ธนาคารแห่งประเทศไทย

แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices)

Phase 2: ธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์

การให้บริการการเงินและการชำระเงินทางอิเล็กทรอนิกส์

(E-Banking และ E-Payment)

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ
สายกำกับสถาบันการเงิน
ธันวาคม 2557

สารบัญ

Executive Summary

ที่มาและเหตุผลความจำเป็น

ระบบเทคโนโลยีสารสนเทศ (IT) นับเป็นโครงสร้างพื้นฐานสำคัญที่ใช้รองรับกลยุทธ์และกระบวนการดำเนินธุรกิจด้านต่าง ๆ (Business Process) ของธนาคารพาณิชย์ (ธพ.) จุดอ่อนหรือช่องโหว่ของระบบ IT อาจมีผลต่อความปลอดภัย ความถูกต้องและความต่อเนื่องในการให้บริการทางการเงินแก่ลูกค้าประชาชน อีกทั้งอาจส่งผลกระทบต่อภาพลักษณ์และความน่าเชื่อถือของ ธพ. แต่ละแห่งหรือระบบสถาบันการเงินโดยรวม ธปท. จึงได้จัดให้มีโครงการจัดทำแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยง (IT Best Practices) ด้าน Operational /IT Risk Management ของ ธพ. ที่เชื่อมโยงกับธุรกิจหลัก โดยมุ่งเน้นธุรกรรมที่มีผลกระทบต่อประชาชน ในวงกว้าง เพื่อให้ ธพ. สามารถนำไปใช้เป็นแนวทางในการควบคุมความเสี่ยงตนเอง (Self Control System) และพัฒนาโครงสร้างพื้นฐานระบบ IT พร้อมรองรับกลยุทธ์การขยายธุรกิจในอนาคต ตลอดจนใช้ในการพัฒนาการกำกับดูแลสถาบันการเงินของ ธปท. ให้ทันกับวิวัฒนาการและความเสี่ยงที่เปลี่ยนแปลงที่เกิดขึ้น โดยในปี 2556 ได้จัดทำ IT Best Practices Phase 1 ครอบคลุมธุรกิจด้านเงินฝาก ถอน และโอนเงินเสร็จไปแล้ว

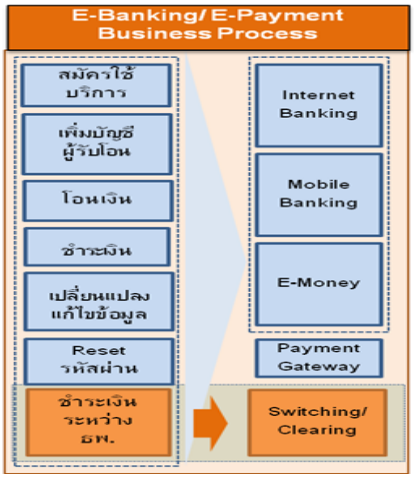
ในปี 2557 โครงการ IT Best Practices Phase 2 นี้ ธปท. ได้เล็งเห็นถึงการขยายตัวของธุรกิจการให้บริการการเงินและการชำระเงินทางอิเล็กทรอนิกส์ (E-Banking และ E-Payment) โดยเฉพาะสำหรับลูกค้ารายย่อย ซึ่งได้รับความนิยมสูงขึ้นอย่างยิ่งในประเทศไทย และตระหนักดีว่าความมั่นคงปลอดภัยของการให้บริการการเงินและการชำระเงินทางอิเล็กทรอนิกส์ เป็นปัจจัยสำคัญที่จะสร้างความเชื่อมั่นให้กับผู้ใช้บริการ และทำให้การพัฒนาธุรกรรมทางการเงินผ่านช่องทางอิเล็กทรอนิกส์ของ ธพ. มีความยั่งยืน อย่างไรก็ตามความเสี่ยงที่เกิดจากภัยคุกคามต่าง ๆ ผ่านช่องทางอิเล็กทรอนิกส์ นอกจากจะมีแนวโน้มเพิ่มขึ้นแล้ว ยังมีการใช้เทคโนโลยีที่มีวิวัฒนาการสูงขึ้น มีการกระทำทุจริตด้วยวิธีการที่ซับซ้อนและเป็นขบวนการข้ามชาติ โดยสามารถแบ่งประเภทของภัยคุกคามผ่านช่องทางอิเล็กทรอนิกส์ได้เป็น 2 รูปแบบ คือ

1) **ภัยคุกคามแบบ Non-Technical** เช่น การปลอมแปลงเอกสารเพื่อสมัครใช้บริการช่องทางอิเล็กทรอนิกส์ หรือการลักลอบ หรือหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลส่วนตัวของผู้ใช้บริการ เป็นต้น

2) **ภัยคุกคามแบบ Technical** เช่น การแพร่กระจายของ Malware ไปยังเครื่องคอมพิวเตอร์เพื่อจะขโมยข้อมูลสำคัญ หรือสร้างความเสียหายให้กับระบบคอมพิวเตอร์ การสร้างและเผยแพร่ Mobile Banking Application เลียนแบบของธนาคาร เป็นต้น

แนวทางการจัดทำแนวปฏิบัติที่ดี (IT Best Practices Phase 2)

ด้วยเหตุผลที่กล่าว ธปท. จึงได้จัดทำ IT Best Practices ต่อเนื่องจาก Phase 1 โดยขยายให้ครอบคลุมไปถึงธุรกรรม E-Banking และ E-Payment เพื่อสนับสนุนการพัฒนาระบบการให้บริการการเงินและการชำระเงินทางอิเล็กทรอนิกส์ของประเทศให้มีการควบคุมความเสี่ยงที่สอดคล้องกับแนวปฏิบัติที่เป็นมาตรฐานสากล อันจะช่วยเสริมสร้างให้เกิดความก้าวหน้าอย่างมั่นคงต่อไป



รูปที่ 1 : ขอบเขตของการให้บริการทางอิเล็กทรอนิกส์

การจัดทำ IT Best Practices Phase 2 ฉบับนี้ยังคงยึดหลักการเดียวกันกับ IT Best Practice Phase 1 ซึ่งเริ่มจากการทำความเข้าใจในกระบวนการทางธุรกิจ (Business Process) ที่เกี่ยวข้องกับการทำธุรกรรมการเงินทางอิเล็กทรอนิกส์ รวมทั้งโครงสร้างและกระบวนการของระบบ IT (IT Process) ที่สนับสนุนธุรกิจดังกล่าว เพื่อนำมาประเมินความเสี่ยงตามมาตรฐานสากลและสอดคล้องกับหลักการตรวจสอบด้าน IT (Security Integrity และ Availability : S-I-A) รวมถึงความเสี่ยงด้านภัยคุกคามทางไซเบอร์ และกำหนดแนวปฏิบัติที่ดีสำหรับกระบวนการทางธุรกิจและระบบ IT ที่รองรับการทำธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์

สาระของ IT Best Practices Phase 2 แบ่งเป็น 2 ส่วน คือ

1. แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของกระบวนการการทำธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์ ซึ่งได้มีการศึกษาและทำความเข้าใจ Business Process และความเสี่ยงที่เกี่ยวข้องของธุรกิจการให้บริการ E-Banking และ E-Payment เพื่อระบุจุดที่เป็นความเสี่ยง และกำหนดการควบคุมที่ดีตามกรอบหลักการที่สอดคล้องตามกฎหมายและมาตรฐานสากลที่เกี่ยวข้อง เช่น มาตรฐาน GTAC[1] เป็นต้น โดยครอบคลุมบริการทางการเงินผ่านช่องทางอิเล็กทรอนิกส์ ดังนี้

- **การให้บริการ E-Banking : Internet Banking/ Mobile Banking** ได้แก่ กระบวนการสมัคร การทำธุรกรรมและการเปลี่ยนแปลงข้อมูลสำคัญผ่านบริการ Internet Banking/ Mobile Banking

- **การให้บริการการชำระเงินทางอิเล็กทรอนิกส์ (E-Payment)** ได้แก่ บริการเงินอิเล็กทรอนิกส์ (e-Money) บริการรับชำระการซื้อสินค้าและบริการผ่านร้านค้า e-commerce (Payment Gateway) และบริการชำระเงินระหว่างธนาคาร (Switching /Clearing)

2. แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบ IT ที่รองรับธุรกรรมทางอิเล็กทรอนิกส์ เนื่องจากระบบ IT ที่ใช้รองรับธุรกิจบริการ E-Banking และ E-Payment มีการเชื่อมโยงสู่ภายนอกโดยใช้โครงข่ายสาธารณะ จึงมีความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Threats) ซึ่งมีแนวโน้มเพิ่มสูงขึ้น อาจก่อให้เกิดความเสียหายและมีผลกระทบต่อความเชื่อมั่นของผู้ใช้บริการค่อนข้างมาก

ธปท. จึงได้จัดทำกรอบแนวปฏิบัติที่ดีสำหรับการบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่สอดคล้องตามกรอบแนวทางมาตรฐานสากล เช่น Cybersecurity Framework ที่จัดทำโดยสถาบัน National Institute of Standards and Technology, USA เป็นต้น เพื่อให้ ธพ. นำไปใช้เป็นแนวทางในการปรับปรุงการกำกับดูแล ระบบการบริหารความเสี่ยงด้าน IT และการรักษาความปลอดภัยของการให้บริการผ่านช่องทางอิเล็กทรอนิกส์อย่างรัดกุมและเป็นมาตรฐาน รวมถึงมีความพร้อมในการรับมือกับความเสี่ยงด้านภัยคุกคามทางไซเบอร์ได้ดียิ่งขึ้น ซึ่งแบ่งออกเป็น 3 ระดับดังนี้

รูปที่ 2: แนวปฏิบัติที่ดีสำหรับการบริหารจัดการภัยคุกคามทางไซเบอร

นอกจากหลักการบริหารจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ข้างต้นแล้ว ยังมีแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบ IT ที่สนับสนุนบริการ E-Banking และ E-Payment ซึ่งประกอบด้วยศูนย์คอมพิวเตอร์ ระบบ Internet Banking ระบบ Core

[1] *Global Technology Audit Guide (GTAG) เป็นกรอบแนวทางการตรวจสอบเทคโนโลยีสารสนเทศของหน่วยงาน Institute of Internal Auditors (IIA) ซึ่งเป็นองค์กรวิชาชีพการตรวจสอบภายใน*

Banking และระบบเครือข่ายสื่อสาร ซึ่งได้กำหนดไว้แล้วใน IT Best Practices Phase 1 และเพื่อให้เกิดความเข้าใจอย่างต่อเนื่องและสะดวกในการนำไปใช้งาน จึงได้นำแนวปฏิบัติที่ดีของ Phase 1 เรื่อง Internet Banking มารวมไว้ในฉบับนี้ด้วย

อย่างไรก็ดี **ธพ. สามารถนำแนวปฏิบัติที่ดีของ Phase 1 ในเรื่องอื่น ๆ ที่อาจเกี่ยวข้องมาประยุกต์ใช้ตามความเหมาะสม**

ประโยชน์ของการจัดทำ IT Best Practices

ธปท. มุ่งหวังให้ IT Best Practices Phase 1 และ 2 เกิดประโยชน์ในวงกว้าง โดย ธพ. สามารถนำแนวปฏิบัติที่ดีนี้ไปประเมินความเสี่ยงและการควบคุมด้วยตนเอง (Self Control System) ตลอดจนการนำไปใช้เป็น benchmark เพื่อการพัฒนาปรับปรุงระบบ IT ให้มีความปลอดภัย ความถูกต้องและความพร้อมใช้งานเทียบเคียงแนวปฏิบัติที่เป็นมาตรฐานสากล รวมถึงพร้อมรองรับการขยายธุรกิจและสามารถเพิ่มประสิทธิภาพในการให้บริการทางการเงินแก่ลูกค้าประชาชน ตลอดจนเพิ่มศักยภาพทางการแข่งขันให้เทียบเคียงกับ ธพ. ต่างประเทศพร้อมก้าวสู่ประชาคมเศรษฐกิจอาเซียนหรือ AEC รวมทั้งยังเป็นประโยชน์กับหน่วยงานตรวจสอบภายในด้าน IT ของ ธพ. ในการนำ IT Best Practices ไปใช้เป็นแนวทางในการตรวจสอบได้ตามความเหมาะสมกับแต่ละแห่ง

นอกจากนี้ IT Best Practices ยังสามารถนำมาใช้พัฒนาแนวทางการตรวจสอบด้าน IT ของ ธปท. ให้มีความทันสมัยและสอดคล้องกับมาตรฐานสากล และเพื่อให้การนำ IT Best Practices ไปใช้ เกิดความสัมฤทธิ์ผลในทางปฏิบัติ ธปท. และ ธพ. จึงควรพัฒนาบุคลากรที่เกี่ยวข้องด้าน IT ให้มีความรู้ความเข้าใจ IT Best Practices เพื่อช่วยกันผลักดันให้ ธพ. มีการพัฒนาระบบ IT ที่สอดคล้องกับมาตรฐานสากล และยกระดับโครงสร้างพื้นฐานระบบ IT ของ ธพ.ไทย ทั้งระบบให้ได้มาตรฐานสากลมากยิ่งขึ้น

อนึ่ง แนวปฏิบัติการควบคุมภายในที่ดี จำเป็นที่จะต้องมีการปรับปรุงให้มีความทันสมัยอย่างต่อเนื่องเพื่อให้เหมาะสมกับเทคโนโลยี รูปแบบบริการทางการเงินใหม่ ๆ รวมถึงความเสี่ยงที่มีการเปลี่ยนแปลงและพัฒนาอย่างรวดเร็ว พร้อมทั้งคำนึงถึงความเหมาะสมกับลักษณะธุรกิจและบริการของ ธพ. ไทย ซึ่งอาจมีความแตกต่าง และอาจยังไม่ครอบคลุมผลิตภัณฑ์และบริการการเงินประเภทอื่นของ ธพ. ธปท. จะต้องพัฒนา ทบทวน และปรับปรุง IT Best Practices อย่างต่อเนื่อง (Dynamic Process) เพื่อให้มีความเหมาะสมและทันกับการเปลี่ยนแปลงของเทคโนโลยีและบริการทางการเงินรูปแบบใหม่ รวมถึงภัยคุกคามด้านไซเบอร์ที่ซับซ้อนยิ่งขึ้น

สรุปกระบวนการในการจัดทำแนวปฏิบัติที่ดี (IT Best Practices) Phase 2

1. การกำหนดขอบเขตการจัดทำแนวปฏิบัติที่ดี

ครอบคลุมกระบวนการทำธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์สำหรับลูกค้ารายย่อยเป็นหลัก ดังต่อไปนี้

(1) การให้บริการธุรกรรมผ่านทาง Internet Banking

(2) การให้บริการธุรกรรมผ่านทาง Mobile Banking

(3) การให้บริการธุรกรรมด้วยบัตรเงินอิเล็กทรอนิกส์ (e-Money) ทั้งประเภท Card และ Non-card

(4) การรับชำระการซื้อสินค้าและบริการผ่านร้านค้า E-Commerce (Payment Gateway)

(5) การให้บริการ Switching/ Clearing รายการชำระเงินระหว่างธนาคาร

ซึ่ง ธปท. ได้ว่าจ้างที่ปรึกษาจากบริษัท Deloitte ทำหน้าที่ให้คำปรึกษาแก่ ธปท. ในทุกกระบวนการจัดทำแนวปฏิบัติที่ดีฉบับนี้

2. การเตรียมความพร้อมผู้ตรวจสอบ ธปท.

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

3. การรวบรวมข้อมูล เพื่อจัดทำแนวปฏิบัติที่ดี

ศึกษาและรวบรวมข้อมูลกระบวนการทางธุรกิจที่ครอบคลุมการทำธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์ในลักษณะ End-to-End Process ของ ธพ. ไทย รวมถึง Non Bank (ผู้ให้บริการ Payment Switching & Clearing)

4. การยกร่างแนวปฏิบัติที่ดี

การยกร่างแนวปฏิบัติที่ดีจัดทำโดยคณะทำงานภายใน ธปท. ประกอบด้วย ฝ่ายตรวจสอบความเสี่ยง ฝ่ายเทคโนโลยีสารสนเทศ และที่ปรึกษา โดยมีการนำข้อมูลที่รวบรวมได้จากข้อ 3 มาประมวลผลและวิเคราะห์เพื่อจัดทำ

- Business Process Flows และ IT Process Flows ของกระบวนการให้บริการธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์ เพื่อเป็น Benchmark ของระบบ ธพ. ไทย
- ร่างแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงครอบคลุมกระบวนการทำธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์ โดยอ้างอิงตามกรอบมาตรฐานสากลดังนี้

  (1) พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551

  (2) มาตรฐานของ The Committee of Sponsoring Organizations of the Tread way Commission (COSO) ซึ่งเป็นคณะกรรมการที่จัดทำแนวปฏิบัติด้านการบริหารความเสี่ยงองค์กร (Enterprise Risk Management : ERM) การควบคุมภายใน และการป้องกันทุจริตที่ได้รับการยอมรับในระดับสากล

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

(4) Control Objectives for Information and Related Technology (COBIT) หรือกรอบการบริหารจัดการด้านเทคโนโลยีสารสนเทศของหน่วยงาน The Information Systems Audit and Control Association (ISACA) ซึ่งเป็นองค์กรระดับสากลที่มุ่งพัฒนาความรู้และการปฏิบัติงานที่ดีด้านเทคโนโลยีสารสนเทศ

(5) ISO27001 (Information Security) ซึ่งเป็นกรอบการควบคุมด้านความปลอดภัยเทคโนโลยีสารสนเทศของหน่วยงาน International Organization for Standardization (ISO) หรือองค์กรมาตรฐานสากลซึ่งเป็นองค์กรระหว่างประเทศ ทำหน้าที่กำหนดมาตรฐานสากลต่าง ๆ ที่เกี่ยวข้องกับธุรกิจ และอุตสาหกรรม รวมทั้งมาตรฐานด้านเทคโนโลยีสารสนเทศด้วย

(6) ISO27032:2012 (Information Technology Security Techniques-Guidelines for Cyber Security) เป็นมาตรฐานด้านความปลอดภัยของ Cyber Security

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

(8) กรอบแนวทางการรักษาความปลอดภัยทางไซเบอร์ (Cybersecurity Framework) โดย National Institute of Standards and Technology : NIST ซึ่งเป็นสถาบันมาตรฐานเทคโนโลยีสารสนเทศแห่งชาติของสหรัฐอเมริกา ที่พัฒนามาตรฐานด้านเทคโนโลยีต่าง ๆ จัดทำและเผยแพร่ เพื่อเสริมสร้างมาตรฐานความมั่นคงปลอดภัยทางด้านเทคนิค

5. การ Finalize แนวปฏิบัติที่ดีฉบับนี้

ธปท. ได้ปรับปรุงร่างแนวปฏิบัติที่ดีฉบับนี้ ตามความเห็นที่ได้รับจาก ธพ. ให้มีความเหมาะสม ชัดเจน สามารถนำไปปฏิบัติจริง และสอดคล้องกับมาตรฐานสากล ซึ่ง ธปท. ได้ร่วมกับที่ปรึกษาจากบริษัท Deloitte ได้สรุปความเห็นว่า แนวปฏิบัติที่ดีฉบับนี้ มีมาตรฐานสอดคล้องกับมาตรฐานสากล และ/หรือมาตรฐานของธนาคารชั้นนำในกลุ่มประเทศอาเซียน

ส่วนที่ 1
แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยง ของกระบวนการทำธุรกิจหลัก

Phase 2 : ธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์
การให้บริการการเงินและการชำระเงินทางอิเล็กทรอนิกส์ (E-Banking และ E-Payment)

