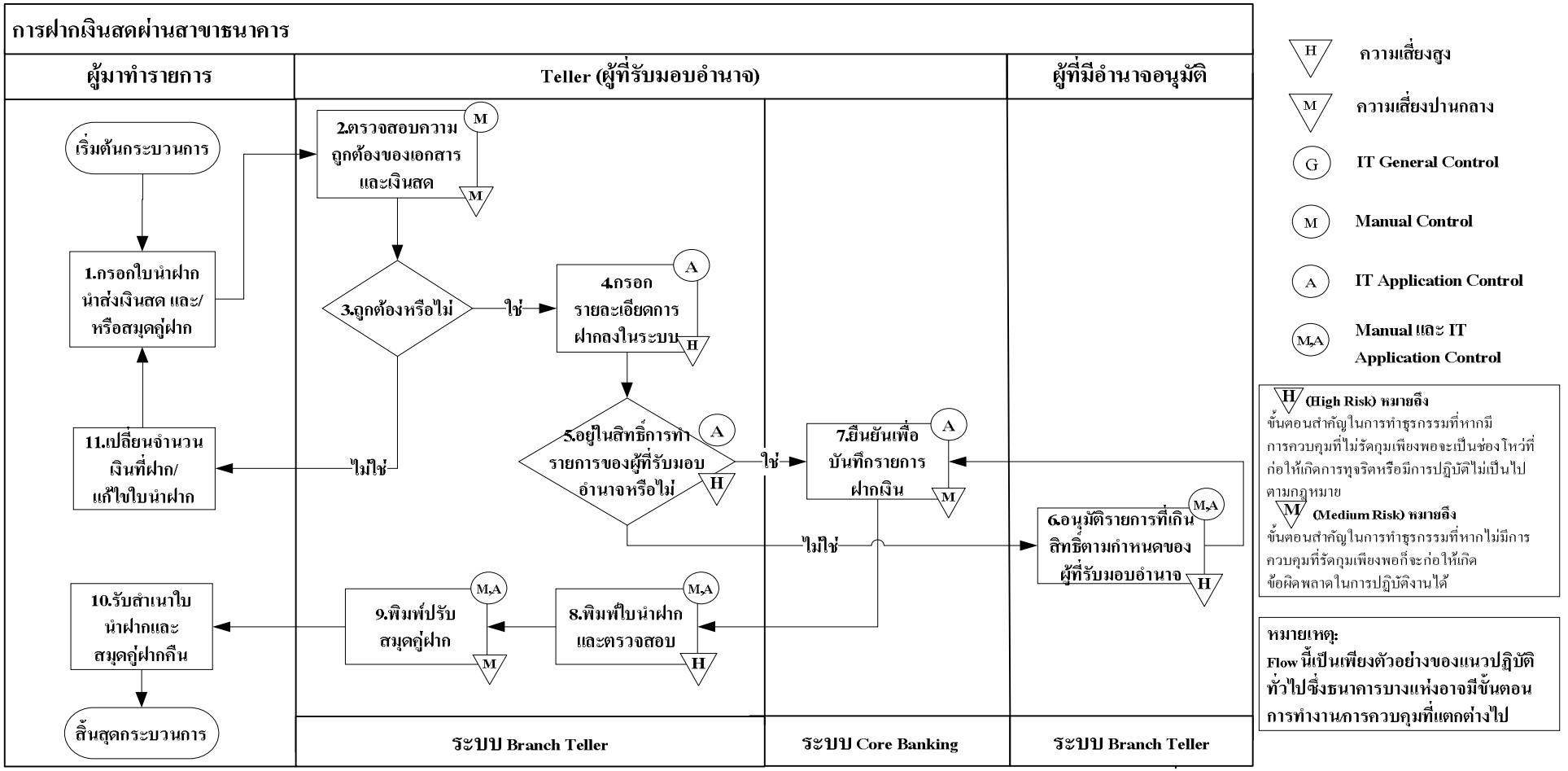
2) Two-Factor Authentication หมายถึง วิธีการพิสูจน์ตัวตนของผู้ทำรายการโดยใช้ข้อมูล 2 อย่าง ประกอบกัน ซึ่งข้อมูลดังกล่าวมี 3 ประเภท ได้แก่ 1) Something You Know เช่น User ID และ Password เป็นต้น 2) Something You Have เช่น บัตรอนุมัติรายการ เป็นต้น และ 3) Something You Are เช่น ลายนิ้วมือ เป็นต้น ตัวอย่างการใช้ Two-Factor Authentication เช่น การที่ผู้ที่มีอำนาจอนุมัติรูดบัตรอนุมัติรายการพร้อมการกรอก Password เพื่ออนุมัติรายการ เป็นต้น

<u>ข้อสังเกต</u>: แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน โดยโครงการใน Phase 2 ปี 2557 ธปท. จะศึกษาจัดทำแนวปฏิบัติที่ยอมรับได้ (Acceptable Practices) และประเมิน Gap ร่วมกับ ธพ. แต่ละแห่ง เพื่อเป็นแนวทางให้ ธปท. และ ธพ. ร่วมกันพิจารณาความเหมาะสมของการจัดทำแผนพัฒนาปรับปรุงระบบ IT ของตนเองให้ได้ตามมาตรฐานสากล ทั้งในระยะสั้นและระยะยาวต่อไป