แนวทางการจัดทำแนวปฏิบัติที่ดี (IT Best Practices) Phase 2

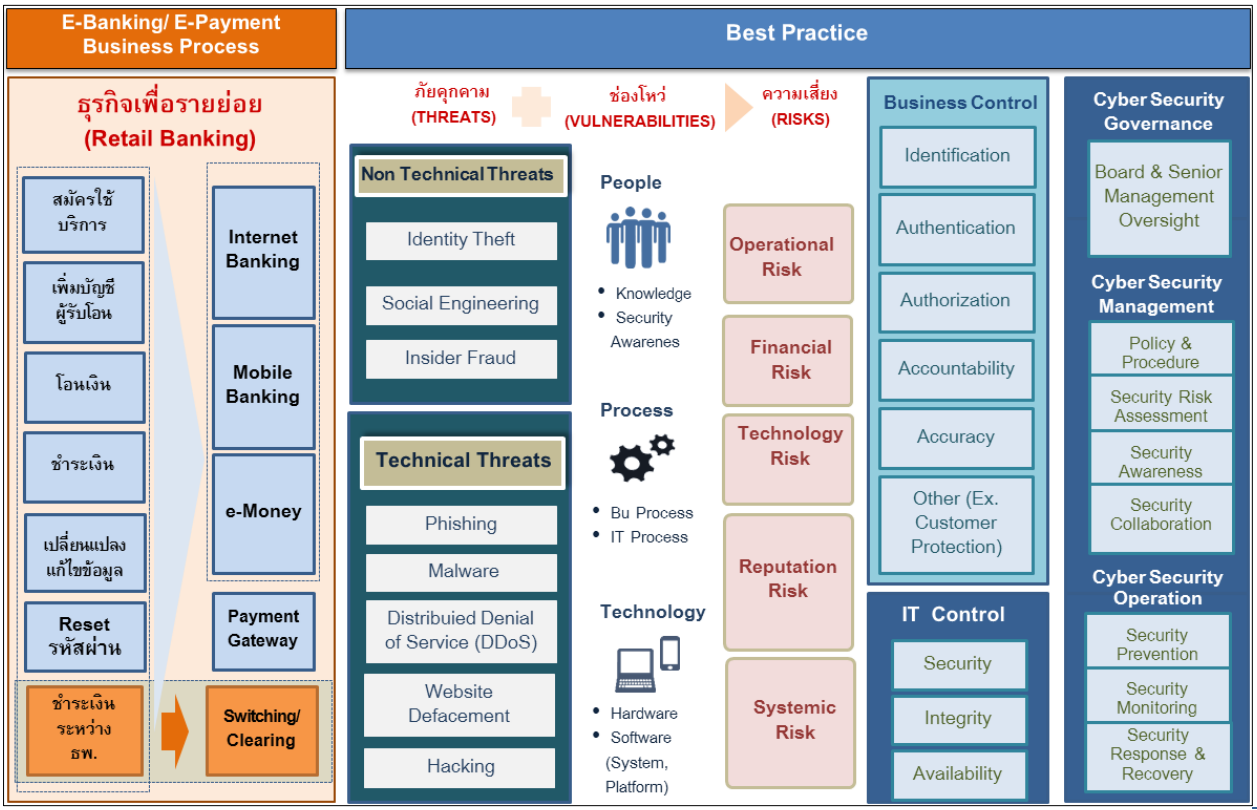
ในปัจจุบัน บริการทางการเงินผ่านช่องทางอิเล็กทรอนิกส์เริ่มได้รับความนิยมและมีการใช้บริการกันอย่างแพร่หลาย และมีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง ธนาคารพาณิชย์ไทยหลายแห่งจึงมีการปรับกลยุทธ์ขยายการให้บริการผ่านช่องทางอิเล็กทรอนิกส์เพิ่มมากขึ้น เพื่อที่จะสามารถเข้าถึงกลุ่มลูกค้าได้มากขึ้นและยังเป็นการช่วยลดต้นทุนด้านการบริการอีกด้วย อย่างไรก็ตาม แม้ว่าการทำธุรกรรมผ่านช่องทางอิเล็กทรอนิกส์จะมีความสะดวกสบายและรวดเร็ว แต่ก็แฝงไว้ซึ่งภัยคุกคามที่มีแนวโน้มสูงขึ้น จากการที่มีผู้ไม่ประสงค์ดีที่อาศัยช่องโหว่หรือจุดอ่อนทั้งจากคน กระบวนการ หรือเทคโนโลยี ที่ขาดการควบคุมที่ดีเพียงพอ ทำให้ระบบงานและผู้ใช้บริการเกิดความเสียหาย ส่งผลกระทบต่อความเชื่อมั่นที่มีต่อระบบการให้บริการของธนาคาร โดยสามารถแบ่งประเภทของภัยคุกคามที่เกิดได้เป็น 2 รูปแบบ คือ

1) **ภัยคุกคามแบบ Non-Technical** เช่น การปลอมแปลงเอกสารเพื่อสมัครใช้บริการช่องทางอิเล็กทรอนิกส์ หรือการลักลอบหรือหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลส่วนตัวของผู้ใช้บริการ เป็นต้น

2) **ภัยคุกคามแบบ Technical** เช่น การแพร่กระจายของ Malware ไปยังเครื่องคอมพิวเตอร์เพื่อทำการขโมยข้อมูลสำคัญหรือสร้างความเสียหายให้กับระบบคอมพิวเตอร์ การสร้าง Mobile Banking Application เลียนแบบของธนาคาร เป็นต้น

ดังนั้นธนาคารพาณิชย์ในฐานะผู้ให้บริการ ซึ่งมีความพร้อมในด้านทักษะความรู้และเทคโนโลยี จึงจำเป็นที่จะต้องจัดให้มีระบบการควบคุมและรักษาความปลอดภัยของการให้บริการผ่านช่องทางอิเล็กทรอนิกส์ที่รัดกุมและสอดคล้องกับแนวทางตามมาตรฐานสากลทั้งด้านกระบวนการให้บริการทางธุรกิจ (Business Process) และด้านโครงสร้างระบบ IT (IT Process) ที่ใช้รองรับบริการทางการเงินและการชำระเงินผ่านช่องทางอิเล็กทรอนิกส์ ตลอดถึงกระบวนการกำกับดูแลและการบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ ดังรูป

กรอบแนวคิดในการจัดทำ IT Best Practices Phase 2 รองรับธุรกรรม E-Banking & E-Payment



ตารางกรอบแนวทางการควบคุมความเสี่ยงของการให้บริการการเงินและการชำระเงินทางอิเล็กทรอนิกส์

กรอบแนวทางการควบคุม[2]	บริการ Internet Banking*/ Mobile Banking	บริการ E-Money	บริการ Payment Gateway	บริการ Payment Switching & Clearing
1. Identification & Verification การระบุหลักฐานการแสดงตัวตนและตรวจสอบข้อมูลตัวตนของผู้สมัครใช้บริการ	✓	✓	✓[3]	–
2. Authorization การกำหนดสิทธิเฉพาะที่ได้รับอนุญาตในการเข้าใช้งานระบบ	✓	✓	✓	–
3. Authentication การพิสูจน์ตัวตนการเข้าใช้บริการชำระเงินทางอิเล็กทรอนิกส์ด้วยวิธีที่มีความปลอดภัย	✓	✓	✓	–
4. Accountability การระบุความรับผิดชอบต่อการทำรายการที่ชัดเจน เพื่อป้องกันการปฏิเสธการทำรายการ (Non-Repudiation) และการจัดเก็บร่องรอยการทำธุรกรรม เพื่อสามารถใช้ในการตรวจสอบและยืนยันผู้ทำรายการ	✓	✓	✓	✓
5. Accuracy การควบคุมความถูกต้องครบถ้วนของข้อมูลรายการด้วยวิธีการที่ปลอดภัย ครอบคลุมตั้งแต่การบันทึก (Input) การประมวลผล (Process) และการแสดงผล (Output)	✓	✓	✓	✓
6. Others (Consumer Protection) ระบบและกระบวนการที่สนับสนุนช่วยเหลือผู้ใช้บริการ ได้แก่ การติดตามรายการที่น่าสงสัย หรือเหตุการณ์ทุจริต กระบวนการจัดการปัญหาและเรื่องร้องเรียนจากผู้ใช้บริการ และการให้ความรู้ที่จำเป็นในการใช้บริการอย่างปลอดภัย	✓	✓	✓	✓

***หมายเหตุ: ได้นำแนวปฏิบัติที่ดีของ IT Best Practices Phase 1 ข้อ 2.4.5 Internet Banking Application Control มากำหนดรวมอยู่ในแนวปฏิบัติที่ดีของส่วนนี้ด้วย เพื่อให้แนวปฏิบัติที่ดีของการควบคุมกระบวนการทางธุรกิจของบริการ Internet Banking มีความครอบคลุมครบถ้วน**

[2] *กรอบแนวทางการควบคุม ได้นำข้อกำหนดจาก "ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553" มาปรับใช้*

[3] *ผู้สมัครใช้บริการในส่วนของบริการ Payment Gateway หมายถึง ร้านค้า e-Commerce ควรมีการระบุหลักฐานการแสดงตัวตนและตรวจสอบข้อมูลตัวตนของร้านค้าก่อนจะให้บริการ*

การให้บริการการเงินและการชำระเงินทางอิเล็กทรอนิกส์ ครอบคลุมกระบวนการสำคัญ ดังต่อไปนี้

บริการ Internet Banking/ Mobile Banking

1. การสมัครใช้บริการ Internet banking/ Mobile banking
   - 1.1 การสมัครใช้บริการ Internet Banking/ Mobile Banking ผ่านทางสาขา
   - 1.2 การสมัครใช้บริการ Internet Banking/ Mobile Banking ผ่านทางตู้ ATM
   - 1.3 การสมัครใช้บริการ Internet Banking/ Mobile Banking ผ่านทาง Online
   - 1.4 การสมัครใช้บริการ Mobile Banking ผ่านทางโทรศัพท์มือถือ
2. การทำรายการผ่าน Internet Banking/ Mobile Banking (การโอนเงิน การชำระเงิน)
   - 2.1 การทำรายการโอนเงิน /ชำระเงิน
   - 2.2 การเพิ่มบัญชีผู้รับโอน
3. การเปลี่ยนแปลงแก้ไขข้อมูลของผู้ใช้บริการผ่านช่องทางต่าง ๆ (สาขา /Call Center/ Internet Banking) และการยกเลิกบริการ
   - 3.1 การ Reset รหัสผ่าน (ผ่านทาง Internet Banking)
   - 3.2 การ Reset รหัสผ่าน (ผ่านทาง Call Center)
   - 3.3 การเปลี่ยนแปลงแก้ไขข้อมูล (ผ่านทาง Internet Banking)
   - 3.4 การเปลี่ยนแปลงแก้ไขข้อมูล และการยกเลิกบริการ (ผ่านทางสาขา)
   - 3.5 การยกเลิกบริการ (ผ่านทาง Internet Banking)

บริการเงินอิเล็กทรอนิกส์ (e-Money)[4]

4. การสมัครใช้บริการและการทำรายการ e-Money ทั้งแบบ Card และ Non-card
   - การสมัครใช้บริการ e-Money
     - 4.1 การสมัครใช้บริการ e-Money ทั้งแบบ Card และ Non-card
   - การทำรายการ e-Money[5]
     - 4.2 การเติมเงิน e-Money แบบ Card
     - 4.3 การเติมเงิน e-Money แบบ Non-card
     - 4.4 การชำระเงิน e-Money แบบ Card
     - 4.5 การชำระเงิน e-Money แบบ Non-card
     - 4.6 การถอนเงิน e-Money ทั้งแบบ Card และ Non-card

บริการรับชำระการซื้อสินค้าและบริการผ่านร้านค้า (Payment Gateway)

5. การรับชำระการซื้อสินค้าและบริการผ่านร้านค้า e-Commerce

บริการ Switching และการหักบัญชีเพื่อชำระดุล (Switching/ Clearing)

6. บริการ Switching/ Clearing รองรับการโอนเงินรายย่อยทีละรายการและการโอนเงินครั้งละหลายรายการ
   - การทำ Switching และ Clearing การโอนเงินรายย่อยทีละรายการ (Single Payment)
     - 6.1 การ Switching การโอนเงินรายย่อยทีละรายการ
     - 6.2 การ Clearing การโอนเงินรายย่อยทีละรายการ
   - การทำ Switching และ Clearing การโอนเงินครั้งละหลายรายการ (Bulk payment)
     - 6.3 การ Switching การโอนเงินครั้งละหลายรายการ
     - 6.4 การ Clearing การโอนเงินรายย่อยครั้งละหลายรายการ

การควบคุมเพิ่มเติมที่สำคัญ

7. การควบคุมเพิ่มเติมที่สำคัญ

---

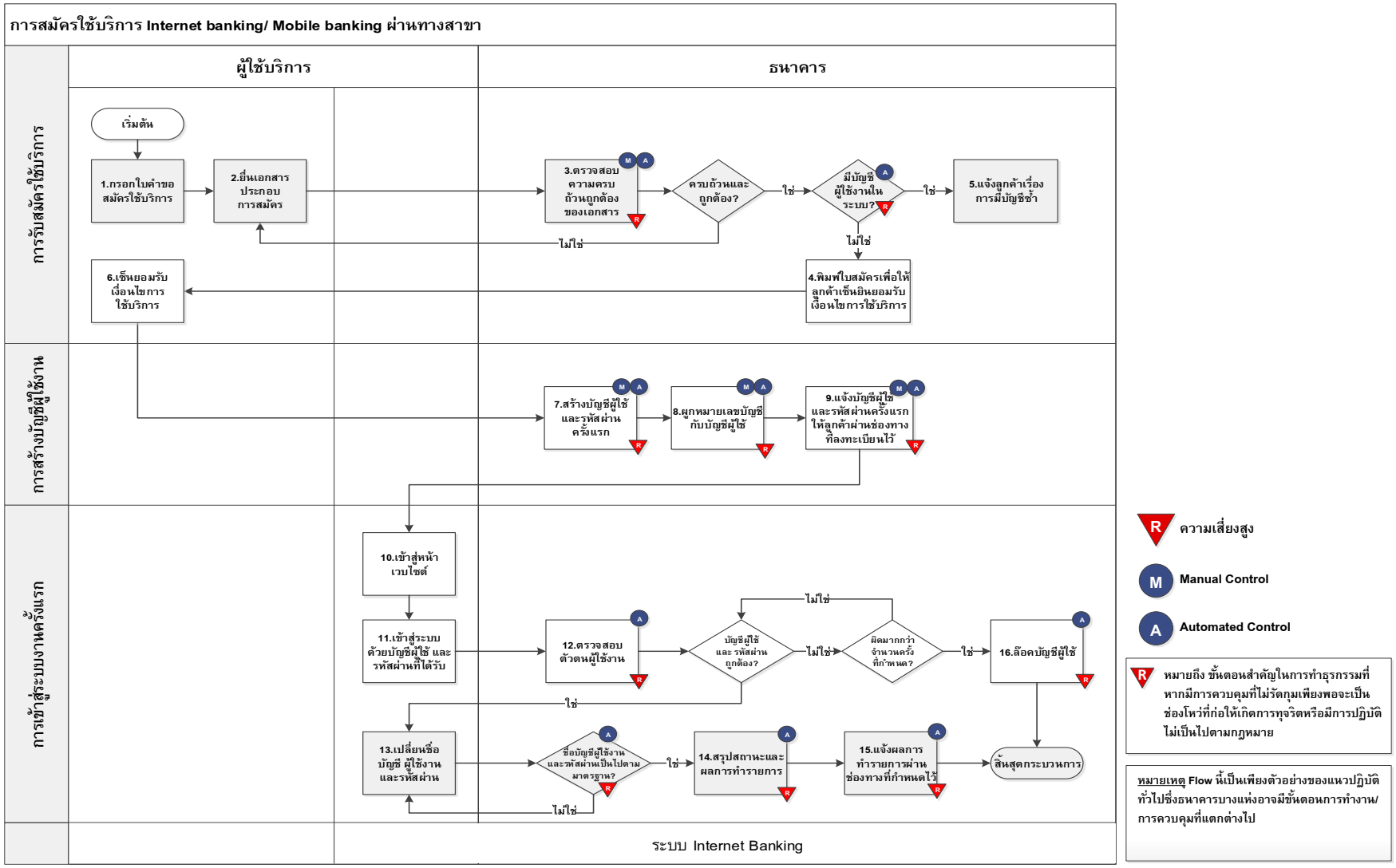
[4] *Electronic Money (e-Money) หมายถึง เงินอิเล็กทรอนิกส์ ซึ่งได้แก่ บัตรเงินอิเล็กทรอนิกส์ (Card) และสื่อการชำระเงินที่ไม่ใช่บัตร (Non-card) หรือกระเป๋าเงินอิเล็กทรอนิกส์ เช่น e-purse หรือ e-Wallet เป็นต้น*

[5] *การทำรายการชำระเงิน e-Money ไม่รวมรายการชำระซื้อสินค้าและบริการจากร้านค้าของผู้ให้บริการ e-Money คนละรายกัน*

1. การสมัครใช้บริการ Internet Banking/ Mobile Banking

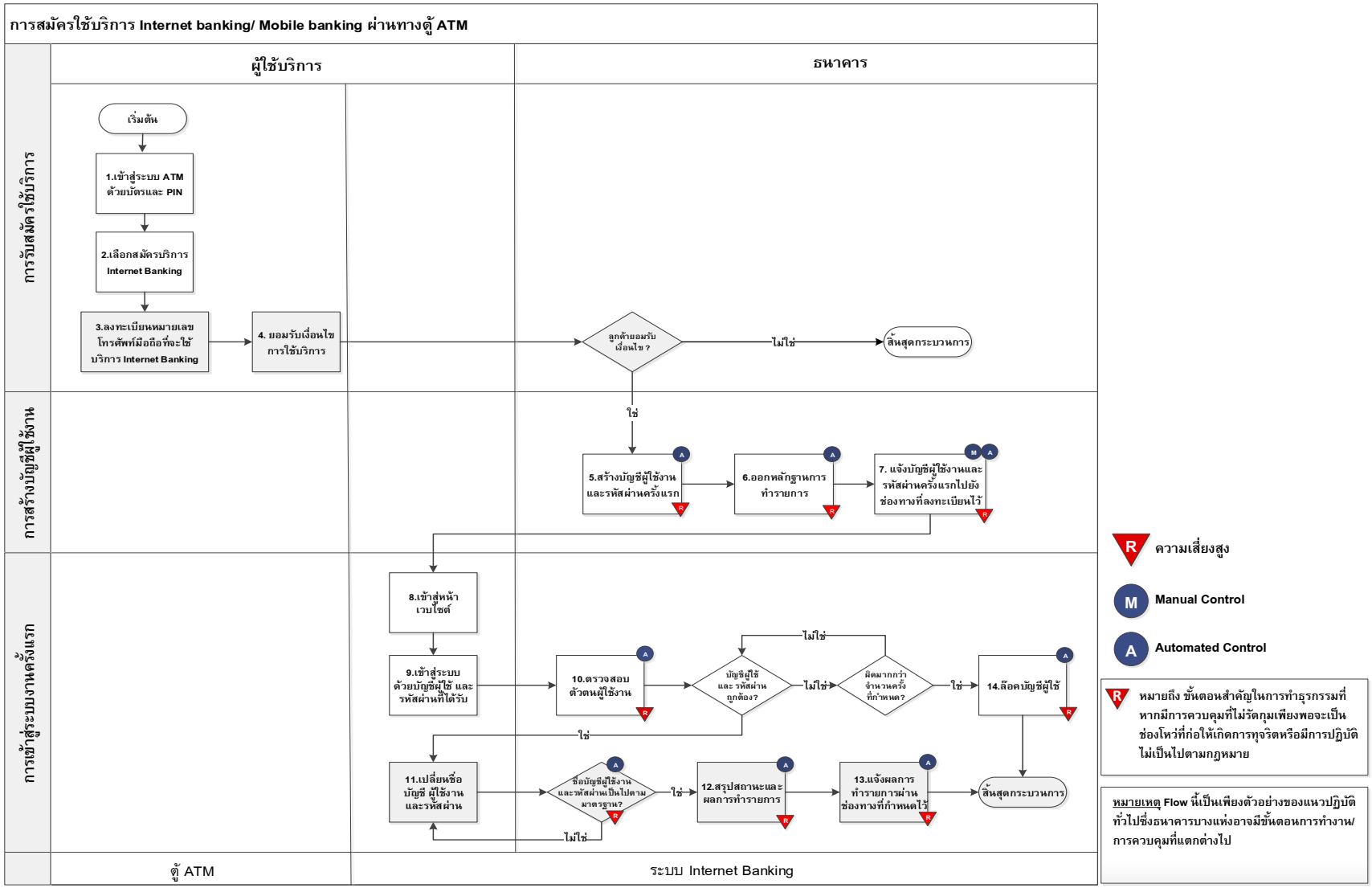
1.1 การสมัครใช้บริการ Internet Banking/ Mobile Banking ผ่านทางสาขา