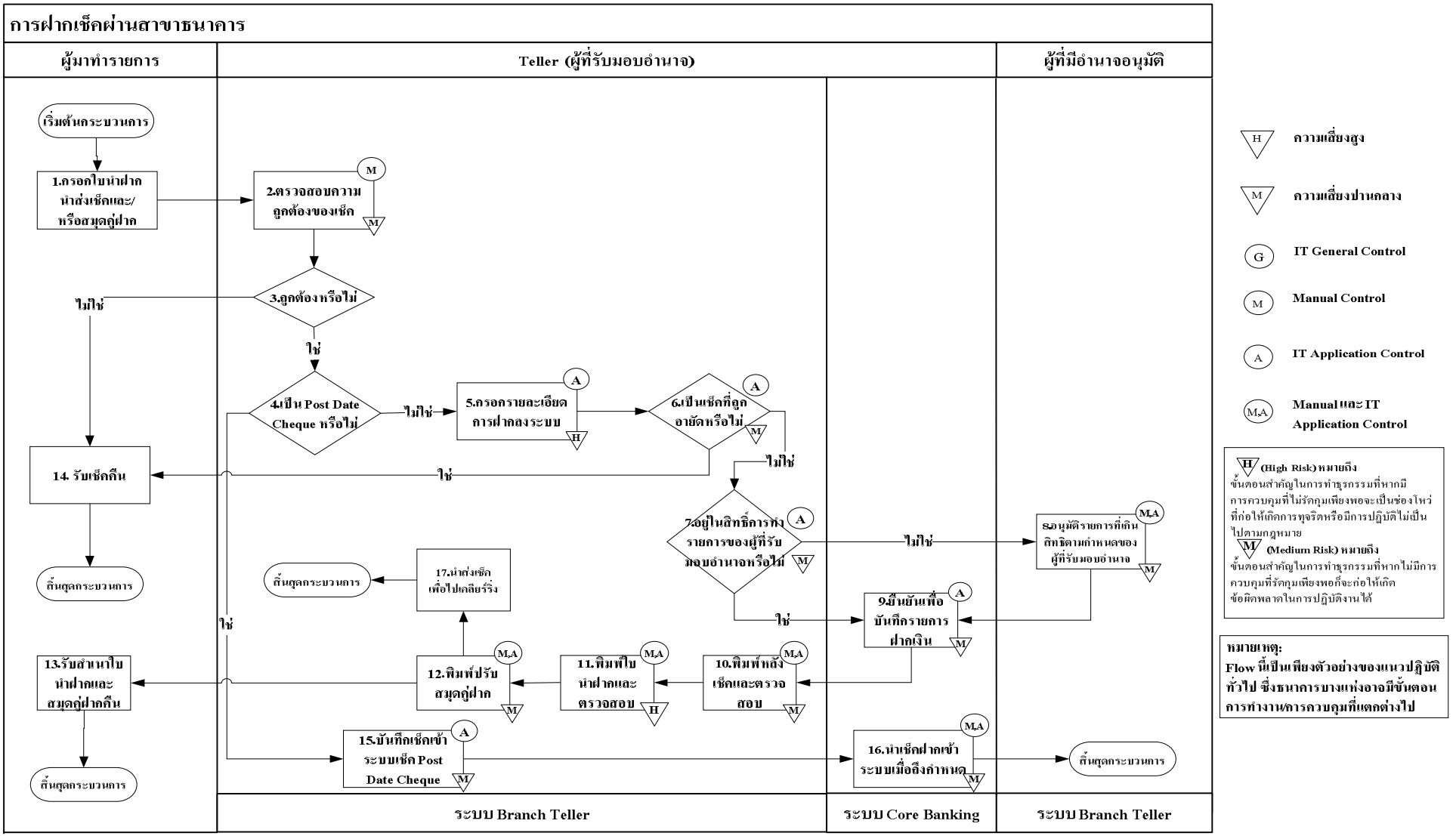
1.3 การฝาก การถอน และการโอนเงิน

<u>ตัวอย่าง Flowchart กระบวนการทำงาน</u>

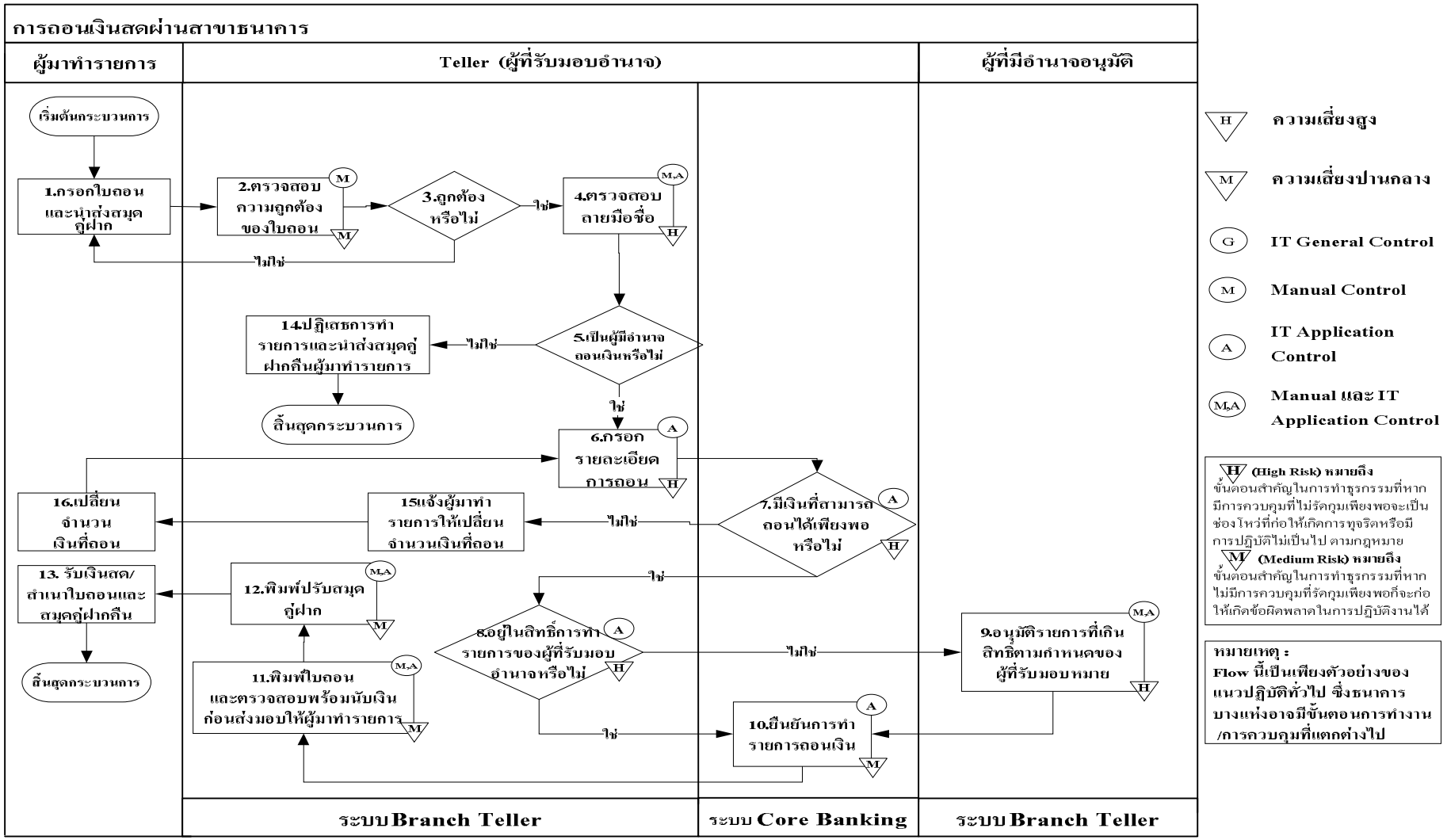
การฝากเงินสด



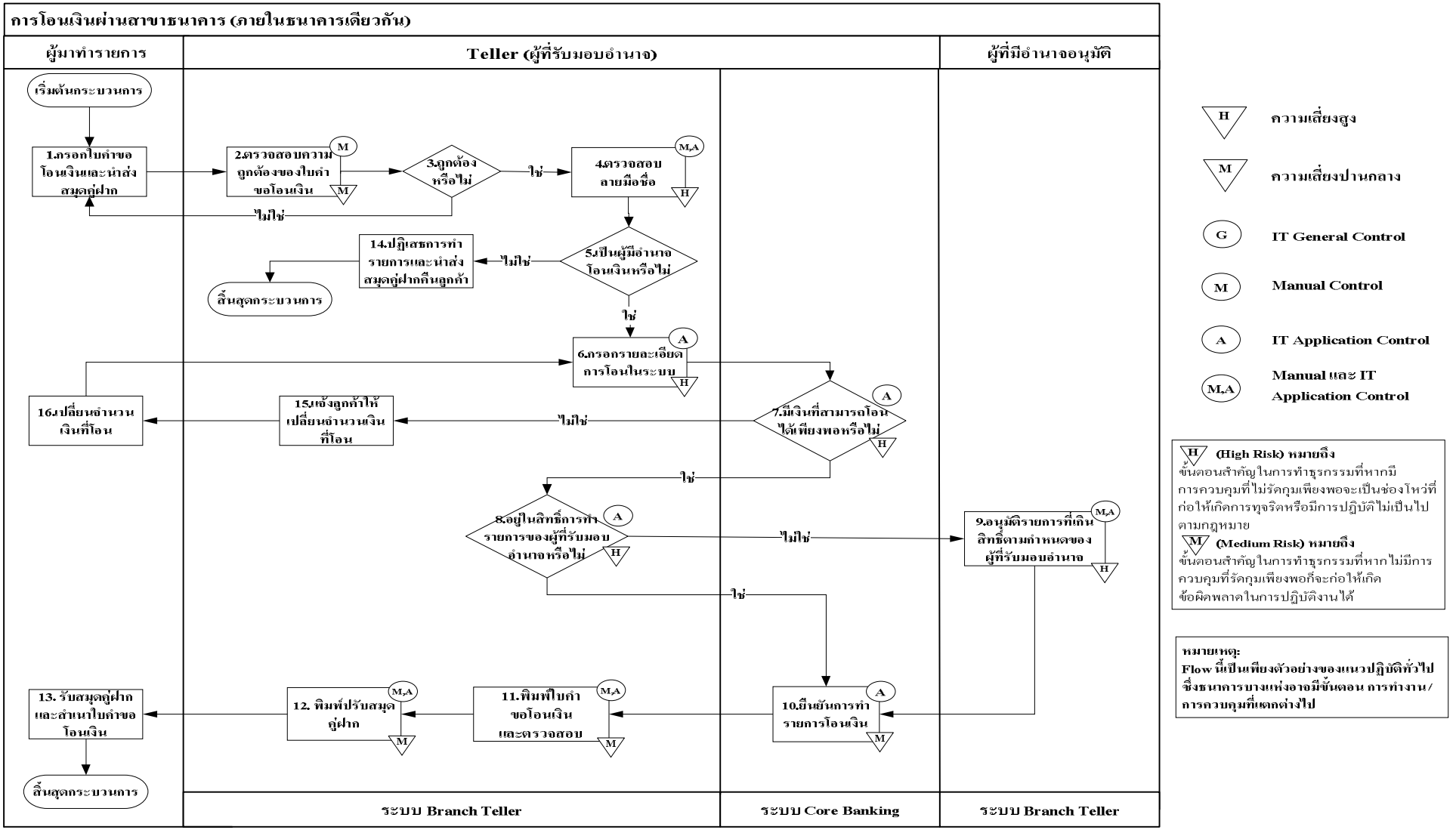
การฝากเช็ค


การฝากเช็คผ่านสาขาธนาคาร
ผู้มาทำรายการ
Teller (ผู้ที่รับมอบอำนาจ)
ผู้ที่มีอำนาจอนุมัติ
เริ่มต้นกระบวนการ
1.กรอกใบนำฝาก นำส่งเช็คและ/หรือสมุดคู่ฝาก
2.ตรวจสอบความถูกต้องของเช็ค
3.ถูกต้องหรือไม่
ไม่ใช่
ใช่
4.เป็น Post Date Cheque หรือไม่
ไม่ใช่
5.กรอกรายละเอียดการฝากลงระบบ
6.เป็นเช็คที่ลูกอาชัดหรือไม่
ไม่ใช่
ใช่
14. รับเช็คคืน
สิ้นสุดกระบวนการ
7.อยู่ในสิทธิ์การทำรายการของผู้ที่รับมอบอำนาจหรือไม่
ไม่ใช่
8.อนุมัติรายการที่เกินสิทธิ์ตามกำหนดของผู้ที่รับมอบอำนาจ
ใช่
9.ยืนยันเพื่อบันทึกรายการฝากเงิน
17.นำส่งเช็คเพื่อไปเคลียร์ริ่ง
สิ้นสุดกระบวนการ
13.รับสำเนาใบนำฝากและสมุดคู่ฝากคืน
สิ้นสุดกระบวนการ
12.พิมพ์ปรับสมุดคู่ฝาก
11.พิมพ์ใบนำฝากและตรวจสอบ
10.พิมพ์หลังเช็คและตรวจสอบ
15.บันทึกเช็คเข้าระบบเช็ค Post Date Cheque
16.นำเช็คฝากเข้าระบบเมื่อถึงกำหนด
สิ้นสุดกระบวนการ
ระบบ Branch Teller
ระบบ Core Banking
ระบบ Branch Teller
H ความเสี่ยงสูง
M ความเสี่ยงปานกลาง
G IT General Control
M Manual Control
A IT Application Control
M,A Manual และ IT Application Control
H (High Risk) หมายถึง ขั้นตอนสำคัญในการทำธุรกรรมที่หากมีการควบคุมที่ไม่รัดกุมเพียงพอจะเป็นช่องโหว่ที่ก่อให้เกิดการทุจริตหรือมีการปฏิบัติไม่เป็นไปตามกฎหมาย
M (Medium Risk) หมายถึง ขั้นตอนสำคัญในการทำธุรกรรมที่หากไม่มีการควบคุมที่รัดกุมเพียงพอก็จะก่อให้เกิดข้อผิดพลาดในการปฏิบัติงานได้
หมายเหตุ: Flow นี้เป็นเพียงตัวอย่างของแนวปฏิบัติทั่วไป ซึ่งธนาคารบางแห่งอาจมีขั้นตอนการทำงาน/การควบคุมที่แตกต่างไป