ตัวอย่าง Flowchart กระบวนการทำงาน



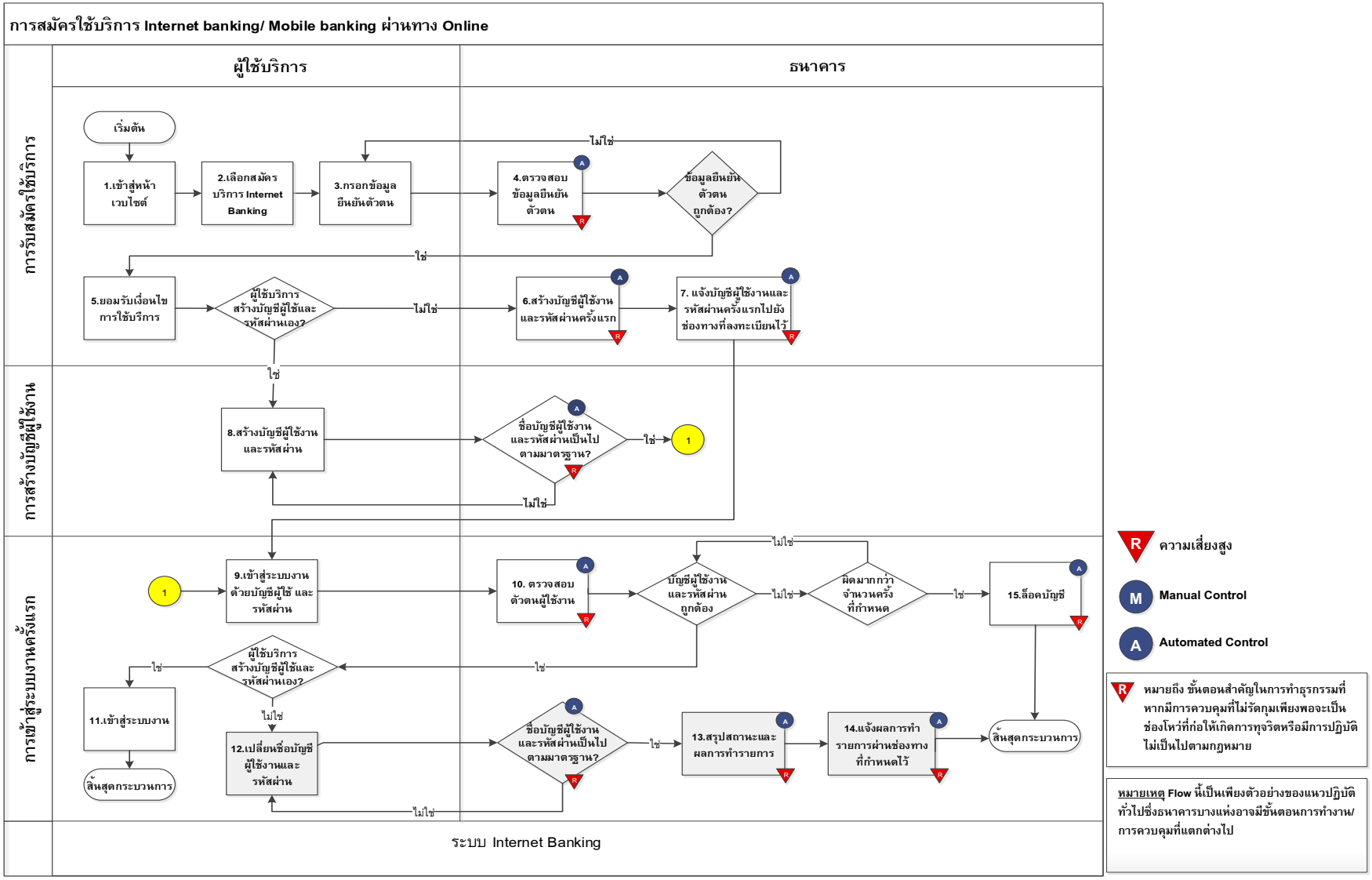
1.2 การสมัครใช้บริการ Internet Banking/ Mobile Banking ผ่านทางตู้ ATM

ตัวอย่าง Flowchart กระบวนการทำงาน



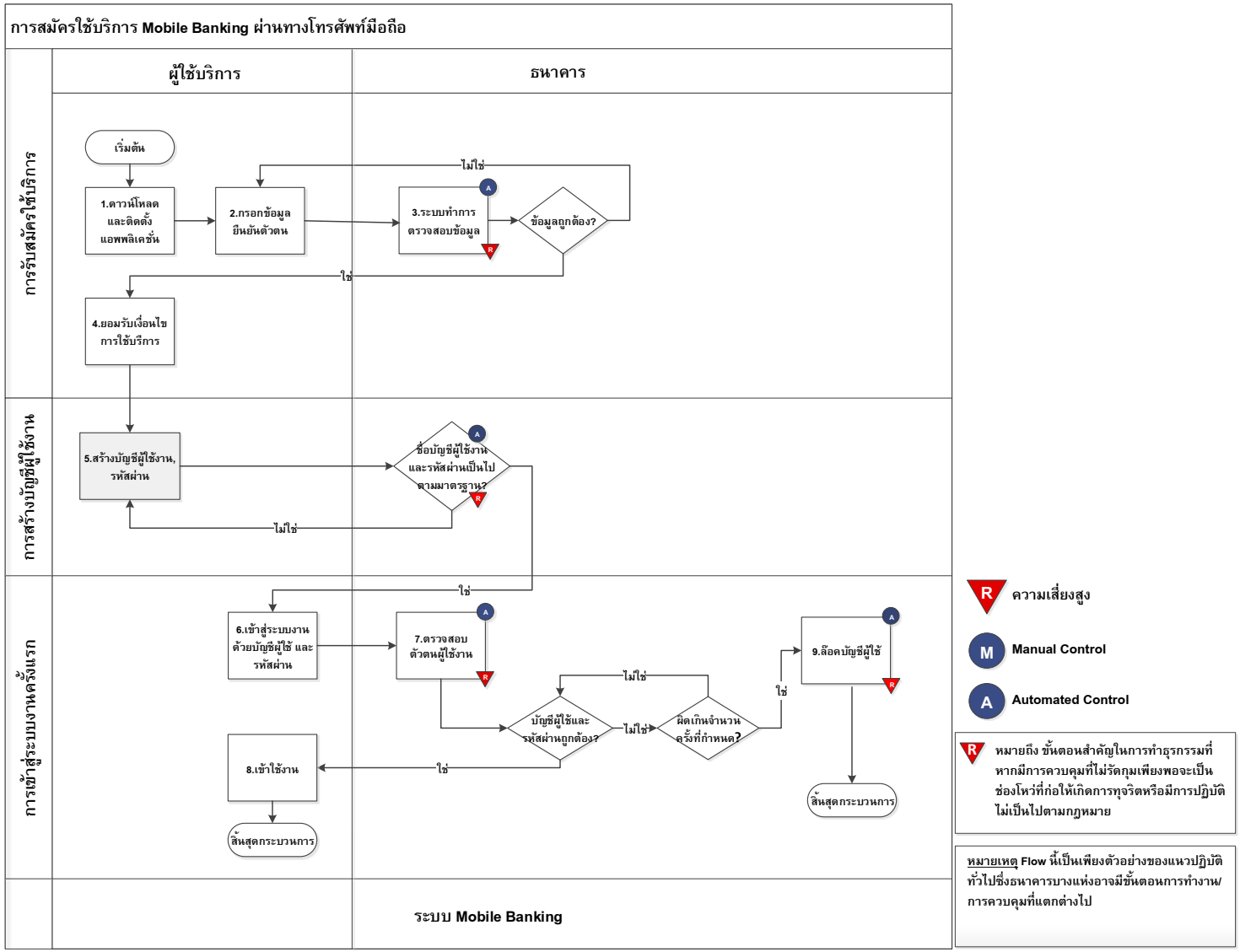
1.3 การสมัครใช้บริการ Internet Banking/ Mobile Banking ผ่านทาง Online

ตัวอย่าง Flowchart กระบวนการทำงาน



1.4 การสมัครใช้บริการ Mobile Banking ผ่านทางโทรศัพท์มือถือ

ตัวอย่าง Flowchart กระบวนการทำงาน



ตารางการควบคุมที่สำคัญ

1. การสมัครใช้บริการ Internet Banking/ Mobile Banking ผ่านช่องทางสาขา ATM, Online และโทรศัพท์มือถือ		
วัตถุประสงค์ เพื่อให้การดำเนินงานของธนาคารเกี่ยวกับการสมัครใช้บริการ Internet Banking และ Mobile Banking มีการตรวจสอบตัวตนของผู้สมัครใช้บริการที่รัดกุม รวมถึงการสร้างบัญชีผู้ใช้งาน สำหรับเข้าใช้งานอย่างถูกต้อง เชื่อถือได้ สอดคล้องตามหลักการควบคุมที่เป็นมาตรฐานสากล และลดความเสี่ยงที่อาจก่อให้เกิดการทุจริตจากการสวมรอย/ แอบอ้างเป็นบุคคลอื่น (Identity Theft)		
ขั้นตอน	**แนวปฏิบัติที่ดี**	
การรับสมัครใช้บริการ	1.1	มีกระบวนการในการระบุและตรวจสอบข้อมูล/เอกสารแสดงตนของผู้สมัครใช้บริการที่มีความรัดกุม โดยใช้ข้อมูล/เอกสารแสดงตน 2 ประเภทควบคู่กันสำหรับการตรวจสอบ **ตัวอย่างเช่น** ▪ กรณีสมัครผ่านทางสาขา : การตรวจสอบบัตรประชาชน ควบคู่กับสมุดบัญชีเงินฝากหรือบัตรเครดิต ▪ กรณีสมัครผ่านทางเครื่อง ATM : การพิสูจน์ตัวตนลูกค้าผู้สมัครใช้บริการด้วยบัตรและรหัส ATM ▪ กรณีสมัครผ่านทาง Online : การตรวจสอบตัวตนด้วยข้อมูลบัตรประชาชน ควบคู่กับหมายเลขบัญชี ทั้งนี้ธนาคารอาจพิจารณาเลือกใช้กระบวนการ หรือวิธีการอื่นในการตรวจสอบตัวตนของผู้สมัครใช้บริการ ที่มีความรัดกุมเทียบเท่า
	1.2	มีวิธีการควบคุมดูแลบริการผ่าน Mobile Application โดยให้มีการดาว์นโหลด Mobile Application จากช่องทางที่มีความน่าเชื่อถือและปลอดภัยตามที่ธนาคารกำหนดเท่านั้น และมีการเฝ้าระวัง และติดตามซอฟท์แวร์ปลอมที่เลียนแบบ Software ของธนาคาร
	1.3	มีการแจ้งข้อกำหนดและเงื่อนไขการใช้บริการ ความรับผิดชอบของผู้ให้บริการและผู้ใช้บริการ รวมถึงความเสี่ยงของบริการ โดยมีขั้นตอนให้ลูกค้ารับทราบข้อมูลดังกล่าวและยอมรับเงื่อนไขต่าง ๆ ที่เกี่ยวข้องกับการใช้บริการก่อนดำเนินการสร้างบัญชีผู้ใช้งานในระบบ
	1.4	มีการจัดเก็บใบคำขอสมัครใช้บริการ และเอกสารประกอบการสมัคร สำหรับการตรวจสอบย้อนหลังได้ โดยจัดเก็บเป็นระยะเวลาไม่ต่ำกว่าที่กฎหมายกำหนด
การสร้างบัญชีผู้ใช้งานและรหัสผ่านครั้งแรก	1.5	มีการควบคุมให้ลูกค้า 1 รายสามารถมีบัญชีผู้ใช้งาน Internet Banking ได้เพียงบัญชีเดียวเท่านั้น เพื่อป้องกันบัญชีผู้ใช้งานซ้ำซ้อน ซึ่งอาจเป็นช่องทางในการทุจริต
	1.6	ในกรณีที่ธนาคารเป็นผู้กำหนดบัญชีผู้ใช้งานหรือรหัสผ่านครั้งแรกแก่ผู้ใช้บริการ ให้มีการใช้ระบบในการตั้งรหัสผ่านโดยอัตโนมัติ และรหัสผ่านควรยากต่อการคาดเดา[6]

[6] *อ้างอิงข้อ 2.4.5 Internet Banking Application Control ส่วนที่ 2 แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบ IT ที่สนับสนุนธุรกิจหลัก Phase 1 ธุรกรรมฝาก ถอน และโอนเงิน*

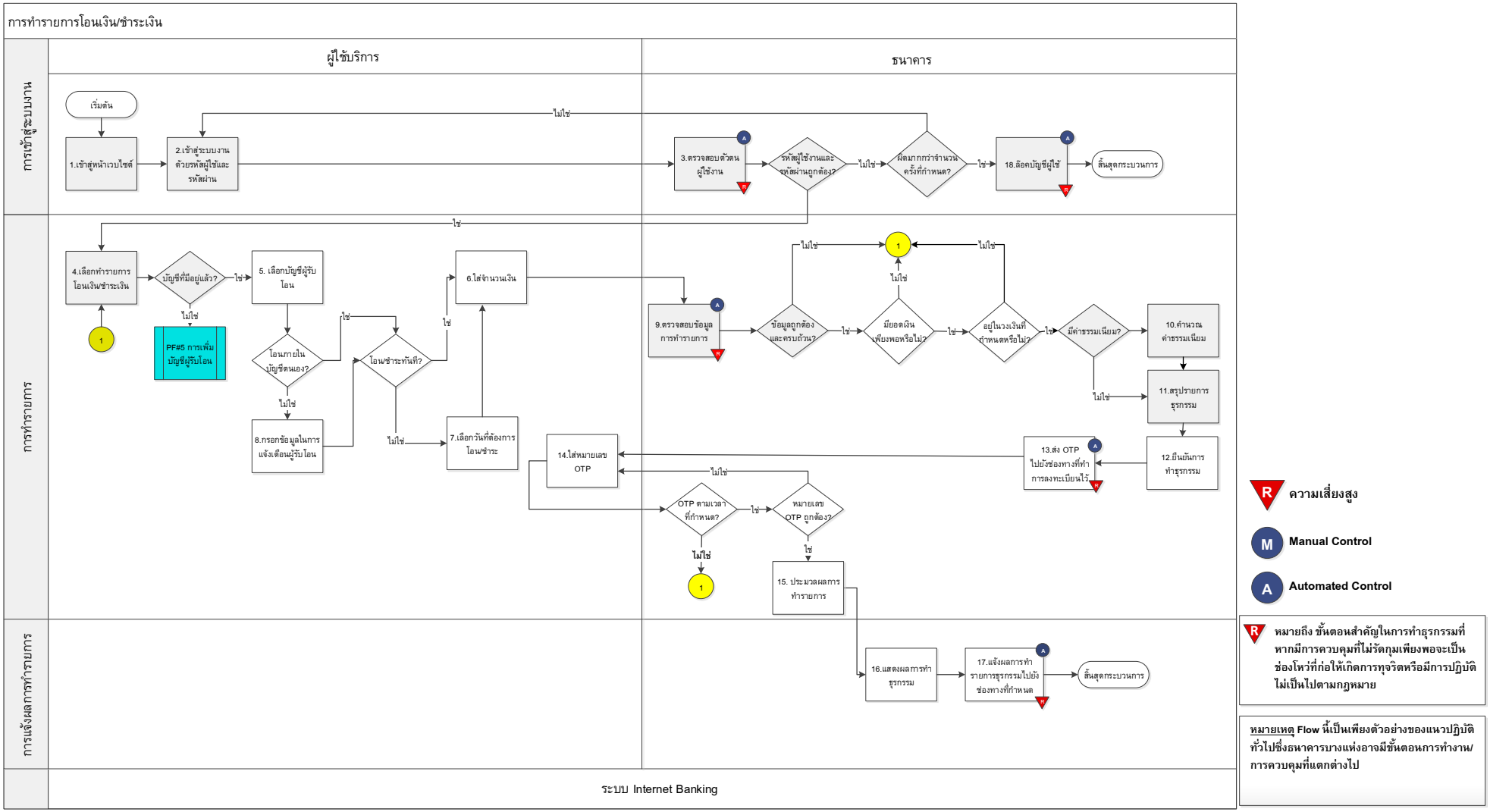
ขั้นตอน	แนวปฏิบัติที่ดี	
	1.7	มีการควบคุมการผูกบัญชีให้แก่ผู้ใช้บริการเฉพาะบัญชีที่ผู้ใช้บริการต้องการเท่านั้น ซึ่งต้องเป็นบัญชีของผู้ใช้บริการ Internet Banking เอง ทั้งนี้กรณีเป็นบัญชีร่วม ให้มีการควบคุมดูแลอื่นที่เหมาะสมเพื่อให้มั่นใจได้ว่าเจ้าของบัญชีร่วมทุกรายได้รับทราบและยอมรับการผูกบัญชีดังกล่าว
	1.8	ในกรณีการสมัครผ่านทางสาขา ให้มีกระบวนการควบคุมความถูกต้องของการสร้างบัญชีผู้ใช้งาน เพื่อลดความเสี่ยงด้านการปฏิบัติงานของเจ้าหน้าที่ เช่น การสอบยันกับเอกสารต่าง ๆ ที่ใช้ประกอบการขอเปิดใช้บริการ การสอบทานการปฏิบัติงาน เป็นต้น
	1.9	มีการแจ้งผลการสมัครใช้บริการให้แก่ผู้สมัครรับทราบภายหลังการสร้างบัญชีผู้ใช้งานแล้วเสร็จ ในกรณีที่ธนาคารเป็นผู้กำหนดบัญชีผู้ใช้งานและรหัสผ่านครั้งแรก ให้มีการจัดส่งบัญชีผู้ใช้งานและรหัสผ่านให้แก่ผู้สมัครผ่านคนละช่องทาง เช่น จัดส่งบัญชีผู้ใช้งานทาง E-mail และจัดส่งรหัสผ่านทาง SMS เป็นต้น
	1.10	ในกรณีที่ธนาคารเป็นผู้กำหนดบัญชีผู้ใช้งานหรือรหัสผ่านครั้งแรกแก่ผู้ใช้บริการ ให้มีการกำหนดระยะเวลาหมดอายุการใช้งานของบัญชีผู้ใช้งาน และรหัสผ่านครั้งแรก หรือมีการควบคุมอื่นที่เหมาะสมเทียบเท่า
การเข้าสู่ระบบงานครั้งแรก	1.11	มีการพิสูจน์ตัวตนผู้ใช้บริการในขั้นตอนการเข้าสู่ระบบงานครั้งแรกด้วยวิธีที่มีความมั่นคงปลอดภัย โดยให้มีการยืนยันตัวตนอีกชั้น เช่น OTP หรือคำถามข้อมูลส่วนบุคคล ในกรณีที่ผู้ใช้บริการใส่ข้อมูลพิสูจน์ตัวตนไม่ถูกต้อง ให้มีการแจ้งเตือนโดยข้อความแจ้งเตือนที่ไม่เป็นการบ่งชี้ว่าข้อมูลพิสูจน์ตัวตนส่วนใดไม่ถูกต้อง
	1.12	มีการล็อคบัญชีผู้ใช้งานเมื่อใส่รหัสผ่านไม่ถูกต้องเกินกว่าจำนวนครั้งที่กำหนด[7]
	1.13	ในกรณีที่ธนาคารเป็นผู้กำหนดชื่อบัญชีผู้ใช้งานหรือรหัสผ่านให้แก่ผู้ใช้บริการ ให้มีการบังคับให้เปลี่ยนชื่อบัญชีผู้ใช้งานและรหัสผ่านเมื่อเข้าสู่ระบบงานครั้งแรก
	1.14	มีการกำหนดให้ผู้ใช้บริการตั้งค่ารหัสผ่านให้มีความซับซ้อนและยากต่อการคาดเดา โดยรหัสผ่านต้องประกอบด้วย ตัวอักษร และตัวเลข และมีแนวทางในการเพิ่มอักขระพิเศษ
	1.15	มีการแจ้งการเข้าใช้งานครั้งแรกให้ผู้ใช้บริการทราบ ผ่านทางช่องทางที่ผู้ใช้บริการลงทะเบียนไว้ เช่น SMS, E-mail เป็นต้น

[7] *อ้างอิงข้อ 2.4.5 Internet Banking Application Control ส่วนที่ 2 แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบ IT ที่สนับสนุนธุรกิจหลัก Phase 1 ธุรกรรมฝาก ถอน และโอนเงิน*

2. การทำธุรกรรมผ่าน Internet Banking/ Mobile Banking (การโอนเงิน การชำระเงิน)

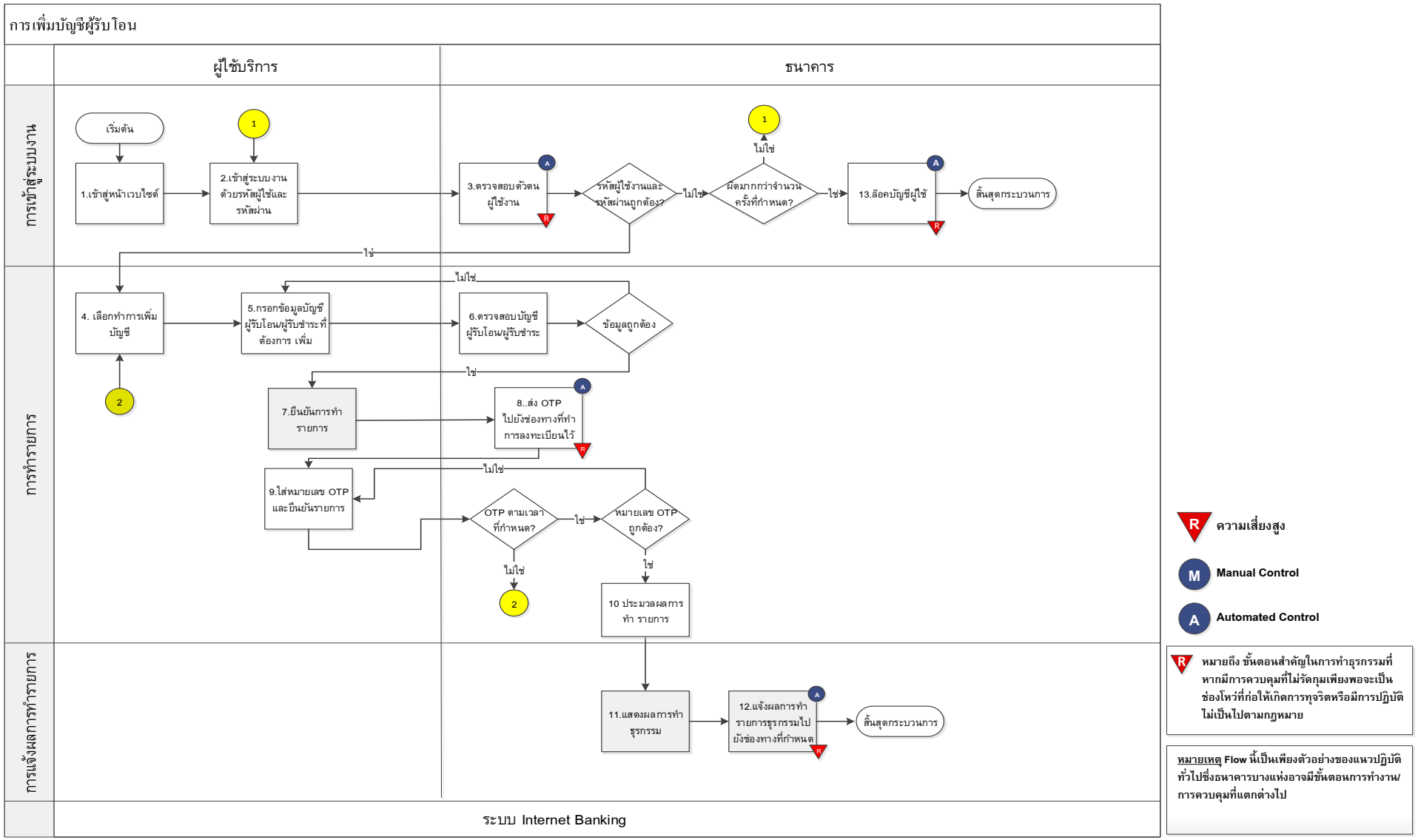
2.1 การทำรายการโอนเงิน/ชำระเงิน

ตัวอย่าง Flowchart กระบวนการทำงาน



2.2 การเพิ่มบัญชีผู้รับโอน

ตัวอย่าง Flowchart กระบวนการทำงาน



ตารางการควบคุมที่สำคัญ

2. การทำรายการผ่าน Internet Banking/ Mobile Banking (การโอนเงิน การชำระเงิน) [8]		
วัตถุประสงค์ เพื่อให้ระบบการให้บริการ Internet Banking/ Mobile Banking ของธนาคาร มีขั้นตอนการทำธุรกรรมที่รัดกุม ปลอดภัย ถูกต้องเชื่อถือได้ตามหลักมาตรฐานสากล และเป็นไปตามกฎหมายที่เกี่ยวข้อง ลดความเสี่ยงของการทุจริตและการทำธุรกรรมผิดพลาดในการทำธุรกรรมผ่านระบบงาน Internet Banking/ Mobile Banking (การโอนเงิน การชำระเงิน)		
ขั้นตอน	**แนวปฏิบัติที่ดี**	
การเข้าสู่ระบบงาน	2.1	มีการระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้บริการในขั้นตอนการเข้าใช้ระบบงานด้วยวิธีที่มั่นคงปลอดภัย เช่นการใช้ชื่อบัญชีผู้ใช้งาน (Username) ควบคู่กับรหัสผ่าน (Password) หรือใช้การระบุตัวตนอุปกรณ์ (Device Identification) ควบคู่กับ PIN เป็นต้น
	2.2	ในกรณีที่ผู้ใช้บริการใส่ข้อมูลพิสูจน์ตัวตนไม่ถูกต้อง ให้มีการแจ้งเตือนให้ผู้ใช้บริการทราบโดยข้อความแจ้งเตือนไม่เป็นการบ่งชี้ว่าข้อมูลพิสูจน์ตัวตนส่วนใดไม่ถูกต้อง
	2.3	มีการควบคุมให้ล๊อคบัญชีผู้ใช้งาน หากผู้ใช้บริการระบุข้อมูลพิสูจน์ตัวตนไม่ถูกต้องเกินกว่าจำนวนครั้งที่กำหนด
	2.4	มีระบบในการแจ้งให้เจ้าของบัญชีทราบถึงสถานการณ์เข้าสู่ระบบงาน (Log in) ทุกครั้งผ่านทางที่ลูกค้าได้ลงทะเบียนไว้ เช่น E-mail หรือ SMS เป็นต้น
	2.5	มีการควบคุมไม่ให้มีการจัดเก็บข้อมูลที่ใช้ในการระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้บริการ เช่น Session ID, User ID หรือรหัสผ่าน ไว้ใน cookie
	2.6	มีการแสดงวันที่และเวลาที่ Log in เข้าสู่ระบบ Internet Banking/ Mobile Banking ครั้งล่าสุดบนหน้าแรก ภายหลังที่ Log in เข้าสู่ระบบสำเร็จ
การทำรายการ	2.7	มีการตรวจสอบข้อมูลที่เข้าสู่ระบบ (Input Validation) โดยอนุญาตเฉพาะข้อมูลที่อยู่ในรูปแบบที่กำหนดเท่านั้น เพื่อป้องกันข้อมูลผิดลักษณะ/รูปแบบ ไม่สมเหตุผล หรือผิด Logic และระบบต้องไม่อนุญาตให้ผู้ใช้บริการข้ามขั้นตอนจนกว่าจะกรอกข้อมูลถูกต้อง
	2.8	มีการตรวจสอบความครบถ้วนของข้อมูลก่อนที่จะทำการประมวลผลในขั้นตอนต่อไป เช่น จำนวนหลักของหมายเลขบัญชี ความครบถ้วนของ Mandatory Fields เป็นต้น หากข้อมูลใน Mandatory Field ไม่ถูกต้องครบถ้วน ควรมีข้อความแจ้งผู้ใช้บริการทราบ และระบบต้องไม่อนุญาตให้ผู้ใช้บริการข้ามขั้นตอนจนกว่าจะกรอกข้อมูลถูกต้อง

[8] *อ้างอิงข้อ 2.4.5 Internet Banking Application Control ส่วนที่ 2 แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบ IT ที่สนับสนุนธุรกิจหลัก Phase 1 ธุรกรรมฝาก ถอน และโอนเงิน*

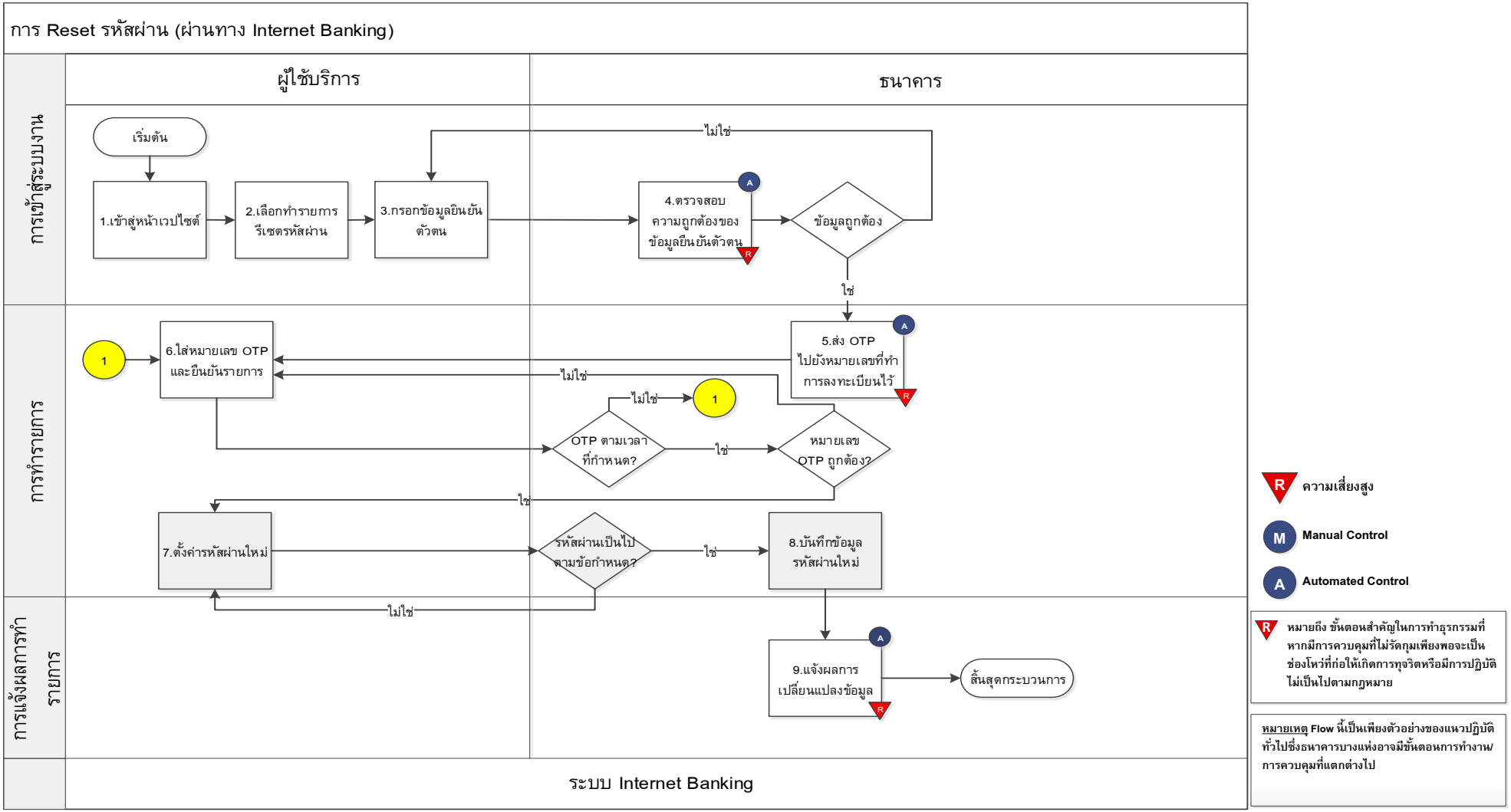
ขั้นตอน	แนวปฏิบัติที่ดี	
	2.9	มีการตรวจสอบเงื่อนไขการทำธุรกรรม เช่น ยอดเงินคงเหลือ วงเงินสูงสุด, วงเงินในการทำรายการต่อครั้ง/ต่อวัน, และค่าธรรมเนียม เป็นต้น ก่อนที่จะดำเนินรายการตามขั้นตอนที่กำหนดไว้ และมีการปฏิเสธการทำรายการ ในกรณีที่รายการไม่ถูกต้องตามเงื่อนไขที่กำหนด
	2.10	มีการจำกัดวงเงินในการทำธุรกรรมที่สำคัญ เช่น วงเงินในการโอนเงินไปยังบัญชีบุคคลอื่น วงเงินในการโอนเงินต่างธนาคาร วงเงินในการชำระเงิน เป็นต้น
	2.11	ในกรณีที่เกิดความผิดพลาดระหว่างที่ระบบประมวลผลข้อมูล ให้ระบบมีการแจ้งผู้ใช้บริการ และต้องสามารถตรวจสอบความถูกต้องของข้อมูล (Data Integrity) เพื่อกลับไปสู่สถานะก่อนทำรายการอย่างถูกต้อง
	2.12	มีกระบวนการที่ทำให้มั่นใจว่าข้อมูลในฐานข้อมูลของระบบงานเป็นปัจจุบัน โดยระบบสามารถดึงข้อมูลบัญชีผู้ใช้งานมาจากระบบฐานข้อมูลได้อย่างถูกต้องและครบถ้วน
	2.13	มีการสรุปข้อมูลการทำรายการเพื่อให้ผู้ใช้บริการตรวจสอบความถูกต้อง ครบถ้วนของรายการธุรกรรมก่อนทำการยืนยันรายการ
	2.14	มีการยืนยันตัวตนของผู้ทำรายการในขั้นตอนการทำรายการที่สำคัญ เช่น การผูกบัญชีผู้รับชำระ, การผูกบัญชีผู้รับโอน, การโอนเงิน, การชำระเงิน, การเปลี่ยนแปลงวงเงิน, และการเปลี่ยนแปลงบัญชีผู้ใช้งานหรือรหัสผ่าน เป็นต้น โดยใช้วิธีที่มีความมั่นคงปลอดภัยเหมาะสมกับระดับความเสี่ยงของธุรกรรม เช่น การส่ง OTP ผ่าน SMS[9] เป็นต้น
การแจ้งผลการทำรายการ	2.15	มีการแสดงผลและรายละเอียดการทำรายการให้ผู้ใช้บริการทราบทันที หลังจากที่ระบบประมวลผลแล้วเสร็จ และมีการจัดเก็บข้อมูลประวัติการทำรายการ (Transaction History) เพื่อให้ผู้ใช้บริการสามารถตรวจสอบย้อนหลังได้
	2.16	มีการแจ้งผลการทำรายการผ่านช่องทางที่ผู้ใช้บริการได้ลงทะเบียนไว้ ซึ่งควรมีการปิดบังบางส่วนของข้อมูลสำคัญของลูกค้า เช่น ชื่อบัญชี และหมายเลขบัญชี เป็นต้น
	2.17	ในกรณีที่เกิดความผิดพลาดกับระบบงานระหว่างที่ระบบประมวลผลข้อมูล ให้ระบบมีข้อความแจ้งเตือนผู้ใช้ (Error Message) ที่สามารถสื่อสารให้ลูกค้าเกิดความเข้าใจที่ถูกต้อง และต้องไม่แสดงข้อมูลภายในของระบบ เช่น ยี่ห้อ รุ่น หรือ Application Path เป็นต้น แต่ควรแสดงรหัสที่บอกถึงสาเหตุของการทำงานที่ผิดพลาด ที่สามารถเข้าใจได้เฉพาะบุคลากรที่มีหน้าที่รับผิดชอบเท่านั้น

[9] *แนวปฏิบัติเกี่ยวกับ OTP ระบุอยู่ใน Appendix A: Internet Banking Security*

3. การเปลี่ยนแปลงแก้ไขข้อมูลของผู้ใช้บริการผ่านช่องทางต่าง ๆ (สาขา /Call Center/ Internet Banking) และการยกเลิกบริการ

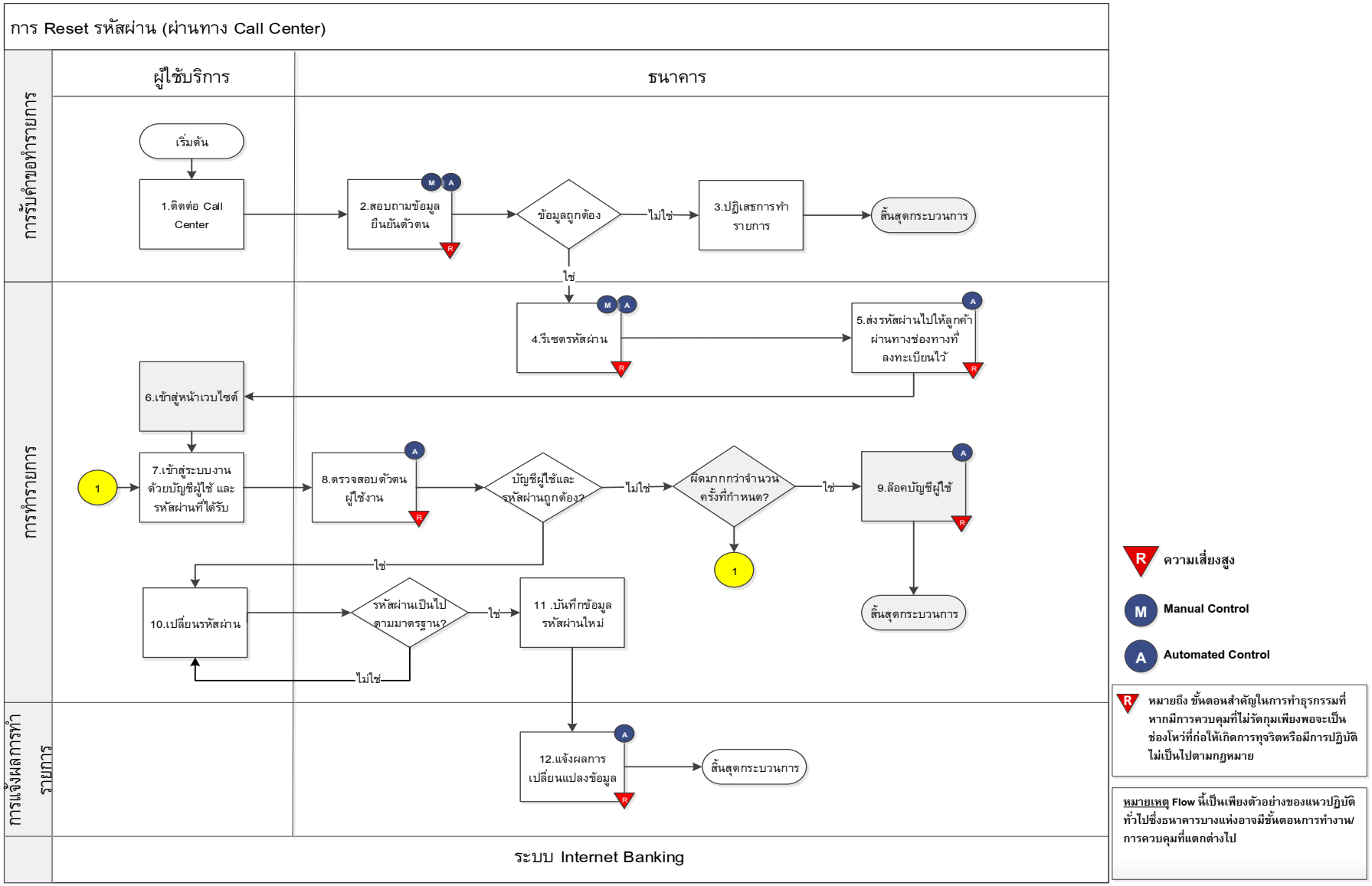
3.1 การ Reset รหัสผ่าน (ผ่านทาง Internet Banking)

ตัวอย่าง Flowchart กระบวนการทำงาน



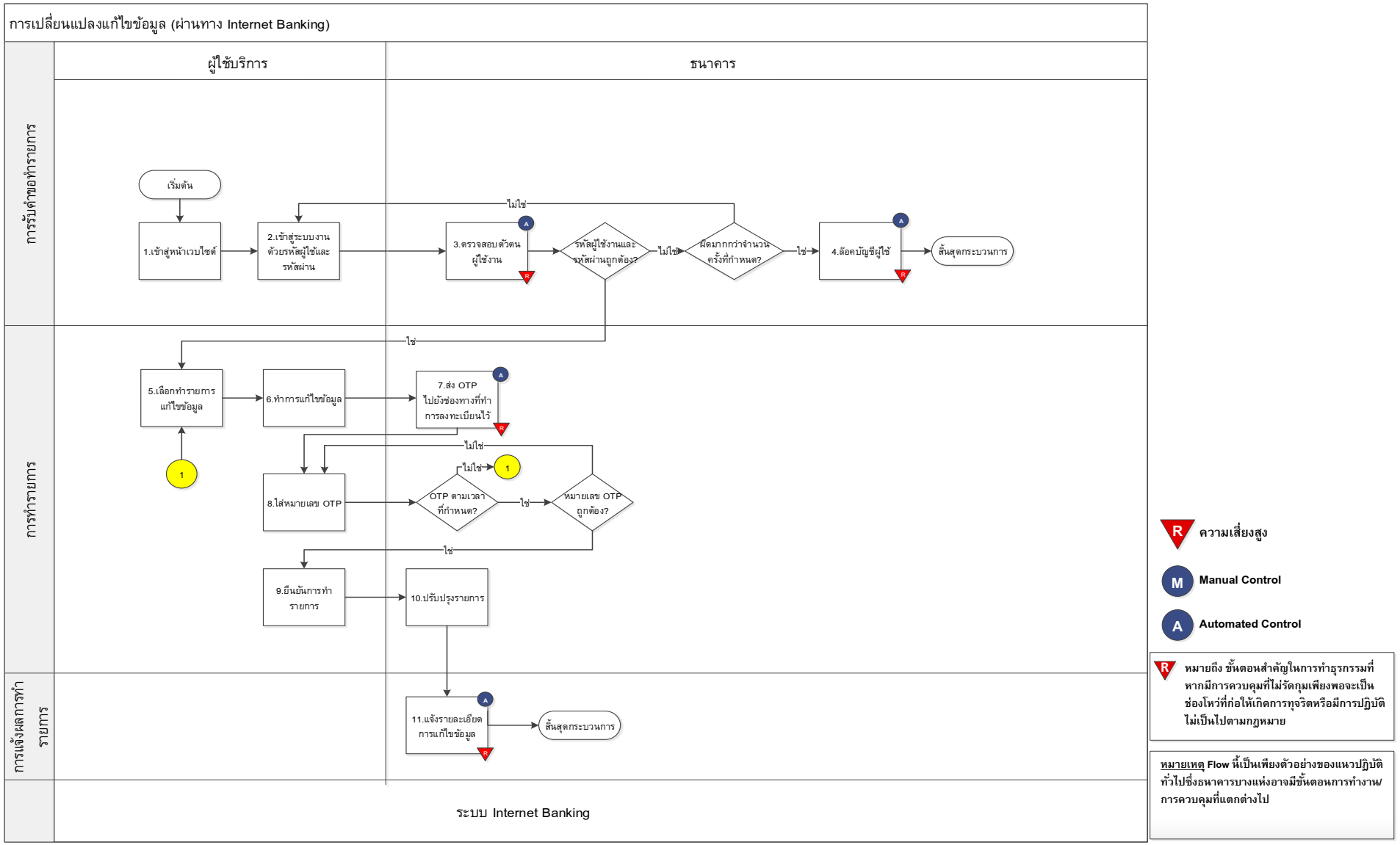
3.2 การ Reset รหัสผ่าน (ผ่านทาง Call Center)