การถอนเงินสด



การโอนเงินผ่านสาขา



ตารางการควบคุมที่สำคัญ

การฝาก การถอน และการโอนเงิน	
วัตถุประสงค์ เพื่อให้การดำเนินงานของธนาคารเกี่ยวกับการทำธุรกรรมของลูกค้าจากการฝาก/ถอน/โอนเงิน กระทำโดยเจ้าหน้าที่ที่ได้รับมอบอำนาจ มีกระบวนการปฏิบัติงานที่ถูกต้องตามหลักมาตรฐานสากล และเป็นไปตามกฎหมายที่เกี่ยวข้อง	
ขั้นตอน	**แนวปฏิบัติที่ดี**
การตรวจสอบความถูกต้อง ครบถ้วนของสิ่งที่รับฝาก/นำส่งให้ลูกค้า	มีเครื่องมือตรวจนับความครบถ้วนของธนบัตรที่ฝาก/ธนบัตรที่จะส่งมอบให้ลูกค้า
	มีเครื่องมือตรวจนับและตรวจสอบธนบัตรปลอม
	มีการตรวจสอบความสมบูรณ์และถูกต้องของเช็คโดย Teller (ผู้ที่รับมอบอำนาจ) **(เฉพาะกรณีฝากเงิน)**
การพิสูจน์ตัวตนของเจ้าของบัญชี	**การตรวจสอบเอกสารเจ้าของบัญชีให้เป็นไปตามมาตรฐานสากล และกฎหมายที่เกี่ยวข้อง เช่น พรบ. ป้องกันและปราบปรามการฟอกเงิน**
	มีการตั้งค่าระบบให้ตรวจสอบจากบัตรประชาชนที่เป็นบัตรอิเล็คทรอนิกส์ (กรณีที่ลูกค้ามีบัตรประชาชนแบบอิเล็คทรอนิกส์เท่านั้น)
	มีการตรวจสอบเอกสารเพิ่มเติมกรณีนำบัตรประชาชนที่ไม่เป็นอิเล็กทรอนิกส์มาพิสูจน์ตัวตนเพื่อถอน/โอนเงิน เช่น บัตรข้าราชการ บัตรพนักงานรัฐวิสาหกิจ บัตรพนักงานองค์การของรัฐ ใบอนุญาตขับรถ กรณีเป็นลูกค้าเดิมให้ตรวจสอบสมุดคู่ฝาก ลายมือชื่อและรูปถ่ายในระบบฐานข้อมูลของธนาคาร
	มีการตรวจสอบสมุดคู่ฝาก (Passbook) ทุกครั้งกรณีที่เป็นผลิตภัณฑ์เงินฝากที่มีสมุดคู่ฝาก
	มีระบบงานที่รองรับการปฏิบัติงานตามที่กฎหมายกำหนด เช่น การรายงานธุรกรรมตาม พรบ. ป้องกันและปราบปรามการฟอกเงิน เป็นต้น
	การควบคุมเพิ่มเติมกรณีที่เจ้าของบัญชีไม่ได้มาทำรายการด้วยตนเอง
	ระบบกำหนดให้ผู้ที่มีอำนาจอนุมัติรายการต้องอนุมัติ รายการถอน/โอน ที่เจ้าของบัญชีไม่ได้มาทำรายการด้วยตนเอง
	มีการตรวจสอบหลักฐานพิสูจน์ตัวตนของผู้รับมอบฉันทะ ได้แก่ บัตรประชาชน และหนังสือมอบฉันทะ
	การตรวจสอบลายมือชื่อในฐานข้อมูลของธนาคาร
	ระบบมีการแสดงลายมือชื่อลูกค้าเจ้าของบัญชีโดยอัตโนมัติเมื่อ Input ข้อมูล เช่น เลขที่บัญชี (ต้องมีการเก็บลายมือชื่อเข้าระบบอิเล็คทรอนิกส์ในขั้นตอนการเปิดบัญชี)
	มีการตั้งค่าระบบให้บังคับให้มีการยืนยันการตรวจลายมือชื่อโดยผู้ที่รับมอบอำนาจ
การคิดค่าธรรมเนียม	มีการตั้งค่าระบบให้คิดค่าธรรมเนียมอัตโนมัติ
	มีระเบียบการแจ้งค่าธรรมเนียมให้ผู้ที่มาทำรายการทราบก่อนทำรายการ
การทำรายการ	**สิทธิ์การเข้าทำรายการของผู้ที่รับมอบอำนาจ**
	มีการกำหนดสิทธิ์การทำรายการในระบบให้แก่ผู้ที่รับมอบอำนาจประจำสาขาเท่านั้น
	ความถูกต้องและครบถ้วนของข้อมูลที่ Input
	มีการใช้เครื่องมือแทนการ Input ข้อมูลเลขที่บัญชี เช่น แถบแม่เหล็กหลังสมุดคู่ฝาก

ขั้นตอน	แนวปฏิบัติที่ดี
	มีการตั้งค่าระบบบังคับให้ Input ข้อมูลของบัญชีที่ทำรายการ เช่น ยอดคงค้างหลังสุดในสมุดคู่ฝาก เพื่อป้องกันการทำรายการถอน/โอนเงินโดยไม่มีสมุดคู่ฝาก
	กรณีใช้เช็คในการถอนเงิน มีการตั้งค่าระบบให้ปฏิเสธการนำเงินตามเช็คเข้าบัญชีเงินฝากสำหรับ 1) Post Date Cheque 2) Expired Cheque **(เฉพาะกรณีถอนเงิน)**
	มีการตั้งค่าระบบให้บังคับ Input ข้อมูลสำคัญให้ครบถ้วน (เช่น เลขที่บัญชี จำนวนเงินที่ต้องการฝาก/ถอน/โอน)
	มีการตั้งค่าระบบให้ตรวจสอบความถูกต้องของข้อมูลที่ Input (เช่น ตรวจ Check Digit จากเลขที่บัญชี แล้วแสดงชื่อบัญชี)
	มีการตั้งค่าระบบให้ปฏิเสธการทำรายการที่มีจำนวนเงินมากกว่าที่สามารถถอนหรือโอนได้ **(เฉพาะกรณีถอน/โอนเงิน)**
	มีการตรวจสอบความถูกต้องของข้อมูลที่พิมพ์จากระบบลงบนใบนำฝาก/ใบถอน/ใบคำขอโอนเงิน กับข้อมูลในใบนำฝาก/ใบถอน/ใบคำขอโอนเงินก่อนเสร็จสิ้นการทำรายการ
	การ Input อัตราดอกเบี้ยเงินฝาก (สำหรับลูกค้าที่ได้อัตราดอกเบี้ยพิเศษ) (เฉพาะกรณีฝากเงิน)
	มีการตั้งค่าระบบให้ปฏิเสธอัตราดอกเบี้ยที่เกินกว่าช่วงอัตราดอกเบี้ยที่กำหนด
	การทำรายการเกี่ยวกับเช็ค (เฉพาะกรณีฝากเงิน)
	มีระบบตรวจสอบ Post Date Cheque
	มีการตั้งค่าระบบให้ปฏิเสธ Expired Cheque
	มีระบบการจัดการ Post Date Cheque (เช่น บันทึก เรียกดูข้อมูล)
	มีการตั้งค่าระบบให้ปฏิเสธเช็คที่ถูกอายัด
	มีการตั้งค่าระบบให้แสดงเหตุผลในการปฏิเสธการนำเงินตามเช็คเข้าบัญชี
	การยืนยันการทำรายการ
	มีการตั้งค่าระบบให้ส่งข้อความแจ้งยืนยันการทำรายการให้แก่เจ้าของบัญชีในกรณีที่เป็นธุรกรรมที่มีความเสี่ยงสูง เช่น กรณีมอบฉันทะให้ถอน/โอนเงินจำนวนมาก เพื่อแจ้งเตือนและป้องกันความเสียหายที่อาจเกิดขึ้นอีก หากรายการดังกล่าวไม่ได้รับการมอบฉันทะจากเจ้าของบัญชี **(เฉพาะกรณีถอน/โอนเงิน)**
	มีการตั้งค่าระบบบังคับให้ผู้ที่รับมอบอำนาจยืนยันรายการก่อนบันทึกรายการในระบบ เช่น แสดงรายการให้ตรวจสอบอีกครั้งก่อนกด Confirm
	มีการตั้งค่าระบบให้มีการแจ้งเตือนสถานะของรายการทั้งในกรณีทำรายการสำเร็จและไม่สำเร็จ เช่น แสดงข้อความ "Success" เมื่อการทำรายการสำเร็จ
	ปริมาณเงินสดที่ผู้ที่รับมอบอำนาจสามารถเก็บรักษาได้
	มีการตั้งค่าระบบให้บังคับให้มีการอนุมัติการทำรายการต่อหรือปฏิเสธการทำรายการเมื่อจำนวนเงินสดที่เครื่องผู้ที่รับมอบอำนาจเกินกว่ากำหนด
การอนุมัติรายการ	มีการพิสูจน์ตัวตนของผู้ที่มีอำนาจอนุมัติในระบบที่ปลอดภัย เช่น การใช้ Two-Factor Authentication หรือการสแกนลายนิ้วมือของผู้มีอำนาจอนุมัติ

ขั้นตอน	แนวปฏิบัติที่ดี
	ระบบกำหนดสิทธิ์การอนุมัติการทำรายการให้กับผู้ที่มีอำนาจอนุมัติเท่านั้น
	ระบบปฏิเสธการทำรายการและอนุมัติรายการโดยใช้รหัสผู้ใช้งานเดียวกัน
	ระบบปฏิเสธรายการฝาก/ถอน/โอนเงินที่จำนวนเงินเกินกำหนดตามสิทธิ์ของผู้ที่รับมอบอำนาจ และการ Input อัตราดอกเบี้ยเงินฝากพิเศษโดยไม่ได้รับอนุมัติ (Teller ต้องขออนุมัติรายการจากผู้ที่มีอำนาจอนุมัติรายการก่อน จึงจะทำรายการได้)
	ระบบมีการจัดเก็บข้อมูลการอนุมัติรายการ
	ระบบปฏิเสธรายการถอน/โอนเงินจากบัญชีที่ไม่เคลื่อนไหวเป็นระยะเวลานาน (Dormant Account) ของผู้รับมอบอำนาจ (Teller ต้องขออนุมัติรายการจากผู้มีอำนาจอนุมัติรายการก่อนถึงจะทำรายการได้) **(เฉพาะกรณีถอน/โอนเงิน)**
การพิมพ์หลักฐานการทำรายการ	**ใบนำฝาก/ใบถอน/ใบคำขอโอนเงิน**
	มีข้อมูลที่ใช้เป็นหลักฐานในใบนำฝาก/ใบถอน/ใบคำขอโอนเงิน ดังนี้
	- วันและเวลาที่ทำรายการ
	- สถานที่ที่ทำรายการ
	- เลขที่บัญชีที่ทำรายการ
	- ชื่อบัญชี
	- ประเภทของรายการ
	- อัตราดอกเบี้ย (กรณีเงินฝากประจำ)
	- จำนวนเงินที่ทำรายการ
	- รหัสผู้ใช้งานของผู้ที่รับมอบอำนาจ
	- รหัสผู้ใช้งานของผู้ที่มีอำนาจอนุมัติ (ในกรณีที่มีการอนุมัติรายการ)
	จัดให้มีการให้หลักฐานการรับ Post Date Cheque แก่ผู้มาทำรายการ **(เฉพาะกรณีฝากเงิน)**
	รายละเอียดที่พิมพ์ลงในสมุดคู่ฝาก
	มีข้อมูลที่พิมพ์ในสมุดคู่ฝากดังนี้
	- วันที่ทำรายการ
	- ประเภทรายการ
	- อัตราดอกเบี้ย (กรณีเงินฝากประจำ)
	- จำนวนเงินที่ทำรายการ
	- ยอดคงเหลือ
	- รหัสใช้งานของผู้ที่รับมอบอำนาจ
	การพิมพ์ปรับสมุดคู่ฝาก
	มีการตั้งค่าระบบให้ปฏิเสธการปรับยอดเงินคงค้างกรณีสมุดคู่ฝากที่มีเลขที่บัญชีไม่สัมพันธ์กับเลขที่บัญชีที่ดำเนินรายการอยู่ (เช่น ระบบตรวจสอบกับข้อมูลเลขที่บัญชีในแถบแม่เหล็กหลังสมุดคู่ฝาก)
	มีไฟสัญญาณแจ้งลำดับการพิมพ์สมุดคู่ฝากในกรณีที่ผู้ที่รับมอบอำนาจใช้เครื่องพิมพ์เดียวกันเกินกว่า 1 คน

ขั้นตอน	แนวปฏิบัติที่ดี
	มีการตั้งค่าระบบให้ขึ้นข้อความแจ้งเตือนที่หน้าจอผู้ที่รับมอบอำนาจให้ปรับสมุดคู่ฝาก
	มีระบบควบคุมการพิมพ์สมุดคู่ฝากให้ต่อเนื่องจากข้อมูลล่าสุดที่ปรากฏในสมุดคู่ฝาก
การตรวจสอบความถูกต้องและครบถ้วนก่อนให้หลักฐานแก่ผู้มาทำรายการ	มีการตรวจสอบการบันทึกรายการในหลักฐานทำรายการทุกใบโดยผู้อื่น (ตรวจสอบรายการที่ระบบพิมพ์ในใบนำฝาก ใบถอน ใบคำขอโอนเงิน กับข้อมูลในใบดังกล่าว)
	มีการกระทบยอดระหว่างใบนำฝาก ใบถอน ใบคำขอโอนเงิน กับยอดเงินในระบบโดยผู้ที่รับมอบอำนาจ และผู้ที่มีอำนาจอนุมัติ
การแก้ไขรายการ	**การอนุมัติก่อนการแก้ไขรายการ**
	มีการตั้งค่าระบบให้บังคับให้มีการอนุมัติการแก้ไขรายการก่อนข้อมูลที่แก้ไขถูกบันทึกในระบบ
	มีการพิสูจน์ตัวตนของผู้ที่มีอำนาจอนุมัติในระบบที่ปลอดภัย เช่น การใช้ Two-Factor Authentication หรือการสแกนลายนิ้วมือของผู้มีอำนาจอนุมัติ
	ระบบกำหนดสิทธิ์การอนุมัติการทำรายการให้กับผู้ที่มีอำนาจอนุมัติเท่านั้น
	ระบบจะปฏิเสธการทำรายการและอนุมัติรายการโดยใช้รหัสผู้ใช้งานเดียวกัน
	การควบคุมอื่น ๆ เกี่ยวกับการแก้ไขรายการ
	การแก้ไขต้องทำโดยความเห็นชอบพร้อมกันของผู้ที่รับมอบอำนาจ ผู้ที่มีอำนาจอนุมัติ และเจ้าของบัญชี
	มีการตรวจสอบความถูกต้อง และความครบถ้วนของการทำรายการทุก ๆ สิ้นวันโดยผู้ที่มีอำนาจอนุมัติ

<u>หมายเหตุ</u>: 1) ผู้ที่มีอำนาจอนุมัติ หมายถึง เจ้าหน้าที่ที่รับมอบอำนาจจากธนาคาร และมีตำแหน่งสูงกว่า Teller

2) Two-Factor Authentication หมายถึง วิธีการพิสูจน์ตัวตนของผู้ทำรายการโดยใช้ข้อมูล 2 อย่าง ประกอบกัน ซึ่งข้อมูลดังกล่าวมี 3 ประเภท ได้แก่ 1) Something You Know เช่น User ID และ Password เป็นต้น 2) Something You Have เช่น บัตรอนุมัติรายการ เป็นต้น และ 3) Something You Are เช่น ลายนิ้วมือ เป็นต้น ตัวอย่างการใช้ Two-Factor Authentication เช่น การที่ผู้ที่มีอำนาจอนุมัติรูดบัตรอนุมัติรายการพร้อมการกรอก Password เพื่ออนุมัติรายการ เป็นต้น

<u>ข้อสังเกต</u>: แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน โดยโครงการใน Phase 2 ปี 2557 ธปท. จะศึกษาจัดทำแนวปฏิบัติที่ยอมรับได้ (Acceptable Practices) และประเมิน Gap ร่วมกับ ธพ. แต่ละแห่ง เพื่อเป็นแนวทางให้ ธปท. และ ธพ. ร่วมกันพิจารณาความเหมาะสมของการจัดทำแผนพัฒนาปรับปรุงระบบ IT ของตนเองให้ได้ตามมาตรฐานสากล ทั้งในระยะสั้นและระยะยาวต่อไป

1.4 การควบคุมเพิ่มเติมที่สำคัญ

ตารางการควบคุมที่สำคัญ

การควบคุมเพิ่มเติมที่สำคัญ
วัตถุประสงค์ เพื่อให้ธนาคารมีการควบคุมเพิ่มเติมที่สำคัญตามมาตรฐานสากล ซึ่งเป็นการควบคุมเสริมจากการควบคุมหลักตามที่ได้กล่าวไว้ในข้อ 1.1-1.3 ทั้งนี้ มาตรฐานการควบคุมเพิ่มเติมที่สำคัญอาจมีการปรับเปลี่ยนไปตามวิวัฒนาการและเทคโนโลยีสารสนเทศในอนาคต
แนวปฏิบัติที่ดี ธนาคารควรมีระบบ Fraud Monitoring ที่สามารถเฝ้าระวังและติดตามพฤติกรรมการดำเนินการใด ๆ และการทำธุรกรรมที่น่าสงสัยและ/หรือเข้าข่ายเป็นการทุจริต ครอบคลุมทุกช่องทางของการทำธุรกรรม ได้แก่ สาขา ATM และ Internet Banking โดยระบบควรมีความสามารถอย่างน้อยดังต่อไปนี้ 1. วิเคราะห์รูปแบบการทุจริตที่เกิดจากบุคคลภายในและภายนอก รวมทั้งการทุจริตที่เกิดจากหลายช่องทางร่วมกัน (Cross Channel Fraud) เช่น • การโอนเงินจาก Internet Banking หลายๆ ครั้ง แล้วไปถอนเงินออกผ่านตู้ ATM ทันที • การเข้าดูข้อมูลลูกค้าของพนักงานที่ไม่ได้รับมอบอำนาจ • การทำรายการเพื่อตนเองของผู้ที่ได้รับมอบอำนาจหรือผู้ที่มีอำนาจอนุมัติ 2. แจ้งเตือนในทันทีที่ตรวจพบรูปแบบการทุจริต เพื่อให้เจ้าหน้าที่ดำเนินการจำกัดความเสียหายไม่ให้ส่งผลกระทบลุกลามเป็นวงกว้าง 3. มีฟังก์ชั่นให้เจ้าหน้าที่ที่ได้รับมอบอำนาจดำเนินการปรับเปลี่ยนเงื่อนไขของระบบ (Fraud Detection Rules) เพื่อปรับปรุงประสิทธิภาพในการติดตามตรวจสอบรายการทุจริตให้สามารถติดตามรูปแบบการทุจริตใหม่ๆได้ โดยระบบมีการควบคุมและจำกัดสิทธิ์ในการปรับเปลี่ยนเงื่อนไขเฉพาะผู้ที่ได้รับมอบหมายเท่านั้น

หมายเหตุ: ผู้ที่มีอำนาจอนุมัติ หมายถึง เจ้าหน้าที่ที่รับมอบอำนาจจากธนาคาร และมีตำแหน่งสูงกว่า Teller

ข้อสังเกต: แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน โดยโครงการใน Phase 2 ปี 2557 ธปท. จะศึกษาจัดทำแนวปฏิบัติที่ยอมรับได้ (Acceptable Practices) และประเมิน Gap ร่วมกับ ธพ. แต่ละแห่ง เพื่อเป็นแนวทางให้ ธปท. และ ธพ. ร่วมกันพิจารณาความเหมาะสมของการจัดทำแผนพัฒนาปรับปรุงระบบ IT ของตนเองให้ได้ตามมาตรฐานสากล ทั้งในระยะสั้นและระยะยาวต่อไป

ส่วนที่ 2

แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบ IT ที่สนับสนุนธุรกิจหลัก

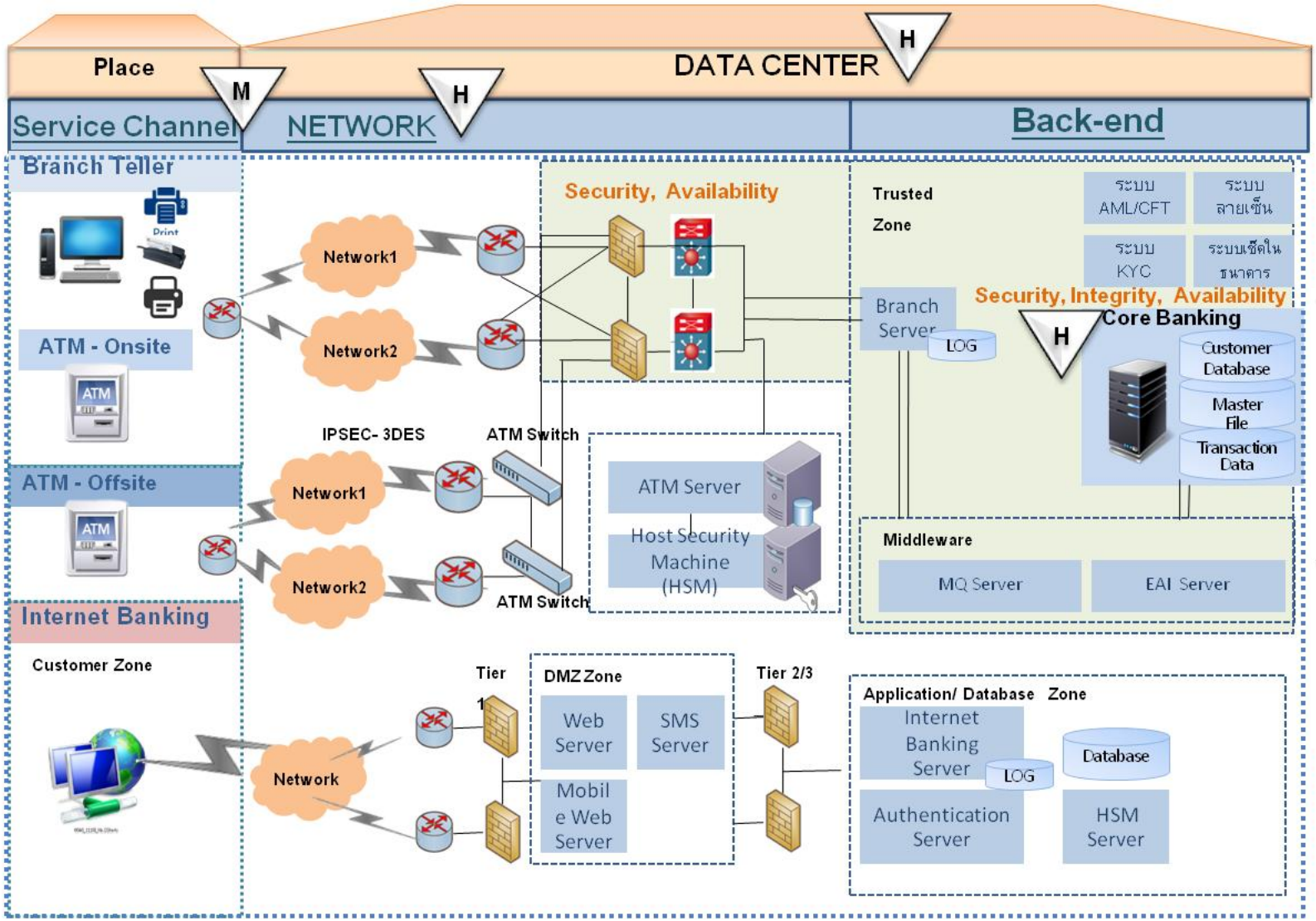
Phase 1 : ธุรกรรมฝาก ถอน และโอนเงิน

สรุปความหมายโดยย่อของคำศัพท์ที่สำคัญ

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 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 อย่าง ประกอบกัน 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 ซึ่งอาจเป็นสถาบันการเงินกับผู้ให้บริการภายนอก หรือหน่วยงานธุรกิจกับหน่วยงาน IT