ตัวอย่าง Flowchart กระบวนการทำงาน



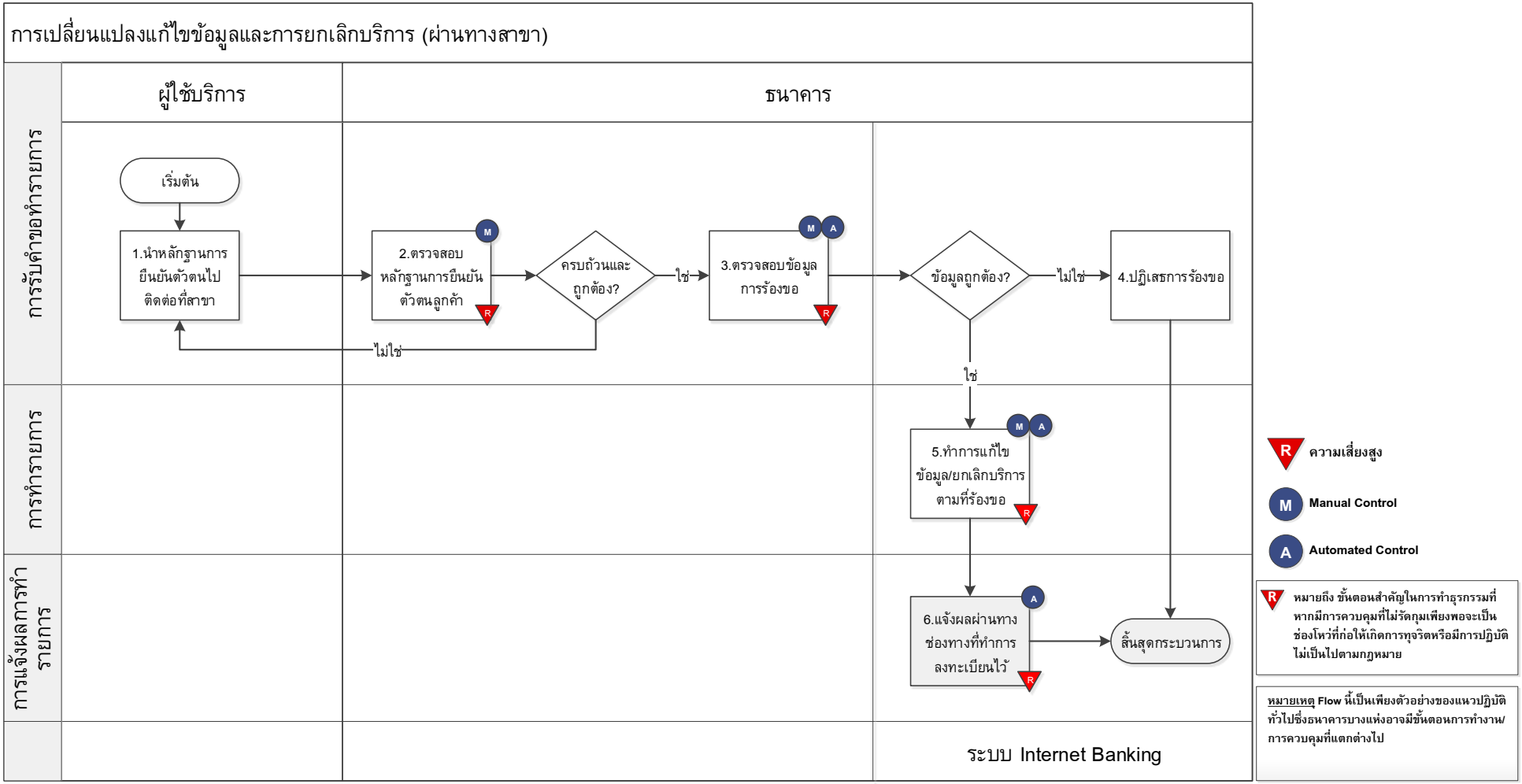
3.3 การเปลี่ยนแปลงแก้ไขข้อมูล (ผ่านทาง Internet Banking)

ตัวอย่าง Flowchart กระบวนการทำงาน



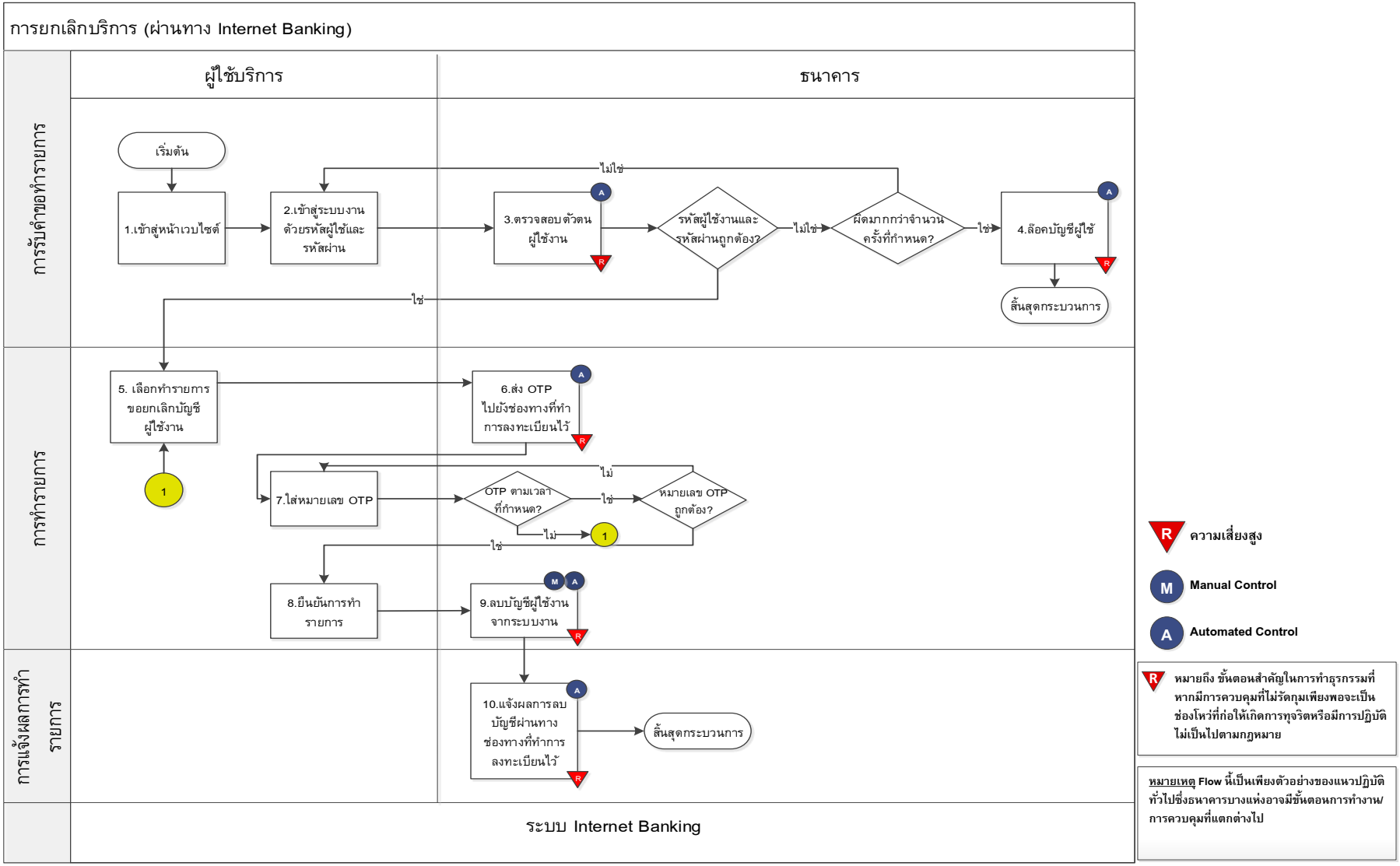
3.4 การเปลี่ยนแปลงแก้ไขข้อมูล และการยกเลิกบริการ (ผ่านทางสาขา)

ตัวอย่าง Flowchart กระบวนการทำงาน



3.5 การยกเลิกบริการ (ผ่านทาง Internet Banking)

ตัวอย่าง Flowchart กระบวนการทำงาน



ตารางการควบคุมที่สำคัญ

3. การเปลี่ยนแปลงแก้ไขข้อมูลสำคัญของผู้ใช้บริการผ่านช่องทางต่าง ๆ (สาขา/Call Center / Internet Banking) และการยกเลิกบริการ หมายเหตุ : ข้อมูลสำคัญของผู้ใช้บริการ เช่น บัญชีผู้ใช้งาน รหัสผ่าน วงเงินการทำรายการ E-Mail Address เบอร์โทรศัพท์ ข้อมูลที่อยู่ เป็นต้น
วัตถุประสงค์ เพื่อให้กระบวนการ และระบบการให้บริการ Internet Banking/ Mobile Banking ของธนาคาร มีขั้นตอนการทำรายการกับข้อมูลสำคัญของลูกค้าที่รัดกุม ปลอดภัย ถูกต้องเชื่อถือได้ ตามหลักมาตรฐานสากล และเป็นไปตามกฎหมายที่เกี่ยวข้อง ลดความเสี่ยงของข้อมูลลูกค้ารั่วไหล หรือการทุจริตโดยการสวมรอยเป็นลูกค้า (Identity Theft)

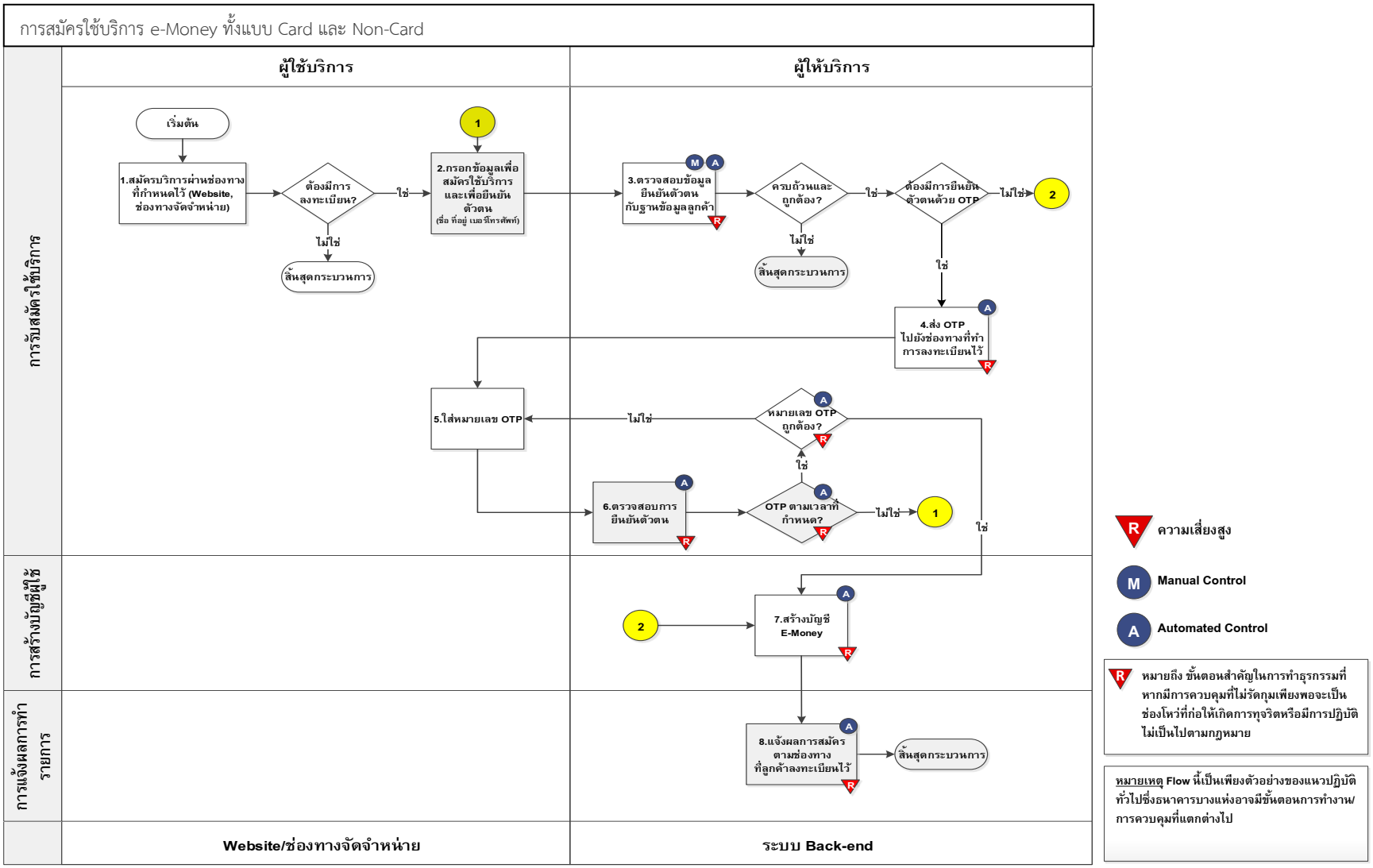
ขั้นตอน	แนวปฏิบัติที่ดี	
การรับคำขอทำรายการ : การ Reset และเปลี่ยนแปลงรหัสผ่าน, การเปลี่ยนแปลงแก้ไขข้อมูล การยกเลิกบริการ	3.1	มีกระบวนการในการระบุและตรวจสอบข้อมูล/เอกสารแสดงตนของเจ้าของบัญชีผู้ใช้งานที่มีความรัดกุม **ตัวอย่างเช่น** ■ กรณีขอเปลี่ยนแปลงข้อมูลผ่านทางสาขา : การตรวจสอบบัตรประชาชนควบคู่กับสมุดบัญชีเงินฝากหรือบัตรเครดิต ■ กรณีขอเปลี่ยนแปลงข้อมูลผ่านทาง Call Center : การจัดทำชุดคำถามที่ใช้ในการยืนยันตัวตนของผู้ใช้บริการ โดยเป็นชุดคำถามที่สามารถใช้ระบุตัวตนผู้ใช้บริการได้เพียงพอ ไม่ใช่คำถามที่สอบถามข้อมูลพื้นฐานทั่วไป และธนาคารควรมีการปรับปรุงชุดคำถามอยู่สม่ำเสมอ ■ กรณีขอเปลี่ยนแปลงข้อมูลผ่านทาง Internet Banking/ Mobile : ควรมี Username/ Password การส่ง OTP ผ่านทาง SMS หรือสอบถามข้อมูลส่วนบุคคลอื่น ๆ ทั้งนี้ ธนาคารอาจพิจารณาเลือกใช้กระบวนการ หรือวิธีการอื่นในการตรวจสอบตัวตนของผู้สมัครใช้บริการ ที่มีความรัดกุมเทียบเท่า
	3.2	มีการจัดเก็บใบคำขอเปลี่ยนแปลงข้อมูล และเอกสารประกอบการเปลี่ยนแปลงข้อมูลหรือบริการ สำหรับการตรวจสอบย้อนหลังได้ เป็นระยะเวลาอย่างน้อยไม่ต่ำกว่าที่กฎหมายกำหนด
การทำรายการ	3.3	ในกรณีการเปลี่ยนแปลงข้อมูลของผู้ใช้บริการผ่านทางสาขาหรือ Call Center ให้มีกระบวนการควบคุมความถูกต้องและปลอดภัยของการเปลี่ยนแปลงข้อมูลของผู้ใช้บริการ เพื่อลดความเสี่ยงด้านการปฏิบัติงานของเจ้าหน้าที่ สำหรับการ Reset รหัสผ่านทางสาขาหรือ Call Center ธนาคารควรจัดส่งรหัสผ่านใหม่ให้แก่ลูกค้าผ่านช่องทางที่มีความปลอดภัย เพื่อป้องกันไม่ให้รหัสผ่านถูกล่วงรู้โดยผู้อื่นรวมถึงเจ้าหน้าที่ของธนาคาร
	3.4	ในกรณีที่ผู้ใช้บริการทำรายการเปลี่ยนแปลงข้อมูลด้วยตนเองผ่านทาง Online ให้มีขั้นตอนให้สามารถตรวจสอบความถูกต้องและปลอดภัยของข้อมูลและมีการยืนยันการทำรายการด้วยวิธีการที่เชื่อถือได้ เช่น การส่ง OTP ผ่าน SMS เป็นต้น ก่อนที่ระบบจะเปลี่ยนแปลงข้อมูลตามที่ร้องขอ

ขั้นตอน	แนวปฏิบัติที่ดี	
การแจ้งผลการทำรายการ	3.5	มีการแสดงผลและรายละเอียดการทำรายการให้ผู้ใช้บริการทราบทันทีหลังจากที่ระบบประมวลผลแล้วเสร็จ และมีการจัดเก็บข้อมูลประวัติการทำรายการ (Transaction History) เพื่อให้ผู้ใช้บริการสามารถตรวจสอบย้อนหลังได้
	3.6	มีการแจ้งผลการทำรายการผ่านช่องทางที่ผู้ใช้บริการได้ทำการลงทะเบียนไว้ โดยเป็นช่องทางอื่นที่ไม่ได้ใช้ทำรายการ เช่น SMS, E-mail เป็นต้น
	3.7	ในกรณีที่เกิดความผิดพลาดกับระบบงานระหว่างที่ระบบประมวลผลข้อมูล ให้ระบบมีข้อความแจ้งเตือน (Error Message) ที่สามารถสื่อสารให้ผู้ใช้บริการเกิดความเข้าใจที่ถูกต้อง และต้องไม่แสดงข้อมูลภายในของระบบเช่น ยี่ห้อ รุ่น หรือ Application Path เป็นต้น แต่ควรแสดงรหัสที่บอกถึงสาเหตุของการทำงานที่ผิดพลาด ที่สามารถเข้าใจได้เฉพาะบุคลากรที่รับมอบอำนาจเท่านั้น