หมายเหตุ : ความหมายของคำศัพท์นี้เป็นความหมายโดยย่อที่จัดทำขึ้นเพื่อมุ่งเน้นให้ผู้อ่านสามารถเข้าใจได้ง่ายและใช้อ้างอิงเฉพาะในแนวปฏิบัติฉบับนี้

แผนภาพแสดง High-Level IT System Process Flow



H องค์ประกอบหรือระบบงาน IT ที่เป็นโครงสร้างพื้นฐานสำคัญรองรับการทำธุรกรรมการเงิน หากมีการเข้าถึง/เปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาติ หรือถูกทำลายจนหยุดชะงักจะส่งผลกระทบเป็นวงกว้างต่อความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมของการให้บริการและการทำธุรกรรมการเงินของลูกค้า (ที่สำคัญ เช่น ศูนย์คอมพิวเตอร์ ระบบเครือข่ายสื่อสาร และระบบ Core Banking เป็นต้น)

M องค์ประกอบหรือระบบ IT ที่สนับสนุนการให้บริการหรือการทำธุรกรรมการเงิน ซึ่งหากมีการเข้าถึง/เปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาติ หรือถูกทำลายจนหยุดชะงักจะส่งผลกระทบต่อความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมของการให้บริการและการทำธุรกรรมการเงินเป็นบางส่วน (วงจำกัด) (เช่น ระบบช่องทางการให้บริการต่าง ๆ เป็นต้น)

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 การปลอมแปลง หรือการทำลายข้อมูลระบบงาน/ 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*

2.1 ศูนย์คอมพิวเตอร์ (Data Center)

2.1.1 การควบคุมการเข้าถึงศูนย์คอมพิวเตอร์ทางกายภาพ (Physical Access Control)

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

<u>แนวปฏิบัติที่ดี</u>

- มีการควบคุมทางกายภาพและมีระบบควบคุมการเข้าถึงตัวอาคารศูนย์คอมพิวเตอร์หลัก (ศูนย์ฯ) และพื้นที่สำคัญต่างๆ ภายในศูนย์ฯ ได้แก่ ห้องจัดเก็บเครื่องประมวลผล ห้องจัดเก็บอุปกรณ์เครือข่าย ห้องจัดเก็บสื่อบันทึกข้อมูล ห้องจัดเก็บอุปกรณ์สาธารณูปโภค และห้องปฏิบัติงาน เป็นต้น (พื้นที่สำคัญฯ) ให้เข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตตามสิทธิ์ที่ได้รับมอบหมายเท่านั้น 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 และมีรายละเอียดเพียงพอสำหรับใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้ โดยเก็บย้อนหลังเป็นระยะเวลาอย่างน้อย 90 วัน ไว้ในสถานที่ที่มีความมั่นคงปลอดภัย
    - สามารถแจ้งเตือนผู้เกี่ยวข้องเมื่อเกิดเหตุผิดปกติได้อย่างทันการณ์ตลอด 24x7 ชม. เช่น เมื่อพบการพยายามเข้าถึงพื้นที่สำคัญภายในศูนย์ฯ โดยผู้ไม่ได้รับอนุญาต การผ่านเข้า-ออกศูนย์ฯ ทางประตูหนีไฟ การเปิดประตูค้างไว้ เป็นต้น

  นอกจากนี้ มีการควบคุมการเข้าถึงทางกายภาพพื้นที่รอบนอกศูนย์ฯ ที่เหมาะสม เช่น มีกำแพงหรือรั้วที่มั่นคง มีเจ้าหน้าที่ตรวจสอบการผ่านเข้า-ออกและมีการตรวจสอบยานพาหนะ เป็นต้น อีกทั้งมีการแบ่งแยกพื้นที่ลานจอดรถบุคคลภายนอก (Visitor Parking Area) รวมถึงพื้นที่/ อุปกรณ์ที่ใช้ในการขนส่งสินค้า (Loading Docks) ออกจากบริเวณศูนย์ฯ
- มีการติดตั้งกล้องวงจรปิดบริเวณรอบนอกอาคารศูนย์ฯ ประตูทางเข้าศูนย์ฯ และภายในศูนย์ฯ อย่างทั่วถึง เพื่อใช้เป็นเครื่องมือสำคัญในการติดตามการเข้า-ออก และการกระทำต่างๆ ภายในศูนย์ โดยเก็บบันทึกภาพจากกล้องวงจรปิดไว้เป็นระยะเวลาอย่างน้อย 90 วัน และให้ภาพที่จัดเก็บมีความชัดเจนเพียงพอที่จะใช้ในการพิสูจน์หลักฐาน
- มีเจ้าหน้าที่ดูแลรักษาความปลอดภัยศูนย์ฯ เฝ้าระวังผ่านระบบกล้องวงจรปิด (CCTV) ตลอดเวลา (24x7)
- ห้ามไม่ให้นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่สามารถบันทึกภาพ/เสียงได้เข้ามาภายในพื้นที่สำคัญภายในศูนย์ฯ ได้แก่ ห้องจัดเก็บเครื่องประมวลผล ห้องจัดเก็บอุปกรณ์เครือข่าย ห้องจัดเก็บสื่อบันทึกข้อมูล เว้นแต่จะได้รับอนุญาตโดยผู้ที่มีอำนาจอนุมัติ
- เครื่องประมวลผลและอุปกรณ์เครือข่ายควรถูกจัดเก็บอยู่ในตู้ Rack ที่มีการปิดล็อกอยู่ตลอดเวลา และการเข้าถึงต้องเป็นแบบ Dual Control

- มีกระบวนการจัดการสิทธิ์และหน่วยงานที่รับผิดชอบชัดเจน ในการเข้าถึงศูนย์ฯ และพื้นที่สำคัญฯ ให้เป็นไปตามหลักความจำเป็น ถูกต้อง และเป็นปัจจุบัน ดังนี้
    - มีการจัดทำตารางการควบคุมการให้สิทธิ์ที่สอดคล้องกับตำแหน่งหน้าที่งานเพื่อใช้เป็นแนวทางการกำหนดสิทธิ์อย่างเป็นระบบและเป็นปัจจุบัน (Authorization Matrix) และมีการทบทวนตารางควบคุมการให้สิทธิ์ (Authorization Matrix) ทุกครั้งที่มีการเปลี่ยนแปลงหรือเป็นประจำอย่างน้อยทุก 6 เดือน
    - การอนุมัติการเข้าถึงศูนย์ฯ และพื้นที่สำคัญต่างๆ ภายในศูนย์ฯ ต้องดำเนินการโดยผู้ที่มีอำนาจอนุมัติและสอดคล้องตามตารางการควบคุมการให้สิทธิ์
    - มีการปรับปรุง/ ยกเลิกสิทธิ์การเข้า–ออกศูนย์ฯ ทันทีที่พนักงานลาออก โยกย้าย หรือเปลี่ยนหน้าที่ความรับผิดชอบ
    - มีการทบทวนสิทธิ์การเข้า-ออกศูนย์ฯ โดยผู้ที่มีอำนาจอนุมัติอย่างสม่ำเสมอ อย่างน้อยทุก 6 เดือน
- การเข้าถึงโดยพนักงานที่ไม่ได้มีหน้าที่ปฏิบัติงานประจำภายในศูนย์ฯ หรือบุคคลภายนอกมีกระบวนการในการควบคุมการเข้าถึงแบบชั่วคราว ดังนี้
    - มีการอนุมัติโดยผู้มีอำนาจอนุมัติก่อนทุกครั้ง
    - มีการมอบหมายให้มีเจ้าหน้าที่ศูนย์ฯ ติดตาม (Escort) ผู้เข้าถึงแบบชั่วคราวตลอดระยะเวลาที่เข้ามาปฏิบัติงานภายในศูนย์ฯ
    - มีเจ้าหน้าที่ควบคุมการลงบันทึกเข้า-ออกศูนย์ฯ โดยมีขั้นตอนและเครื่องมือที่สามารถระบุตัวตนของผู้ที่ได้รับอนุญาตให้เข้าถึงศูนย์ฯ แบบชั่วคราว พร้อมทั้งจัดทำทะเบียนคุมสำหรับลงบันทึกการเข้า-ออกศูนย์ฯ ที่มีรายละเอียดเพียงพอสำหรับใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลได้
- มีกระบวนการสอบทาน Log Files ตลอดจนทะเบียนคุมการเข้า-ออกศูนย์ฯ โดยผู้ที่มีอำนาจอนุมัติอย่างสม่ำเสมออย่างน้อยทุก 30 วัน เพื่อติดตามการเข้าถึงศูนย์ฯ ที่ผิดปกติ เช่น ช่วงเวลาหรือความถี่ที่ผิดปกติ หรือการพยายามเข้าถึงโดยบุคคลไม่เหมาะสม

2.1.2 การบริหารจัดการศูนย์ฯ (Facility Management)

<u>วัตถุประสงค์</u> เพื่อให้ศูนย์คอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศมีความพร้อมใช้งานรองรับธุรกิจอย่างต่อเนื่อง

<u>แนวปฏิบัติที่ดี</u>

- จัดให้มีการประเมินความเสี่ยงของศูนย์ฯ ครอบคลุมปัจจัยเสี่ยงอย่างน้อยในเรื่องความปลอดภัยของพื้นที่รอบนอกศูนย์ฯ ตัวอาคารศูนย์ฯ และภายในศูนย์ฯ ความพร้อมใช้ของระบบสาธารณูปโภค ประสิทธิ์ภาพระบบป้องกันภัยต่างๆ และความเพียงพอของการปฏิบัติงานภายในศูนย์ฯ การประเมินความเสี่ยงควรดำเนินการอย่างน้อยเป็นประจำทุกปี และเมื่อมีการเปลี่ยนแปลงที่สำคัญ โดยมีการบันทึกไว้เป็นลายลักษณ์อักษรและนำเสนอต่อคณะกรรมการที่ได้รับมอบหมายเพื่อรับทราบและ/ หรือขออนุมัติแผนปิด/ ลดความเสี่ยง
- ในการสร้างศูนย์ฯ สถานที่ตั้งไม่อยู่ในพื้นที่เสี่ยงภัย เช่น ตั้งอยู่ใกล้ปั๊มน้ำมัน ปั๊มแก๊ส หรือทางด่วน ควรกำหนดเป็นปัจจัยหนึ่งของการพิจารณาที่ตั้งของศูนย์ฯ สำหรับกรณีศูนย์ฯ ในปัจจุบันควรจัดให้มีมาตรการรองรับเหตุฉุกเฉินจากภัยพิบัติต่างๆ

- สถานที่ตั้งศูนย์ฯ อยู่แยกจากอาคารสำนักงาน (Stand Alone) โดยมีการออกแบบโครงสร้างอาคาร สถานที่ และการติดตั้งระบบสาธารณูปโภคที่เหมาะสม
- โครงสร้างตัวอาคารศูนย์ฯ ถูกออกแบบให้สามารถรองรับภัยต่างๆ ในระดับที่เหมาะสม ปลอดภัย และยากต่อการทำลาย ดังนี้
    - การบุกรุก การทุบทำลาย และการรองรับแรงระเบิด
    - การป้องกันอัคคีภัย ผนังภายนอกศูนย์ฯ สามารถกันไฟได้อย่างน้อย 4 ชั่วโมง ผนังภายในที่กั้นพื้นที่สำคัญสามารถกันไฟได้อย่างน้อย 2 ชั่วโมง และผนังกั้นพื้นที่อื่นๆ 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 ทั้งนี้แต่ละชุดควรติดตั้งให้ครอบคลุมความเสี่ยงจากกรณีที่เครื่องใดเครื่องหนึ่งในชุดหยุดชะงัก/ 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))

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

- มีการสำรองน้ำมันไว้ในระดับที่เพียงพอให้อุปกรณ์ Generator สามารถจ่ายไฟให้ศูนย์ฯ ได้อย่างต่อเนื่องเป็นระยะเวลาอย่างน้อย 4 วัน[3] และมีมาตรการในการดำเนินการเพื่อขนส่งน้ำมันมายังศูนย์ฯ เพิ่มเติมเพื่อการให้บริการอย่างต่อเนื่อง
- อุปกรณ์ระบบไฟฟ้า เช่น High Voltage, Transformer, ATS, UPS และ Generator ติดตั้งในห้องที่แยกจากห้องจัดเก็บอุปกรณ์อื่นๆ โดยมีการควบคุมอุณหภูมิ ความชื้น และมีการระบายอากาศที่เหมาะสม

- ระบบทำความเย็นและควบคุมความชื้น
  - มีการติดตั้งระบบทำความเย็นและควบคุมความชื้น (ระบบทำความเย็นฯ) เช่น Precision Air Conditioner, Computer Room Air Conditioner (CRAC) เพื่อรองรับพื้นที่สำคัญฯ โดยมีเครื่องสำรองเพื่อรองรับการทำงานในกรณีที่เครื่องหลักชำรุดหรือหยุดซะงักหรือบำรุงรักษาเครื่องที่เหลือต้องสามารถรองรับการให้บริการได้อย่างต่อเนื่อง
  - ระบบไฟฟ้าและระบบท่อน้ำเย็น (Chiller System) ที่รองรับระบบทำความเย็นฯ ควรมีระบบสำรองสามารถรองรับการให้บริการได้อย่างต่อเนื่อง โดยระบบทำความเย็นฯ ควรควบคุมอุณหภูมิให้อยู่ในระหว่าง 20-25 C° 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) โดยติดตั้งให้ครอบคลุมพื้นที่สำคัญฯ
- การบำรุงรักษา
  - มีกระบวนการ และเจ้าหน้าที่รับผิดชอบในการตรวจเช็คประจำวัน (Daily Checklist) ของระบบสาธารณูปโภคที่สำคัญในศูนย์ฯ ได้แก่ สภาพแวดล้อมของสถานที่จัดเก็บอุปกรณ์ และการทำงานของอุปกรณ์ต่างๆ 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

[2] มาตรฐาน TIA-942 ในเรื่องการระยะเวลาการสำรองไฟฟ้าของแบตเตอรี่ใน UPS (Tier 4)
[3] มาตรฐาน TIA-942 ในเรื่องการสำรองน้ำมันของอุปกรณ์ generator สำหรับจ่ายไฟที่ full load
[4] มาตรฐาน TIA-942 ในเรื่องการควบคุมอุณหภูมิและความชื้น

และระบบตรวจจับน้ำรั่วซึม ตามรอบระยะเวลาที่ผู้ผลิตแนะนำ - มีการทดสอบการใช้งานระบบสาธารณูปโภคอย่างสม่ำเสมอ โดยในการทดสอบควรพึงระวังไม่ให้การทดสอบนั้นกระทบต่อการดำเนินงานปกติของธนาคาร - มีระบบศูนย์กลางในการติดตามสถานะของระบบสาธารณูปโภคที่สำคัญภายในศูนย์ฯ เช่น อุปกรณ์ UPS, แบตเตอรี่ของอุปกรณ์ UPS, อุปกรณ์ Generator, Chiller System, ระบบป้องกัน/ ระงับอัคคีภัย และระบบตรวจจับน้ำรั่วซึม โดยมีเจ้าหน้าที่เฝ้าระวังระบบตลอด 24 ชม. และมีระบบแจ้งเตือนอัตโนมัติให้ผู้เกี่ยวข้องทราบทันทีเมื่อมีเหตุผิดปกติ

ข้อสังเกต: แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน โดยโครงการใน Phase 2 ปี 2557 ธปท. จะศึกษาจัดทำแนวปฏิบัติที่ยอมรับได้ (Acceptable Practices) และประเมิน Gap ร่วมกับ ธพ. แต่ละแห่ง เพื่อเป็นแนวทางให้ ธปท. และ ธพ. ร่วมกันพิจารณาความเหมาะสมของการจัดทำแผนพัฒนาปรับปรุงระบบ IT ของตนเองให้ได้ตามมาตรฐานสากล ทั้งในระยะสั้นและระยะยาวต่อไป

2.2 ระบบเครือข่ายสื่อสาร (Network)

2.2.1 Network Access Control

<u>วัตถุประสงค์</u> เพื่อให้โครงสร้างของระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย โดยมีการออกแบบระบบเครือข่ายที่เหมาะสมตามมาตรฐานสากล และมีการป้องกัน/เฝ้าระวังภัยบุกรุกหรือภัยคุกคามรูปแบบต่างๆ

<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 โดยคำนึงถึง ระดับความสำคัญของระบบงาน ระดับความสำคัญของข้อมูลที่ถูกประมวลผล รวมถึงความจำเป็นในการเชื่อมต่อจากระบบงานอื่นๆ หรือจากภายนอกองค์กร และจัดให้มีการควบคุมการเชื่อมต่อจากระบบงานต่างๆ มายังระบบงานที่มีความสำคัญอย่างเข้มงวด
- ในจุดที่มีการแบ่งแยกเครือข่ายที่พิจารณาว่ามีความสำคัญและมีความเสี่ยง ควรติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่ายที่มีความสามารถในการควบคุมและคัดกรอง Traffic ที่ส่งผ่านระบบเครือข่าย การเฝ้าระวังการบุกรุก การป้องกันการบุกรุก และการตรวจจับไวรัส หรือมัลแวร์ต่างๆ ที่อาจบุกรุกเข้าสู่เครือข่าย
- มีการใช้อุปกรณ์รักษาความปลอดภัยเครือข่ายเพื่อคัดกรอง Traffic ในระดับ Application ในจุดที่มีการเชื่อมต่อกับ Internet เช่น การใช้ Web Application Firewall เป็นต้น
- กรณีมีการแบ่งแยกเครือข่ายเป็นหลายชั้น ควรใช้อุปกรณ์รักษาความปลอดภัยเครือข่ายที่ต่างยี่ห้อกันในแต่ละจุด เพื่อเพิ่มประสิทธิภาพในการคัดกรอง Traffic ที่ส่งผ่านระบบเครือข่าย
- มีการควบคุม และจำกัดให้เฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงระบบเครือข่ายได้ รวมถึงมีการระบุตัวตนของอุปกรณ์ที่มาเชื่อมต่อกับระบบเครือข่ายอย่างเหมาะสม
- มีการจำกัดให้เฉพาะบุคคลที่ได้รับมอบอำนาจเท่านั้นที่สามารถเข้าถึงระบบเครือข่าย โดยจำกัดสิทธิ์ในการเข้าถึงระบบเครือข่ายให้อยู่ในส่วนที่มีความจำเป็น และเหมาะสมตามหน้าที่การทำงานเท่านั้น
- การเข้าถึงอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเพื่อบริหารจัดการค่าต่างๆ 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

2.2.2 Network Security Management

<u>วัตถุประสงค์</u> เพื่อให้อุปกรณ์ระบบเครือข่ายมีการรักษาความปลอดภัยและมีความถูกต้องเชื่อถือได้

<u>แนวปฏิบัติที่ดี</u>

- มีการตั้งค่าอุปกรณ์รักษาความปลอดภัยเครือข่ายเพื่อควบคุมให้ระบบงานติดต่อสื่อสารกันได้ตามความจำเป็น รวมถึงมีการปรับแต่งค่า (Tuning) เพื่อเพิ่มประสิทธิภาพในการดักจับภัยบุกรุกและมีการทบทวนการตั้งค่าอย่างสม่ำเสมอหรืออย่างน้อยปีละ 2 ครั้ง หรือเมื่อมีการบุกรุกรูปแบบใหม่ๆ
- มีการใช้ระบบในการควบคุมค่าเวลาของเครื่องประมวลผล ให้ตรงกับเครื่องเซิร์ฟเวอร์ NTP (Clock Synchronization) เพื่อให้ค่าเวลาในการบันทึกเหตุการณ์ (Log) มีความถูกต้องในลักษณะ Real-Time ซึ่งเซิร์ฟเวอร์ NTP ต้องรับสัญญาณนาฬิกาจากสถาบันที่มีความน่าเชื่อถือ ยกตัวอย่างเช่น กรมอุทกศาสตร์ (กองทัพเรือ) หรือ สถาบันมาตรวิทยา (กระทรวงวิทยาศาสตร์และเทคโนโลยี)
- มีกระบวนการหรือเครื่องมือในการตรวจสอบการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นกับอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายที่พิจารณาว่ามีความสำคัญหรือมีความเสี่ยง 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 และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยผู้เชี่ยวชาญ 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