4. การสมัครใช้บริการและการทำรายการ e-Money ทั้งแบบ Card และ Non-card

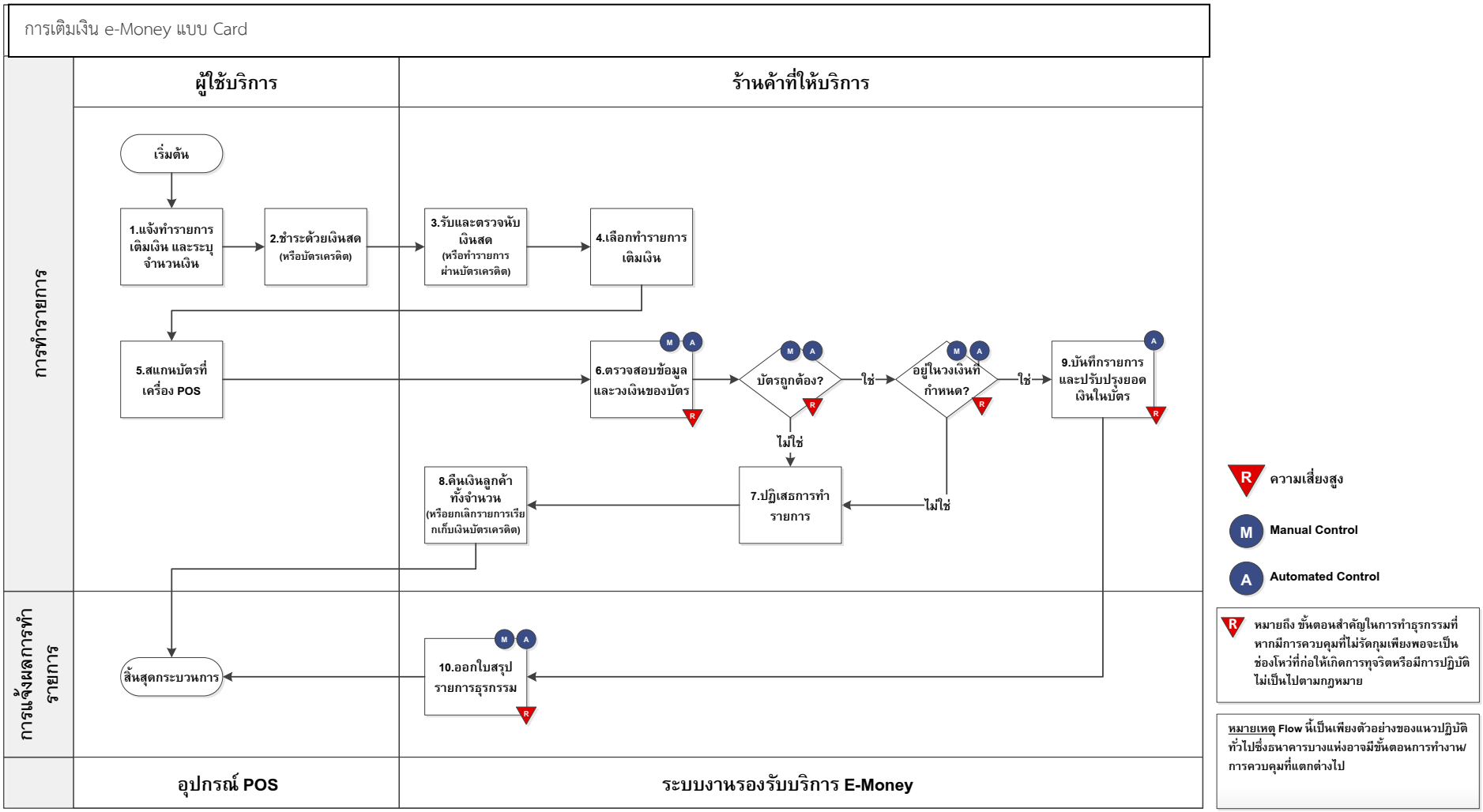
4.1 การสมัครใช้บริการ e-Money ทั้งแบบ Card และ Non-Card

ตัวอย่าง Flowchart กระบวนการทำงาน



4.2 การเติมเงิน e-Money แบบ Card

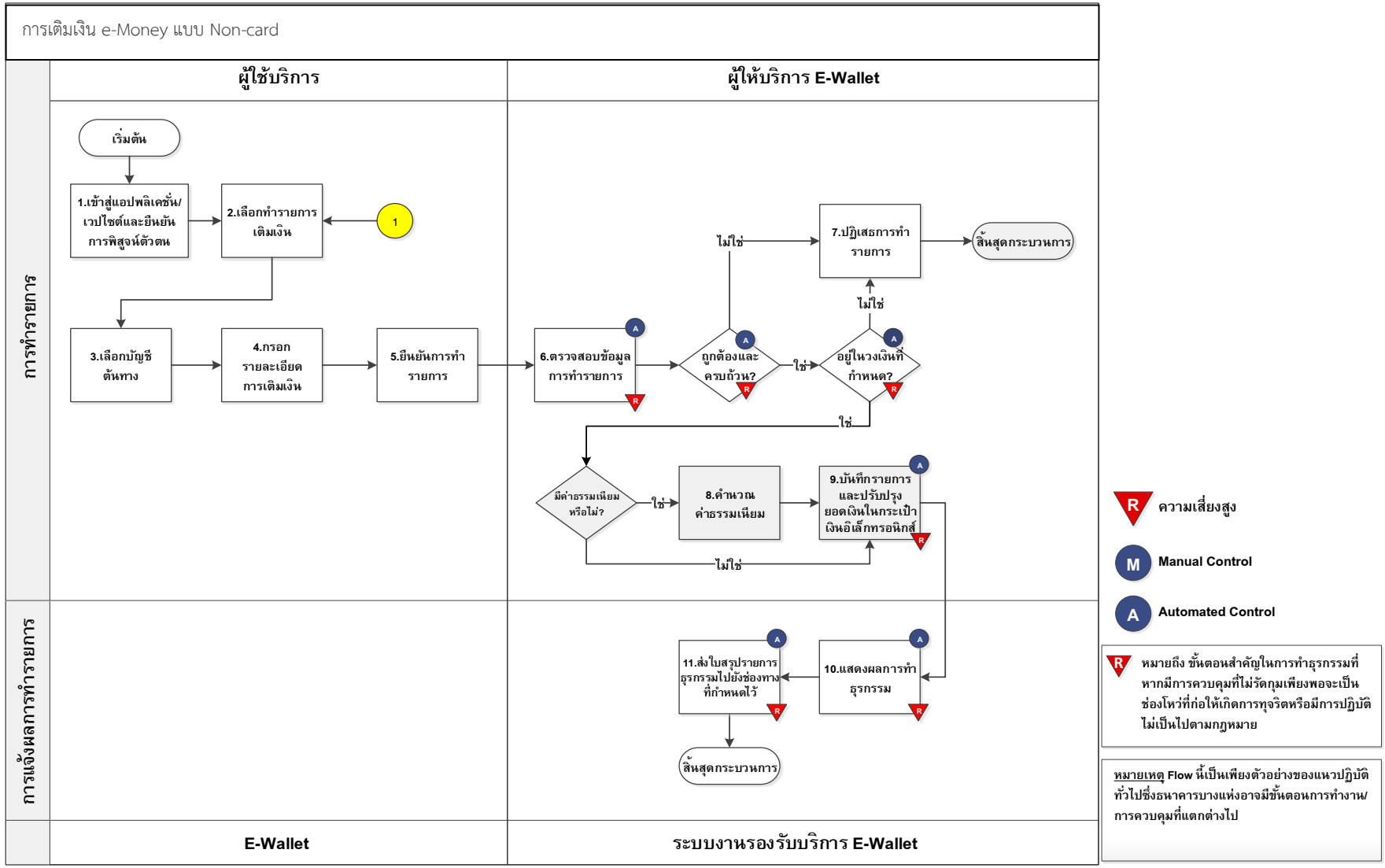
ตัวอย่าง Flowchart กระบวนการทำงาน



หมายเหตุ: อุปกรณ์ POS (Point of Sale) หมายถึงอุปกรณ์อ่านบัตร ณ จุดขาย

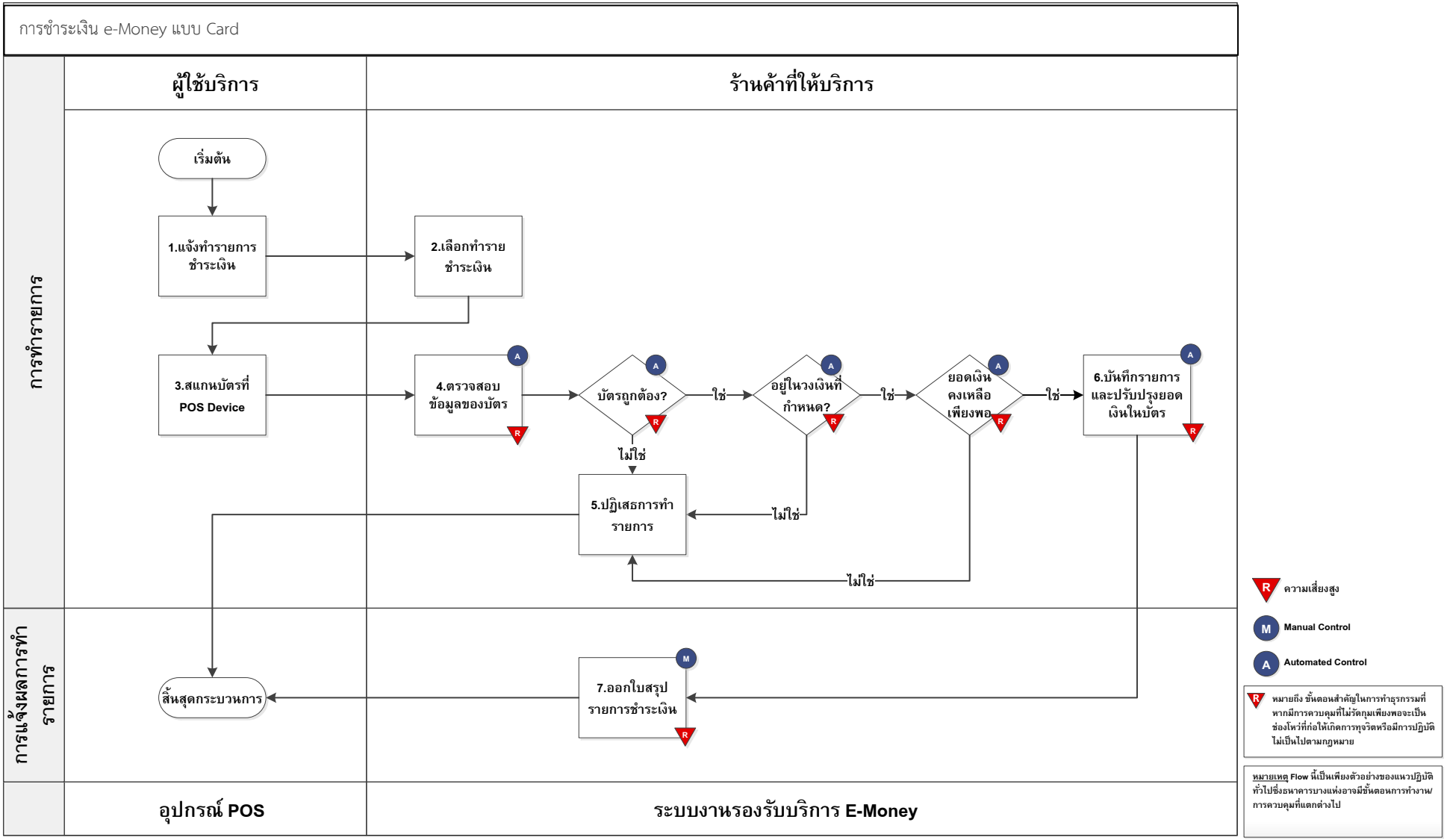
4.3 การเติมเงิน e-Money แบบ Non-card

ตัวอย่าง Flowchart กระบวนการทำงาน



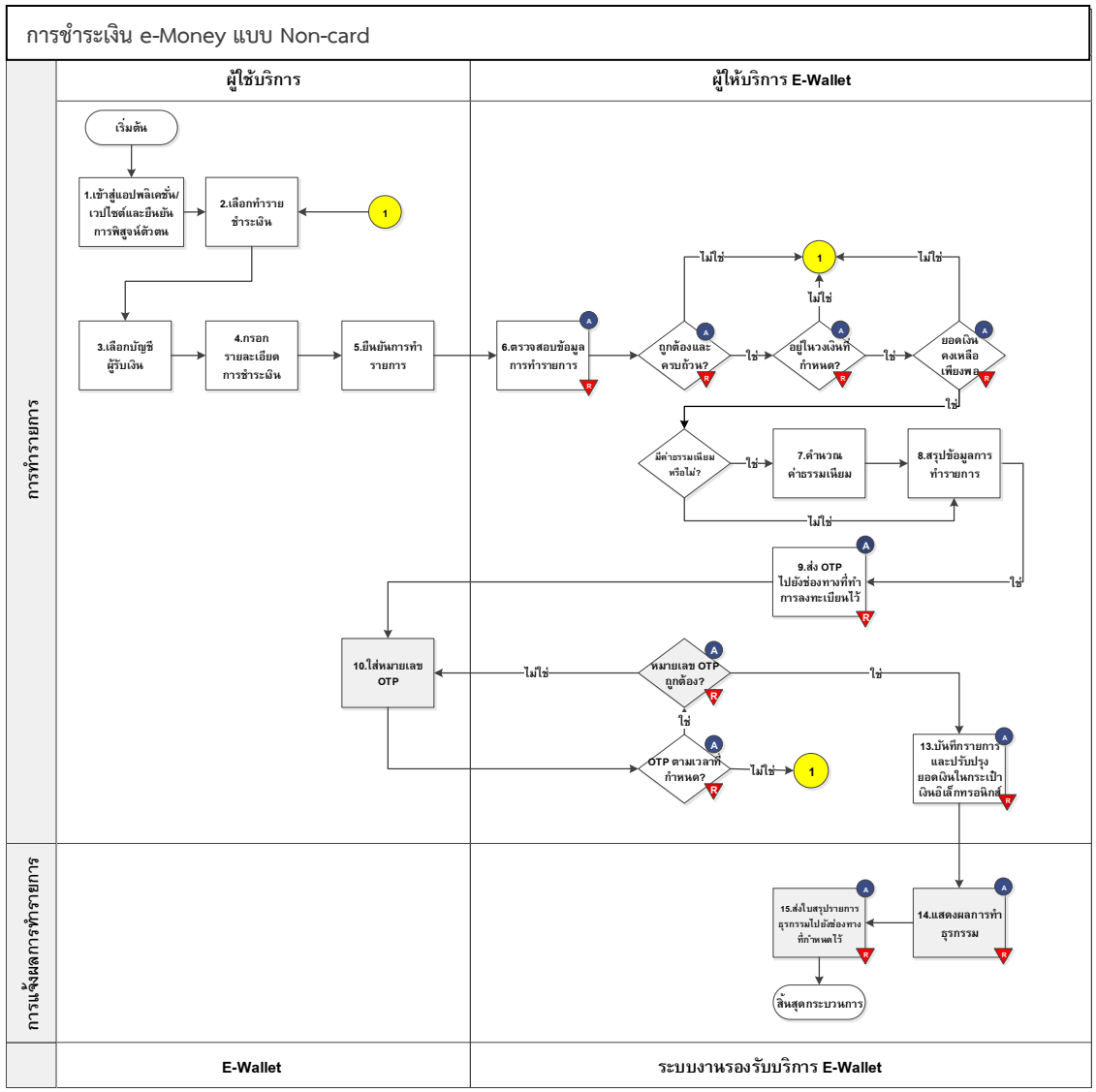
4.4 การชำระเงิน e-Money แบบ Card

ตัวอย่าง Flowchart กระบวนการทำงาน



4.5 การชำระเงิน e-Money แบบ Non-card

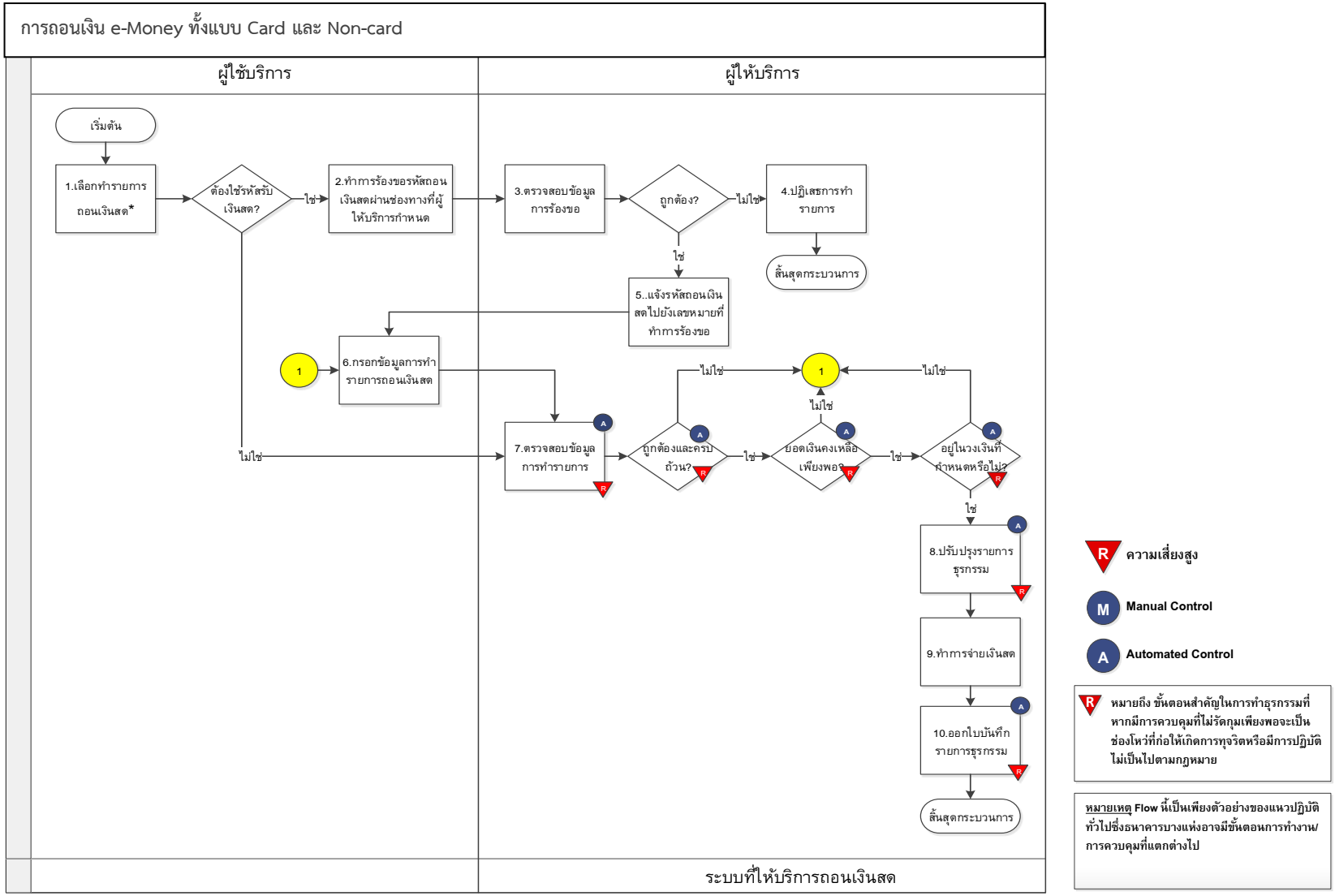
ตัวอย่าง Flowchart กระบวนการทำงาน



หมายเหตุ : Flowchart กระบวนการนี้ สามารถใช้ได้กับธุรกรรมโอนเงิน ผ่าน e-Money

4.6 การถอนเงิน e-Money ทั้งแบบ Card และ Non-card

ตัวอย่าง Flowchart กระบวนการทำงาน



หมายเหตุ : ปัจจุบันการทำรายการถอนเงินสด ผ่าน e-Money มีได้หลายวิธี ได้แก่ ใช้บัตร e-Money ทำรายการที่ตู้ ATM และ/หรือ ระบุหมายเลขโทรศัพท์มือถือคู่กับการใช้รหัสผ่านรับเงิน เป็นต้น