2.2.3 Network Availability Management

<u>วัตถุประสงค์</u> 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

<u>ข้อสังเกต</u>: แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน โดยโครงการใน Phase 2 ปี 2557 ธปท. จะศึกษาจัดทำแนวปฏิบัติที่ยอมรับได้ (Acceptable Practices) และประเมิน Gap ร่วมกับ ธพ. แต่ละแห่ง เพื่อเป็นแนวทางให้ ธปท. และ ธพ. ร่วมกันพิจารณาความเหมาะสมของการจัดทำแผนพัฒนาปรับปรุงระบบ IT ของตนเองให้ได้ตามมาตรฐานสากล ทั้งในระยะสั้นและระยะยาวต่อไป

2.3 ระบบ Core Banking

2.3.1 Logical Access Control

<u>วัตถุประสงค์</u> เพื่อให้การบริหารจัดการบัญชีและสิทธิ์ของผู้ใช้งานมีประสิทธิภาพเป็นไปตามหลักความจำเป็นของการใช้งานและสอดคล้องกับหลักการแบ่งแยกงาน IT ที่ดี โดยสามารถป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

<u>แนวปฏิบัติที่ดี</u>

- มีหน่วยงานและกระบวนการมาตรฐานในการเพิ่ม เปลี่ยนแปลง และลบบัญชีผู้ใช้ รวมถึงสิทธิ์ของผู้ใช้ และมีการใช้ระบบเพื่อสนับสนุนการจัดการสิทธิ์ให้มีประสิทธิภาพ มากยิ่งขึ้น 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 เดือนสำหรับบัญชีผู้ใช้ดูแลระบบและบัญชีผู้ใช้ที่มีสิทธิ์เทียบเท่าสิทธิ์สูง
    - 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) ออกจากหน้าที่การทำงานอื่นๆ
    - แบ่งแยกบุคคลากรที่มีหน้าที่พัฒนาระบบงาน (Developer) ออกจาก คนที่ได้สิทธิ์ในการโอนย้ายระบบขึ้นสู่ Production (Migration)
- มีกระบวนการควบคุมดูแลการเบิกใช้บัญชีผู้ใช้งานที่มีสิทธิ์สูงสุด (Highest Privilege User) อย่างเหมาะสม โดยครอบคลุม
    - มีการจัดเก็บรหัสผ่านของบัญชีผู้ใช้ที่มีสิทธิ์สูงสุดโดยหน่วยงานที่มีความเป็นอิสระจากหน่วยงานของผู้ขอเบิกใช้
    - มีการจำกัดผู้ใช้งานที่มีสิทธิ์ในการเบิกใช้และช่วงเวลาในการเบิกใช้บัญชีผู้ใช้ที่มีสิทธิ์สูงสุดไว้สำหรับกรณีที่มีความจำเป็นเท่านั้น

- 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 จะต้องมีการระบุตัวตนและพิสูจน์ตัวตนด้วยวิธีการที่เหมาะสมเช่น 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 วันและทุกครั้งหลังใช้งาน
    - 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

2.3.2 System Security Management

<u>วัตถุประสงค์</u> เพื่อให้การประมวลผลข้อมูลเป็นไปอย่างถูกต้องครบถ้วนและไม่กระทบกับการให้บริการทางธุรกิจ

<u>แนวปฏิบัติที่ดี</u>

- มีกระบวนการตรวจสอบความถูกต้องและครบถ้วนของการประมวลผลข้อมูลโดยอย่างน้อยต้องครอบคลุมถึง
    - จัดให้มีการตรวจสอบความถูกต้องและครบถ้วนโดยผู้รับมอบอำนาจทันทีภายหลังขั้นตอนที่มีจุด Check Point ตามที่ธนาคารกำหนดเสร็จสิ้น
    - มีการสอบทานรายงานการปฏิบัติงานการประมวลผลสิ้นวันโดยหัวหน้างานในวันทำการถัดไป
    - มีกระบวนการแก้ไขปัญหาที่ชัดเจนในกรณีที่การประมวลผลข้อมูลไม่สำเร็จ และมีแนวทางในการรายงานให้ผู้บังคับบัญชาทราบตามลำดับชั้น ตั้งแต่เกิดปัญหาจนกระทั่งแก้ไขปัญหาแล้วเสร็จ

<u>วัตถุประสงค์</u> 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

<u>วัตถุประสงค์</u> เพื่อให้การเปลี่ยนแปลงระบบ ตั้งแต่การตั้งค่าของระบบงาน การปรับปรุงแก้ไขระบบ ไปจนถึงการพัฒนาระบบ มีความถูกต้องเหมาะสม

<u>แนวปฏิบัติที่ดี</u>

- มีกระบวนการและเครื่องมือการบริหารจัดการการเปลี่ยนแปลงที่เกี่ยวข้องกับระบบอย่างเป็นขั้นตอนดังนี้
    - การประเมินผลกระทบที่เกี่ยวข้อง
    - การทดสอบ
    - การจัดเตรียมแผนย้อนกลับ (Roll Back Plan) หรือแผนสำรองฉุกเฉินกรณีที่ทำการเปลี่ยนแปลงไม่สำเร็จ (Fall Back Plan)

[6] Development Tools คือ เครื่องมือหรือโปรแกรมที่ใช้ในการพัฒนาระบบงาน

[7] Compliers เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าแปลงชุดคำสั่งภาษาคอมพิวเตอร์ (Source Code) ให้ไปอยู่ในรูปแบบที่คอมพิวเตอร์ประมวลผลได้ (Execute File)

- การอนุมัติโดยผู้ที่มีอำนาจอนุมัติ
- การติดตามผลหลังจากติดตั้ง (Post Implementation Review)

- มีการจำกัดสิทธิ์ในการเปลี่ยนแปลงการตั้งค่าและการเข้าถึงหน้าการบริหารจัดการเครื่องแม่ข่ายไว้เฉพาะผู้ที่รับมอบอำนาจเท่านั้น
- มีการตั้งค่าความปลอดภัยของเครื่องประมวลผลตามแนวปฏิบัติขั้นต่ำด้านการรักษาความปลอดภัย (Security Baseline) และมีการสอบทานการตั้งค่าดังกล่าวโดยผู้มีหน้าที่ควบคุมดูแลความปลอดภัย หรือความเสี่ยงด้านเทคโนโลยีอย่างสม่ำเสมอ
- มีกระบวนการประเมินช่องโหว่ (Vulnerability Assessment) ของระบบงานประมวลผลหลัก อย่างสม่ำเสมอโดยผู้เชี่ยวชาญ 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 ยกตัวอย่างเช่น กรมอุทกศาสตร์ (กองทัพเรือ) หรือ สถาบันมาตรวิทยา (กระทรวงวิทยาศาสตร์และเทคโนโลยี)
- มีการติดตั้งโปรแกรมป้องกันภัยจากมัลแวร์บนระบบงานประมวลผลหลัก โดยต้องเป็นโปรแกรมที่ได้รับอนุมัติเท่านั้น และควรมีการอัพเดทซิกเนเจอร์ของโปรแกรมป้องกันมัลแวร์ให้เป็นปัจจุบัน
- มีการติดตั้ง Software Updates/ Patch ที่จำเป็นสำหรับระบบงานประมวลผลหลัก ตามคำแนะนำของผู้ผลิต โดยการติดตั้งต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงอย่างเป็นขั้นตอน

<u>วัตถุประสงค์</u> เพื่อให้การบันทึกเหตุการณ์สามารถใช้ติดตามตรวจสอบการเข้าใช้งานระบบของผู้ใช้งาน และการทำธุรกรรมที่เหมาะสม

<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

<u>วัตถุประสงค์</u> 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

<u>วัตถุประสงค์</u> 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 ควรมีการจัดเตรียมเครื่อง อุปกรณ์ ระบบ และข้อมูลสำรองพร้อมทำงานโดยอัตโนมัติเมื่อเกิดเหตุฉุกเฉิน ในลักษณะ High Availability
- มีการจัดเตรียมเครื่อง อุปกรณ์ ระบบ ข้อมูลสำรอง ไว้ที่ศูนย์ฯ สำรอง โดยมีกระบวนการที่ทำให้มั่นใจได้ว่าโปรแกรมระบบงาน รวมถึงการตั้งค่าและการปรับแต่งค่าบนระบบสำรองถูกต้องเป็นปัจจุบันสำหรับพร้อมรองรับการทำธุรกรรม หากเกิดเหตุขัดข้องและระบบงานหลักไม่สามารถให้บริการได้ตามปกติ
- มีกระบวนการทดสอบเพื่อให้แน่ใจว่าระบบงานสำรองมีความพร้อมในการใช้งาน

<u>หมายเหตุ</u>: ธพ. สามารถนำแนวปฏิบัติของระบบ Core Banking ไปประยุกต์ใช้ตามความเหมาะสมกับเครื่องประมวลผลอื่น เช่น เครื่องประมวลผลสาขา (Branch Server) เครื่องประมวลผล ATM เป็นต้น

<u>ข้อสังเกต</u>: แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน โดยโครงการใน Phase 2 ปี 2557 ธปท. จะศึกษาจัดทำแนวปฏิบัติที่ยอมรับได้ (Acceptable Practices) และประเมิน Gap ร่วมกับ ธพ. แต่ละแห่ง เพื่อเป็นแนวทางให้ ธปท. และ ธพ. ร่วมกันพิจารณาความเหมาะสมของการจัดทำแผนพัฒนาปรับปรุงระบบ IT ของตนเองให้ได้ตามมาตรฐานสากล ทั้งในระยะสั้นและระยะยาวต่อไป

2.4 ระบบงานการให้บริการแก่ลูกค้า

2.4.1 เครื่องคอมพิวเตอร์ส่วนบุคคลที่สาขา

2.4.1.1 PC Security Control

<u>วัตถุประสงค์</u> 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 Harddisk และ Internet เป็นต้น
- มีการลงโปรแกรมป้องกันภัยจากมัลแวร์ที่เครื่องคอมพิวเตอร์สาขา และควรมีการอัพเดทซิกเนเจอร์ของโปรแกรมป้องกันมัลแวร์ให้เป็นปัจจุบัน
- มีการควบคุมการการเข้าใช้บริการเครือข่าย Internet โดยคำนึงถึง
    - การจำกัด Website ที่เข้าถึงได้
    - การจำกัดการดาวน์โหลด/ อัพโหลดข้อมูลจากอินเตอร์เน็ต
- มีการกำหนดทะเบียนโปรแกรมที่ได้รับอนุญาตให้สามารถติดตั้งบนเครื่องคอมพิวเตอร์สาขาตามความจำเป็นในการใช้งาน โดยจัดให้มีกระบวนการในการขออนุญาตติดตั้งโปรแกรม และมีหน่วยงานควบคุมดูแลการติดตั้ง การใช้งานโปรแกรม รวมถึงการตั้งค่าต่างๆของคอมพิวเตอร์
- มีการตั้งค่าความปลอดภัยของเครื่องคอมพิวเตอร์อย่างเหมาะสมและมีการควบคุมไม่ให้ผู้ใช้งานได้รับสิทธิ์ในการติดตั้งโปรแกรมหรือเปลี่ยนแปลงแก้ไขค่าต่างๆ ที่เกี่ยวข้องกับการรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ด้วยตนเอง