ตารางการควบคุมที่สำคัญ

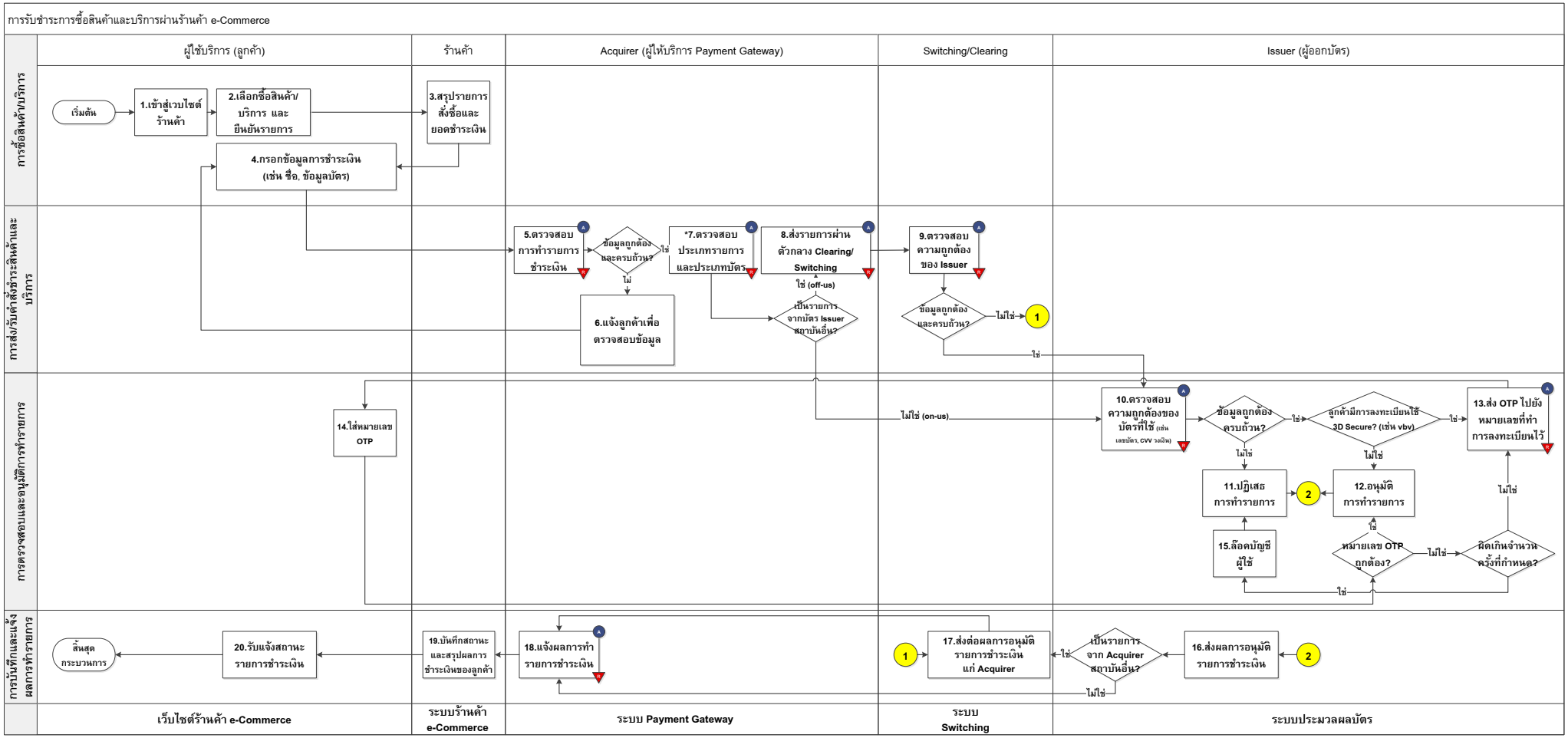
4. การสมัครใช้บริการและการทำรายการด้วยเงินอิเล็กทรอนิกส์ (e-Money)		
วัตถุประสงค์ เพื่อให้การดำเนินงานของผู้ให้บริการ e-Money ที่เกี่ยวกับการสมัครใช้บริการ การทำธุรกรรมที่สำคัญมีความรัดกุม ปลอดภัย ถูกต้อง เชื่อถือได้ และเพื่อลดโอกาสในการใช้ผลิตภัณฑ์เงินอิเลคทรอนิคส์เป็นช่องทางในการฟอกเงินและการทุจริตอื่น ๆ		
ขั้นตอน	**แนวปฏิบัติที่ดี**	
การสมัครใช้บริการ	4.1	มีการควบคุมการจัดจำหน่ายบัตรเงินอิเลคทรอนิคส์ให้ผ่านช่องทางที่ผู้ให้บริการกำหนด โดยบัตรที่จัดจำหน่ายต้องเป็นบัตรที่ได้รับการลงทะเบียนและอนุมัติโดยผู้ให้บริการแล้วเท่านั้น
	4.2	มีวิธีการควบคุมดูแลบริการผ่าน Mobile Application โดยควรมีการเฝ้าระวังและติดตามซอฟท์แวร์ปลอมที่เลียนแบบ Software ของผู้ให้บริการ รวมถึงให้มีการดาวน์โหลด Mobile Application จากช่องทางที่มีความน่าเชื่อถือและปลอดภัย ตามที่ผู้ให้บริการกำหนดเท่านั้น
	4.3	ในกรณีการผูกกับบัญชีธนาคารหรือมีวงเงินในการทำธุรกรรมมูลค่าสูง ให้มีการลงทะเบียนผู้ใช้บริการก่อนเริ่มต้นการใช้งาน และมีการตรวจสอบข้อมูลยืนยันตัวตนผู้สมัครใช้บริการในขั้นตอนการลงทะเบียน เพื่อให้เป็นไปตามเงื่อนไขหลักเกณฑ์ตามที่กฎหมายกำหนด[10]
การทำรายการ	4.4	มีการระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้บริการในขั้นตอนการเข้าใช้ระบบงาน Non-card based ด้วยวิธีที่มั่นคงปลอดภัย เช่นการใช้ชื่อบัญชีผู้ใช้งาน (Username) ควบคู่กับรหัสผ่าน (Password) หรือใช้การระบุตัวตนอุปกรณ์ (Device Identification) ควบคู่กับ PIN เป็นต้น
	4.5	ในกรณีการทำรายการประเภทที่สำคัญและมีความเสี่ยงสูง เช่น การผูกบัญชี การโอนเงิน การถอนเงินสด เป็นต้น ให้มีการพิสูจน์ตัวตนผู้ใช้บริการอีกชั้นด้วยวิธีที่มีความมั่นคงปลอดภัยเหมาะสมกับระดับความเสี่ยงของธุรกรรม เช่น การส่ง OTP ผ่าน SMS เป็นต้น
	4.6	มีการกำหนดมูลค่าเงินสูงสุดของบริการ e-Money ทั้งประเภท Card-based และ Non-card based รวมทั้งมีการจำกัดวงเงินในการทำธุรกรรมที่มีความเสี่ยงสูง เช่น การโอนเงินระหว่างบัญชีผู้ใช้บริการ การถอนเงินสดเป็นต้น
	4.7	มีการตรวจสอบข้อมูลที่เข้าสู่ระบบ (Input Validation) โดยอนุญาตเฉพาะข้อมูลที่อยู่ในรูปแบบที่กำหนดเท่านั้น เพื่อป้องกันข้อมูลผิดลักษณะ/รูปแบบไม่สมเหตุผล หรือผิด Logic และระบบต้องไม่อนุญาตให้ผู้ใช้บริการข้ามขั้นตอนจนกว่าจะกรอกข้อมูลถูกต้อง

[10] *การตรวจสอบตัวตน ให้เป็นไปตาม พรฎ. ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 และประกาศที่เกี่ยวข้อง รวมถึงกฎหมายของสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.)*

ขั้นตอน	แนวปฏิบัติที่ดี	
	4.8	มีการกำหนดและแสดง Mandatory Field ให้ลูกค้าทราบ โดยกำหนดให้ระบบตรวจสอบความถูกต้องครบถ้วนของการกรอกข้อมูลใน Mandatory Field ก่อน หากไม่ถูกต้อง ควรมีข้อความแจ้งผู้ใช้บริการทราบ และระบบต้องไม่อนุญาตให้ผู้ใช้บริการข้ามขั้นตอนจนกว่าจะกรอกข้อมูลถูกต้อง
	4.9	มีการตรวจสอบเงื่อนไขการทำรายการ เช่น ยอดเงินคงเหลือ วงเงินสูงสุดวงเงินในการทำรายการต่อครั้ง/ต่อวัน และค่าธรรมเนียม เป็นต้น และมีการปฏิเสธการทำรายการ ในกรณีที่รายการไม่ถูกต้องตามเงื่อนไขที่กำหนด ก่อนที่จะดำเนินรายการตามขั้นตอนที่กำหนดไว้
	4.10	มีการสรุปข้อมูลการทำรายการ เพื่อให้ลูกค้าตรวจสอบความถูกต้อง ก่อนทำการยืนยันรายการ
	4.11	มีขั้นตอนที่สามารถตรวจสอบสถานะของการทำรายการ เพื่อรองรับกรณีรายการ E-Money มีความผิดพลาดระหว่างขั้นตอนการประมวลผลหรือขั้นตอนการส่ง message แจ้งผลการทำรายการกลับไปยังระบบ POS/Acquirer ต้นทาง ซึ่งหากพบว่าสถานะล่าสุดระบบทำรายการไม่สำเร็จแต่ได้ทำการตัดชำระแล้ว ควรทำการ reverse รายการ และแจ้งสถานะรายการไม่สำเร็จให้ระบบต้นทางทราบ ก่อนที่จะดำเนินรายการตามขั้นตอนที่กำหนดไว้
การแจ้งผลการทำธุรกรรม	4.12	มีการแสดงผลและรายละเอียดการทำรายการให้ผู้ใช้บริการทราบทันทีหลังจากที่ระบบประมวลผลแล้วเสร็จ และมีการจัดเก็บข้อมูลประวัติการทำรายการ (Transaction History) เพื่อให้ผู้ใช้บริการสามารถตรวจสอบย้อนหลังได้
	4.13	ในกรณีที่เกิดความผิดพลาดกับระบบงานระหว่างที่ระบบประมวลผลข้อมูล ให้ระบบมีข้อความแจ้งเตือนผู้ใช้ (Error Message) ที่สามารถสื่อสารให้ลูกค้าเกิดความเข้าใจที่ถูกต้อง และต้องไม่แสดงข้อมูลภายในของระบบ เช่น ยี่ห้อรุ่น หรือ Application Path เป็นต้น แต่ควรแสดงรหัสที่บอกถึงสาเหตุของการทำงานที่ผิดพลาด ที่สามารถเข้าใจได้เฉพาะบุคลากรที่รับมอบอำนาจเท่านั้น

5. การรับชำระการซื้อสินค้าและบริการผ่านร้านค้า e-Commerce

ตัวอย่าง Flowchart กระบวนการทำงาน



หมายเหตุ: "**7.ตรวจสอบประเภทรายการ และประเภทบัตร*" เป็นขั้นตอนเพื่อเลือกตัดสินว่าจะส่งรายการไปตัดเงินผ่านตัวกลาง Switching ใด (เช่น กรณีรายการบัตรเดบิทซื้อสินค้าในประเทศจะต้องตัดเงินผ่าน Local Switching, หรือกรณีรายการบัตร Visa หรือ Master Card จะต้องถูกส่งรายการไปตัดคนละวง Switching กัน

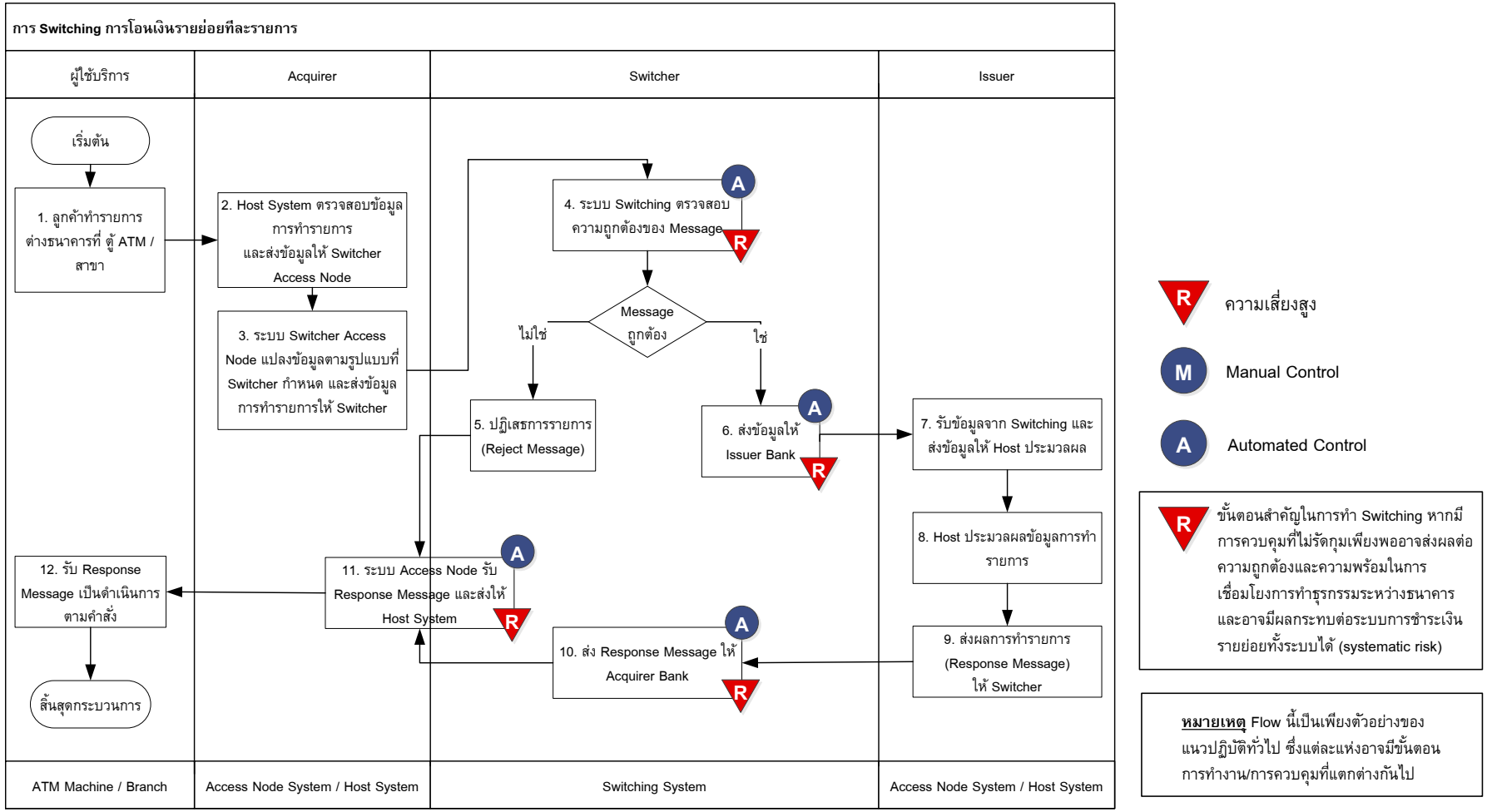
ตารางการควบคุมที่สำคัญ

5. การรับชำระการซื้อสินค้าและบริการผ่านร้านค้า e-Commerce (Payment Gateway)		
วัตถุประสงค์ เพื่อให้การดำเนินการของผู้ให้บริการ Payment Gateway มีความรัดกุมปลอดภัย น่าเชื่อถือ และพร้อมใช้งาน สอดคล้องกับมาตรฐานสากลและเป็นไปตามกฎหมายหลักเกณฑ์ที่เกี่ยวข้อง		
ขั้นตอน	**แนวปฏิบัติที่ดี**	
การส่ง/รับคำสั่งชำระสินค้าและบริการ	5.1	มีระบบตรวจสอบความถูกต้องของข้อมูลรายการชำระเงินที่รับจากร้านค้าสมาชิก **ตัวอย่างเช่น** ▪ 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 ระหว่างระบบงานให้ครอบคลุมเหตุการณ์กรณีต่าง 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. การทำ Switching และ Clearing รองรับการโอนเงินรายย่อยทีละรายการ (Single Payment) และการโอนเงินครั้งละหลายรายการ (Bulk payment)

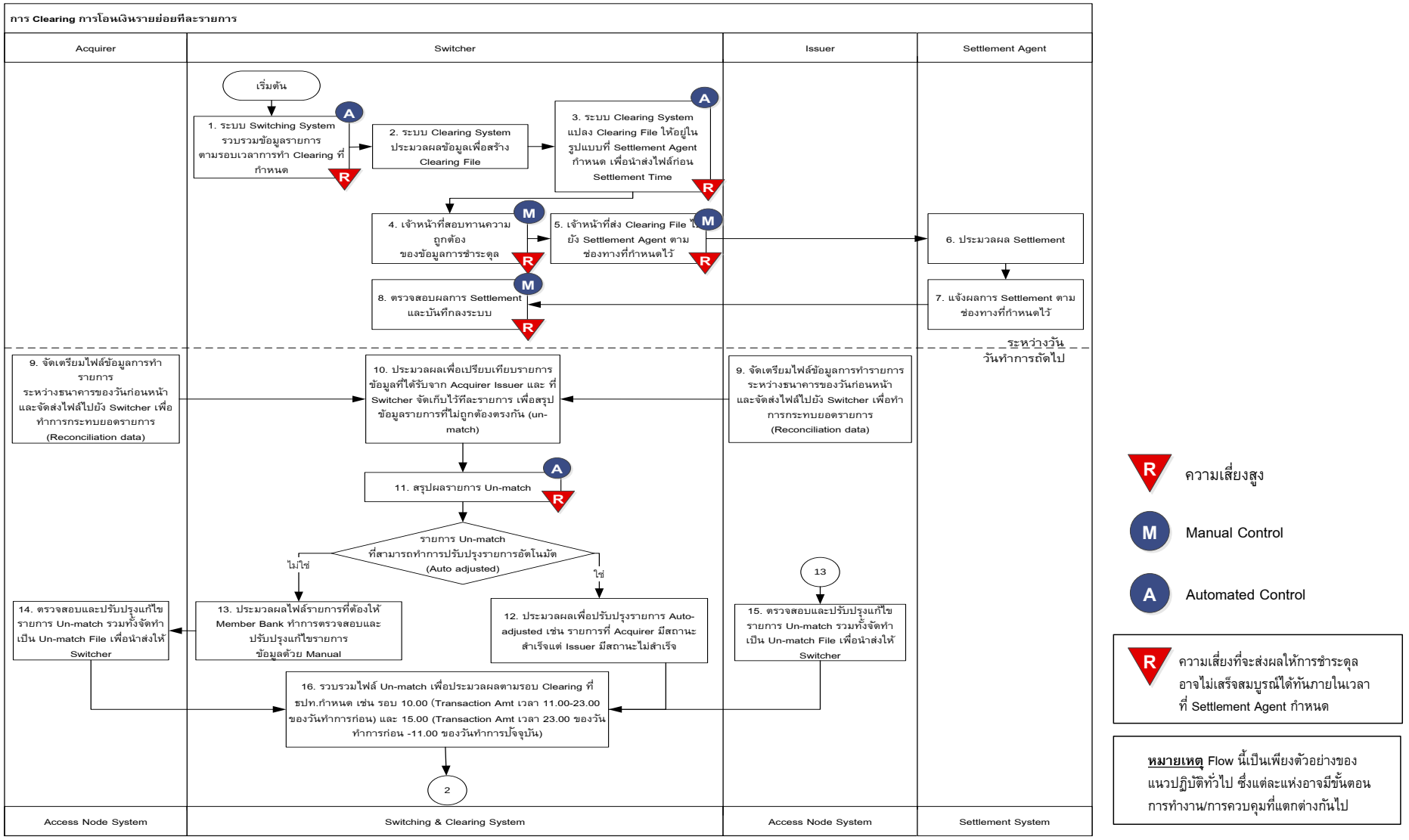
6.1 การ Switching การโอนเงินรายย่อยทีละรายการ

ตัวอย่าง Flowchart กระบวนการทำงาน



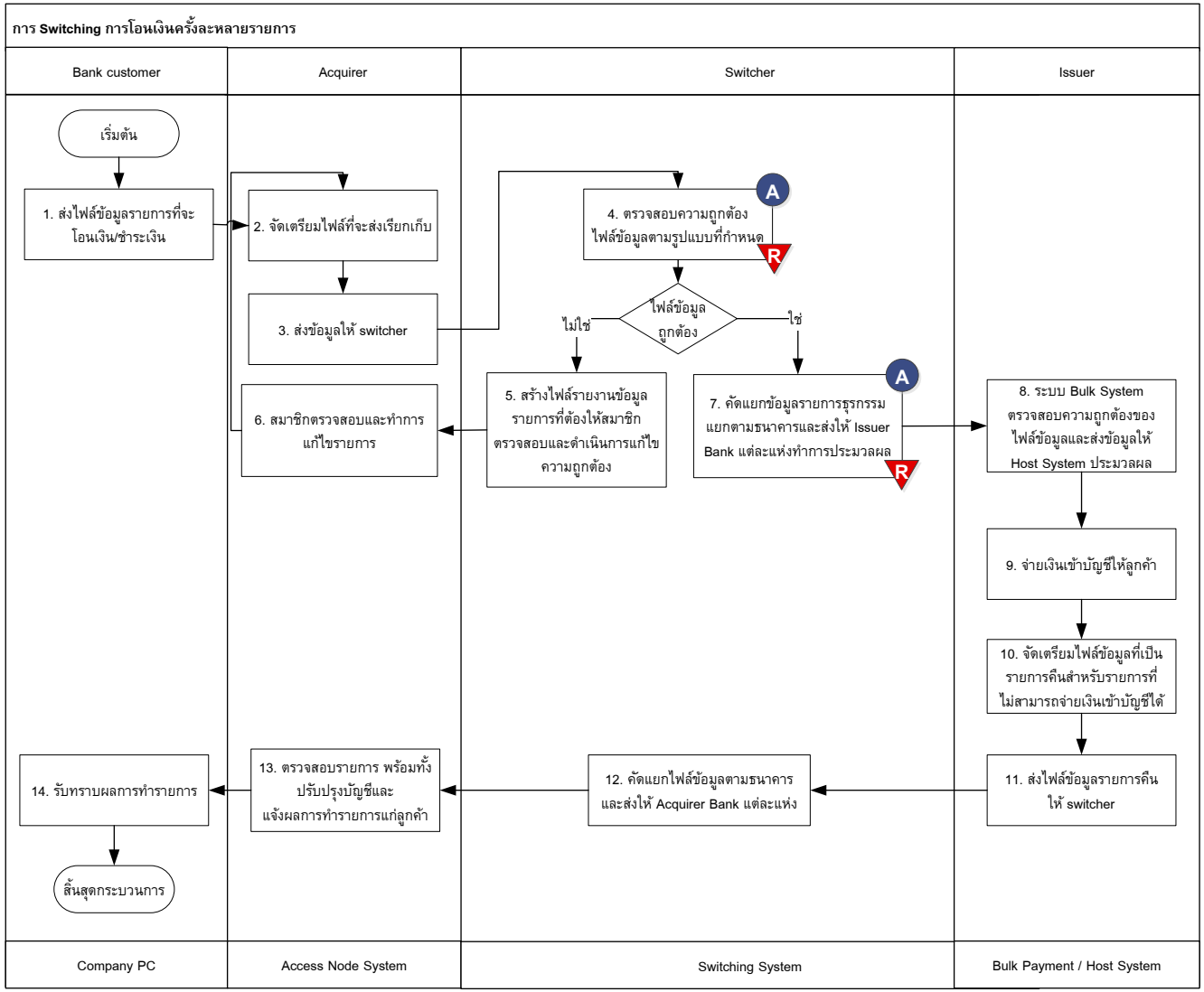
6.2 การ Clearing การโอนเงินรายย่อยทีละรายการ