<u>ข้อสังเกต</u>: แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน โดยโครงการใน Phase 2 ปี 2557 ธปท. จะศึกษาจัดทำแนวปฏิบัติที่ยอมรับได้ (Acceptable Practices) และประเมิน Gap ร่วมกับ ธพ. แต่ละแห่ง เพื่อเป็นแนวทางให้ ธปท. และ ธพ. ร่วมกันพิจารณาความเหมาะสมของการจัดทำแผนพัฒนาปรับปรุงระบบ IT ของตนเองให้ได้ตามมาตรฐานสากล ทั้งในระยะสั้นและระยะยาวต่อไป

2.4.2 ATM Application Control

2.4.2.1 การควบคุมการบันทึกข้อมูลเข้าสู่ระบบ (Input Validation)

<u>วัตถุประสงค์</u> เพื่อให้ข้อมูลเข้าสู่ระบบมีความครบถ้วนถูกต้อง

<u>แนวปฏิบัติที่ดี</u>

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

2.4.2.2 การควบคุมข้อมูลขณะประมวลผล (Processing Control)

<u>วัตถุประสงค์</u> เพื่อให้การประมวลผลข้อมูลมีความครบถ้วนถูกต้อง

<u>แนวปฏิบัติที่ดี</u>

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

2.4.2.3 การควบคุมการนำข้อมูลออกจากระบบ (Output Control)

<u>วัตถุประสงค์</u> เพื่อให้ข้อมูลออกจากระบบมีความครบถ้วนถูกต้อง

<u>แนวปฏิบัติที่ดี</u>

- 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 โดยโครงการใน Phase 2 ปี 2557 ธปท. จะศึกษาจัดทำแนวปฏิบัติที่ยอมรับได้ (Acceptable Practices) และประเมิน Gap ร่วมกับ ธพ. แต่ละแห่ง เพื่อเป็นแนวทางให้ ธปท. และ ธพ. ร่วมกันพิจารณาความเหมาะสมของการจัดทำแผนพัฒนาปรับปรุงระบบ IT ของตนเองให้ได้ตามมาตรฐานสากล ทั้งในระยะสั้นและระยะยาวต่อไป

2.4.3 ตู้ Automatic Teller Machine (ATM)

2.4.3.1 ATM Security Control

<u>วัตถุประสงค์</u> 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 ควรมีการควบคุมการปฏิบัติงานที่เกี่ยวข้องกับส่วนสำคัญต่างๆ ของตู้ อย่างรัดกุมเพียงพอและเป็นไปตามหลัก Dual Control โดยจำกัดเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น โดยครอบคลุม
    - การเข้าถึงและปฏิบัติงานผ่านหน้าจอ Console ของตู้ ATM
    - การเข้าถึงกล่องเงินสด กล่องรับบัตร Reject อุปกรณ์เครือข่ายสื่อสาร สายไฟ อุปกรณ์ UPS (ถ้ามี)
    - การบำรุงรักษาและซ่อมแซมตู้ทางกายภาพ
- มีการแบ่งแยกหน้าที่ต่างๆของบุคคลากรที่มีหน้าที่ในการดูแลรักษาระบบ โดยครอบคลุมหน้าที่ดังต่อไปนี้
    - การดำเนินงานทั่วไป ได้แก่ การเติมเงินหรือเอาเงินออกจากตู้ ,การเติมกระดาษ ,การเก็บบัตรคงค้างในตู้ 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 ปรับปรุงแก้ไขต่างๆ 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

<u>ข้อสังเกต</u>: แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน โดยโครงการใน Phase 2 ปี 2557 ธปท. จะศึกษาจัดทำแนวปฏิบัติที่ยอมรับได้ (Acceptable Practices) และประเมิน Gap ร่วมกับ ธพ. แต่ละแห่ง เพื่อเป็นแนวทางให้ ธปท. และ ธพ. ร่วมกันพิจารณาความเหมาะสมของการจัดทำแผนพัฒนาปรับปรุงระบบ IT ของตนเองให้ได้ตามมาตรฐานสากล ทั้งในระยะสั้นและระยะยาวต่อไป

2.4.4 อุปกรณ์ Hardware Security Machine (HSM)

2.4.4.1 HSM Security Control

<u>วัตถุประสงค์</u> เพื่อให้การปฏิบัติงานกับเครื่อง HSM ซึ่งใช้เป็นส่วนสำคัญในการพิสูจน์ตัวตนของลูกค้ามีความรัดกุมปลอดภัยสูงสุด

<u>แนวปฏิบัติที่ดี</u>

- มีการระบุตัวตนและพิสูจน์ตัวตนของผู้เข้าใช้ระบบ HSM โดยอาศัยหลักการ Dual Control และ Split Knowledge โดยจำกัดให้เฉพาะบุคคลที่ได้รับมอบอำนาจเท่านั้นที่สามารถเข้าถึงได้โดยการพิสูจน์ตัวตน จะต้องทำที่หน้า 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

<u>ข้อสังเกต</u>: แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน โดยโครงการใน Phase 2 ปี 2557 ธปท. จะศึกษาจัดทำแนวปฏิบัติที่ยอมรับได้ (Acceptable Practices) และประเมิน Gap ร่วมกับ ธพ. แต่ละแห่ง เพื่อเป็นแนวทางให้ ธปท. และ ธพ. ร่วมกันพิจารณาความเหมาะสมของการจัดทำแผนพัฒนาปรับปรุงระบบ IT ของตนเองให้ได้ตามมาตรฐานสากล ทั้งในระยะสั้นและระยะยาวต่อไป

2.4.5 Internet Banking Application Control

2.4.5.1 การควบคุมการบันทึกข้อมูลเข้าสู่ระบบ (Input Validation)

<u>วัตถุประสงค์</u> เพื่อให้ข้อมูลเข้าสู่ระบบมีความครบถ้วนถูกต้อง

<u>แนวปฏิบัติที่ดี</u>

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

2.4.5.2 การควบคุมข้อมูลขณะประมวลผล (Processing Control)

<u>วัตถุประสงค์</u> เพื่อให้การประมวลผลข้อมูลมีความครบถ้วนถูกต้อง

<u>แนวปฏิบัติที่ดี</u>

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

2.4.5.3 การควบคุมการนำข้อมูลออกจากระบบ (Output Control)

<u>วัตถุประสงค์</u> เพื่อให้ข้อมูลออกจากระบบมีความครบถ้วนถูกต้อง

<u>แนวปฏิบัติที่ดี</u>

- 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 โดยโครงการใน Phase 2 ปี 2557 ธปท. จะศึกษาจัดทำแนวปฏิบัติที่ยอมรับได้ (Acceptable Practices) และประเมิน Gap ร่วมกับ ธพ. แต่ละแห่ง เพื่อเป็นแนวทางให้ ธปท. และ ธพ. ร่วมกันพิจารณาความเหมาะสมของการจัดทำแผนพัฒนาปรับปรุงระบบ IT ของตนเองให้ได้ตามมาตรฐานสากล ทั้งในระยะสั้นและระยะยาวต่อไป

2.4.6 Internet Banking Security

2.4.6.1 System Security

<u>วัตถุประสงค์</u> 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 หรือเมื่อมีภัยใหม่ๆ และมีการปรับปรุงแก้ไข Application หรือเพิ่มการควบคุมที่จำเป็นอย่างทันท่วงที

[8] OWASP หรือ The Open Web Application Security Project เป็นองค์กรที่จัดตั้งโดยไม่แสวงหาผลกำไรเพื่อศึกษาและเก็บข้อมูลภัยคุกคามที่เกิดขึ้นทางInternet รูปแบบใหม่ ๆ

2.4.6.2 Access Control

<u>วัตถุประสงค์</u> เพื่อให้มั่นใจว่าระบบงาน Internet Banking มีการป้องกันการเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต

<u>แนวปฏิบัติที่ดี</u>

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

2.4.6.3 Application Security

<u>วัตถุประสงค์</u> 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 โดยอย่างน้อยให้มีการควบคุมที่ลดความเสี่ยงจาก Man-in-the-Middle Attack และ Man-in-the-Browser Attack
- มีการควบคุมไม่ให้มีการเก็บข้อมูลที่สำคัญของลูกค้าไว้ใน Session และมีการสร้าง Session Key ใหม่เมื่อมีการเปลี่ยนหน้า/ขั้นตอนการทำรายการ
- มีการตรวจสอบลำดับของขั้นตอนการทำธุรกรรมอย่างเหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีสามารถข้ามขั้นตอนใดขั้นตอนหนึ่งได้ หากพบว่ามีการกระทำดังกล่าว 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 โดยไม่สามารถใช้กับรายการธุรกรรมอื่นๆได้ 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

<u>ข้อสังเกต</u>: แนวปฏิบัติข้างต้นเป็นแนวปฏิบัติที่ดีตามมาตรฐานสากล อย่างไรก็ตาม ธพ. แต่ละแห่งมีนโยบายการทำธุรกิจ แผนการลงทุนด้าน IT ปริมาณธุรกรรม และผลกระทบในเชิงธุรกิจแตกต่างกัน โดยโครงการใน Phase 2 ปี 2557 ธปท. จะศึกษาจัดทำแนวปฏิบัติที่ยอมรับได้ (Acceptable Practices) และประเมิน Gap ร่วมกับ ธพ. แต่ละแห่ง เพื่อเป็นแนวทางให้ ธปท. และ ธพ. ร่วมกันพิจารณาความเหมาะสมของการจัดทำแผนพัฒนาปรับปรุงระบบ IT ของตนเองให้ได้ตามมาตรฐานสากล ทั้งในระยะสั้นและระยะยาวต่อไป

[9] OTP หรือ One Time Password คือ รหัสผ่านที่ใช้เพียงครั้งเดียวสำหรับยืนยันการทำธุรกรรมผ่านทางInternet/Mobile Banking

ธนาคารแห่งประเทศไทย

เพื่อความเป็นอยู่ที่ดี อย่างยั่งยืนของไทย