ตัวอย่าง Flowchart กระบวนการทำงาน



6.3 การ Switching การโอนเงินครั้งละหลายรายการ

ตัวอย่าง Flowchart กระบวนการทำงาน



R ความเสี่ยงสูง

M Manual Control

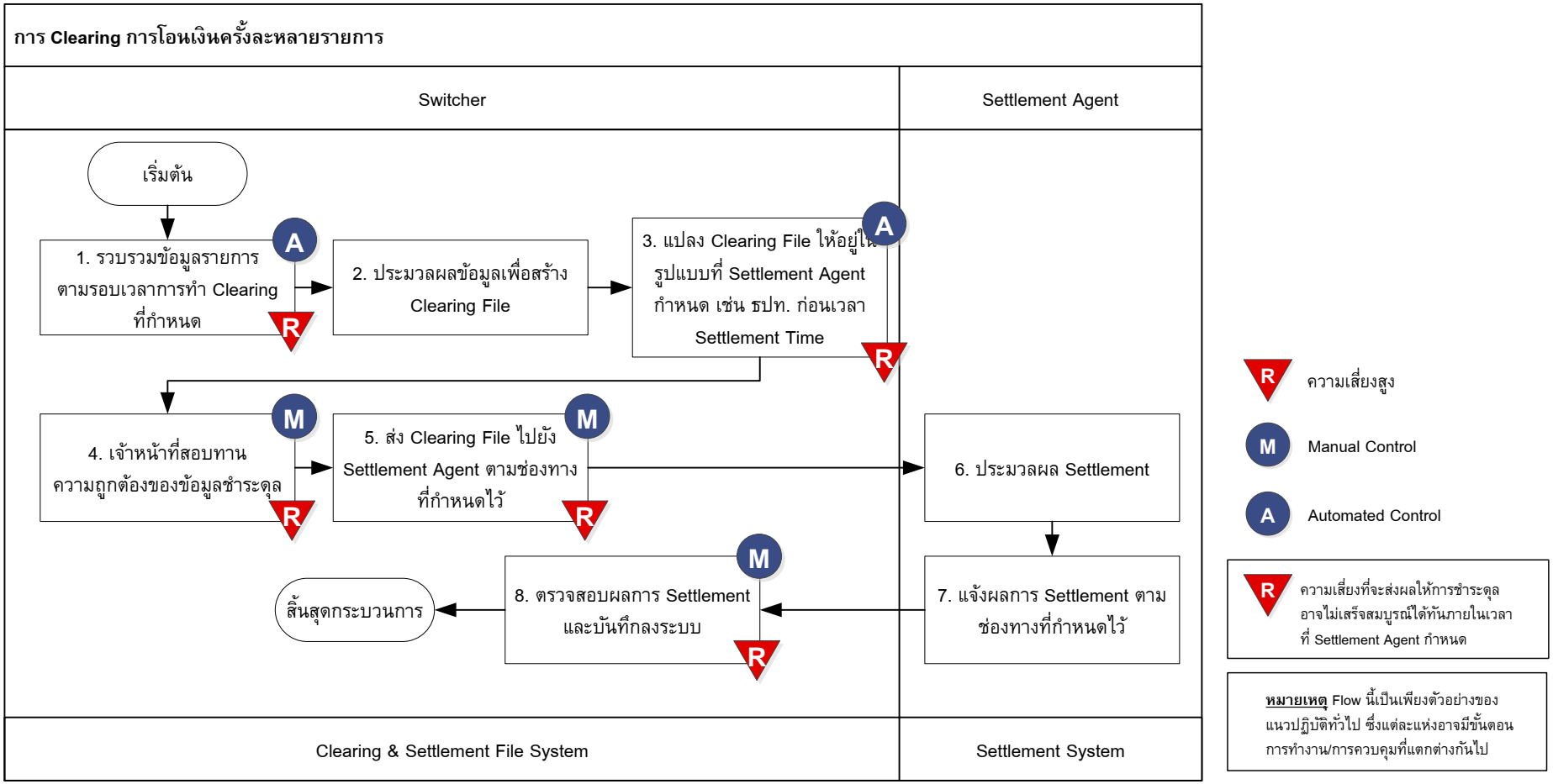
A Automated Control

R ขั้นตอนสำคัญในการทำ Switching หากมีการควบคุมที่ไม่รัดกุมเพียงพออาจส่งผลต่อความถูกต้องและความพร้อมในการเชื่อมโยงการทำธุรกรรมระหว่างธนาคาร และอาจมีผลกระทบต่อระบบการชำระเงินรายย่อยทั้งระบบได้ (systematic risk)

หมายเหตุ Flow นี้เป็นเพียงตัวอย่างของแนวปฏิบัติทั่วไป ซึ่งแต่ละแห่งอาจมีขั้นตอนการทำงาน/การควบคุมที่แตกต่างกันไป

6.4 การ Clearing การโอนเงินครั้งละหลายรายการ

ตัวอย่าง Flowchart กระบวนการทำงาน



ตารางการควบคุมที่สำคัญ

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 โดยมีการลงนามร่วมกัน ระหว่างผู้ให้บริการและสมาชิก ข้อตกลงข้างต้นควรมีการทบทวนให้มีความเหมาะสมอย่างสม่ำเสมอ
	6.2	มีการกำหนดรูปแบบ Message ที่เป็นมาตรฐานร่วมกันระหว่างสมาชิก และมีระบบการตรวจสอบความถูกต้องของรูปแบบ Message ซึ่งหากพบว่า Message อยู่ในรูปแบบที่ไม่ถูกต้อง ควรมีการแจ้งกลับ และปฏิเสธการรับ Message ก่อนประมวลผลในขั้นตอนต่อไป
	6.3	มีการกำหนดมาตรฐานของช่วงเวลา (time out) ในการส่งและรับ Message ระหว่างระบบงานให้ครอบคลุมเหตุการณ์กรณีต่าง 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 และทำให้มั่นใจว่าระบบมีความพร้อมและเหมาะสมกับการใช้งานในปัจจุบัน 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

ขั้นตอน	แนวปฏิบัติที่ดี	
	6.7	มีกระบวนการและ/หรือเครื่องมือในการติดตามและเฝ้าระวังไม่ให้เกิดปัญหาในการให้บริการ และมีแนวปฏิบัติในการตอบสนองและจัดการกับปัญหาที่เกิดขึ้นร่วมกับสมาชิกอย่างชัดเจน รวมถึงกำหนดช่องทางการติดต่อสื่อสารและรายชื่อผู้ประสานงานทั้งผู้ให้บริการและสมาชิกที่เหมาะสม ชัดเจน และมีประสิทธิภาพ
	6.8	มีกระบวนการในการจัดการการเปลี่ยนแปลงอย่างเหมาะสม สำหรับทุกระบบงานที่เกี่ยวข้อง รวมถึงระบบงานภายในของสมาชิกแต่ละรายที่อาจส่งผลกระทบต่อการให้บริการ Switching โดยรวม โดยควรมีการดำเนินการดังต่อไปนี้ เป็นอย่างน้อย 1. มีการวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลงที่จะดำเนินการ 2. มีช่องทาง วิธีการ และกระบวนการในการสื่อสาร ชี้แจ้งข้อมูลการเปลี่ยนแปลงและทำความเข้าใจร่วมกันระหว่างผู้เกี่ยวข้องรวมถึง ธปท. อย่างชัดเจนและเป็นทางการ โดยมีการบันทึกเป็นความตกลงร่วมกันเป็นลายลักษณ์อักษร 3. มีการทดสอบระบบที่เกี่ยวข้องร่วมกัน ซึ่งอาจพิจารณาให้มีการทดสอบร่วมกันทั้งวง Switching (Industry-Wide Test) ในกรณีการเปลี่ยนแปลงมีนัยสำคัญ หรืออาจกระทบต่อระบบโดยรวม โดยมีขั้นตอนการลงนามรับรองผลการทดสอบ และจัดเก็บเอกสารประกอบการทดสอบอย่างเป็นระบบ 4. มีการจัดเตรียมแผนย้อนกลับ (Roll Back Plan) และแผนสำรองฉุกเฉินกรณีที่ทำการเปลี่ยนแปลงไม่สำเร็จ (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

ขั้นตอน	แนวปฏิบัติที่ดี	
	6.13	มีระบบการจัดเก็บข้อมูลการ Clearing อย่างเพียงพอสำหรับใช้ในการพิสูจน์การทำรายการระหว่างสมาชิกย้อนหลัง โดยจัดเก็บเป็นระยะเวลาไม่ต่ำกว่าที่กฎหมายกำหนด และมีการควบคุมการเข้าถึงข้อมูลดังกล่าว
	6.14	มีช่องทางและระบบให้สมาชิกสามารถเรียกดูข้อมูลที่เกี่ยวข้อง และสามารถนำออกไปใช้ประมวลผลในระบบงานของสมาชิกได้ ได้แก่ ▪ ยอดดุลระหว่างวันแบบ Real-time เพื่อให้สมาชิกสามารถใช้บริหารจัดการสภาพคล่อง ▪ สรุปยอดดุลในแต่ละรอบ Clearing และหรือแต่ละวัน
	6.15	มีการกำหนดนโยบาย/ปฏิบัติ ให้ครอบคลุมเหตุติดขัดต่าง ๆ ที่อาจเกิดขึ้น เพื่อให้มั่นใจว่าการชำระดุลจะดำเนินต่อไปได้ เช่น เมื่อมีสมาชิกบางรายไม่สามารถชำระดุลได้ ผู้ให้บริการอาจดำเนินการ Unwind (การหักยอดของสมาชิกรายที่มีปัญหาออก แล้วคำนวณ Netting Position ของสมาชิกที่เหลือใหม่) และส่งชำระดุลด้วยยอดใหม่ หรือผู้ให้บริการอาจจะให้สมาชิกดังกล่าวกู้เพื่อให้สามารถชำระดุลได้สำเร็จ

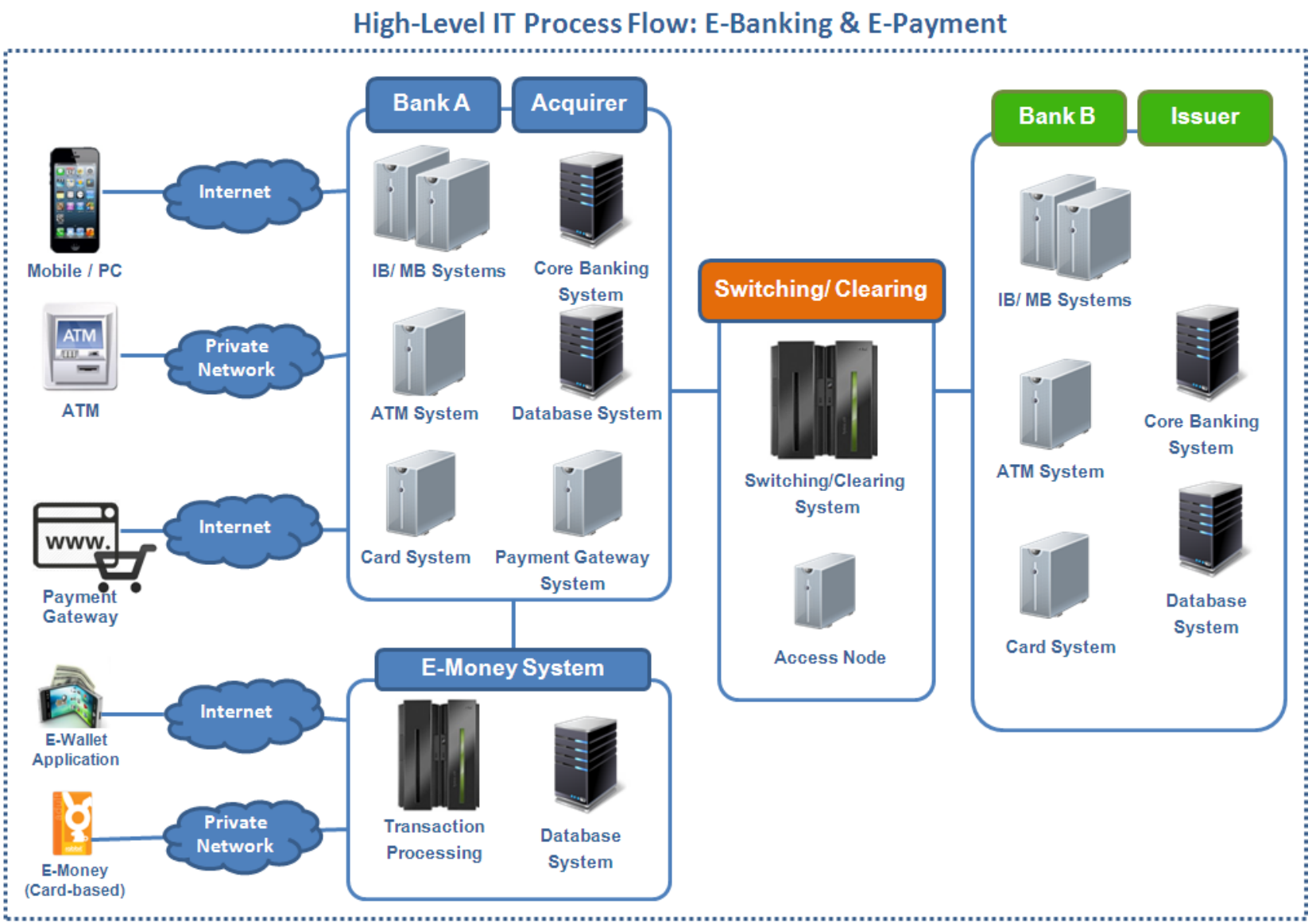
ตารางการควบคุมที่สำคัญ

7. การควบคุมเพิ่มเติมที่สำคัญ	
วัตถุประสงค์ เพื่อให้ธนาคารมีการควบคุมเพิ่มเติมที่สำคัญ เกี่ยวกับการคุ้มครองผู้ใช้บริการธุรกรรมการเงินทางอิเล็กทรอนิกส์ซึ่งเป็นไปตามหลักเกณฑ์มาตรฐานสากลและกฎหมายที่เกี่ยวข้อง	
แนวปฏิบัติที่ดี	
7.1	มีการเสริมสร้างความรู้ความเข้าใจเกี่ยวกับความปลอดภัยในการใช้บริการธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์ ซึ่งรวมถึงความเสี่ยงหรือภัยคุกคามต่าง ๆ ในปัจจุบันที่อาจเกิดขึ้น ข้อควรระวังและวิธีป้องกันแก่ผู้ใช้บริการอย่างสม่ำเสมอ
7.2	มีการกำหนดช่องทางที่ผู้ใช้บริการสามารถติดต่อแจ้งข่าวสาร เหตุการณ์ทางด้านความมั่นคงปลอดภัย หรือร้องเรียนปัญหาการใช้บริการมายังธนาคาร และมีกระบวนการจัดการเรื่องร้องเรียนที่สามารถรองรับการแก้ไขปัญหาในการทำธุรกรรมได้
7.3	มีการติดตามลักษณะการใช้งานที่ต้องสงสัยหรือเข้าข่ายเป็นการทุจริต รวมถึงรายการที่เข้าข่ายตามเกณฑ์ของสำนักงานป้องกันและปราบปรามการฟอกเงิน (AML/CFT) เพื่อป้องกันความเสี่ยงและการทุจริตที่อาจเกิดขึ้นได้อย่างทันท่วงที
7.4	มีการจัดเก็บข้อมูลรายละเอียดการทำรายการอย่างถูกต้อง เช่น สถานะของรายการ วันและเวลาที่ทำรายการ จุดรับรายการ หรือข้อมูลระบุตัวตนของอุปกรณ์ที่ทำรายการ เป็นต้น เพื่อให้ลูกค้าสามารถตรวจสอบ เรียกดูรายการย้อนหลังได้ และเพื่อเป็นหลักฐานทางอิเล็กทรอนิกส์ที่ใช้พิสูจน์การทำรายการ (Audit Trail) โดยจัดเก็บเป็นระยะเวลาไม่ต่ำกว่าที่กฎหมายกำหนด
7.5	มีการประเมินความเสี่ยงของการให้บริการการเงินทางอิเล็กทรอนิกส์อย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงเกี่ยวกับระบบการให้บริการ รวมถึงเมื่อมีภัยคุกคามใหม่ ๆ เกิดขึ้นที่อาจกระทบความมั่นคงปลอดภัยของการให้บริการ และประเมินสิทธิภาพของกลไก/วิธีการควบคุมที่ใช้อยู่ เพื่อจะได้ทำการปรับปรุงให้เพียงพอและทันสมัยยิ่งขึ้น

ส่วนที่ 2
แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบ IT ที่รองรับธุรกรรมทางอิเล็กทรอนิกส์

Phase 2 : ธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์
การให้บริการการเงินและการชำระเงินทางอิเล็กทรอนิกส์ (E-Banking และ E-Payment)

แผนภาพ High-Level IT Process Flow ของ E-Banking และ E-Payment



ในช่วงปีที่ผ่านมา การทุจริตผ่านทางช่องทางอิเล็กทรอนิกส์มีความซับซ้อนขึ้น ใช้เทคโนโลยีที่มีวิวัฒนาการสูงขึ้น รวมทั้งกระทำเป็นขบวนการข้ามชาติ รวมถึงระบบการรักษาความปลอดภัยของการให้บริการธุรกรรมการเงินทางอิเล็กทรอนิกส์ที่องค์กรหลายแห่งใช้ ก็ปรากฏช่องโหว่ที่เป็นความเสี่ยงต่อความมั่นคงปลอดภัยของระบบการให้บริการฯ ซึ่งเหตุการณ์ภัยคุกคามต่าง ๆ ที่เกิดขึ้นในระยะหลัง ก่อให้เกิดความเสียหายทางการเงินของลูกค้าวงกว้างขึ้น ส่งผลกระทบต่อชื่อเสียงภาพลักษณ์ของ ธพ. และหากเกิดขึ้นกับระบบบริการอิเล็กทรอนิกส์ที่เป็นโครงสร้างพื้นฐานของการทำธุรกรรมของประเทศ เช่น e-Payment ก็อาจก่อให้เกิดความเสี่ยงเชิงระบบ (Systemic Risk) ที่กระทบต่อเสถียรภาพและความมั่นคงของระบบสถาบันการเงินของประเทศได้

ธปท. ได้ตระหนักถึงความเสี่ยงด้านภัยคุกคามทางไซเบอร์ จึงได้ศึกษา Framework for Improving Critical Infrastructure Cyber Security ที่จัดทำโดย National Institute of Standards and Technology (NIST) ร่วมกับ ISACA ซึ่งกล่าวถึงหลักการบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ ประกอบด้วยการระบุความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Identify) การป้องกัน (Protect) การตรวจพบ (Detect) การรับมือ (Respond) และการกู้คืน (Recover) โดยได้นำมาใช้กำหนดเป็นแนวปฏิบัติที่ดีสำหรับการบริหารจัดการภัยคุกคามทางไซเบอร์ เพื่อให้ ธพ. มีแนวทางสำหรับนำไปใช้ปรับปรุงการกำกับดูแลและบริหารความเสี่ยงด้าน IT ขององค์กร ให้มีความครอบคลุม และพร้อมรับมือกับความเสี่ยงด้านภัยคุกคามทางไซเบอร์มากยิ่งขึ้น

อย่างไรก็ตาม โครงสร้างระบบ IT ที่สำคัญในการสนับสนุนกระบวนการทางธุรกิจของ E-Banking และ E-Payment ประกอบด้วย ศูนย์คอมพิวเตอร์ ระบบงานธุรกิจหลัก (เช่น Core Banking System) และระบบเครือข่ายสื่อสาร จึงขอให้ ธพ. อ้างถึงแนวปฏิบัติที่ดีสำหรับการควบคุมระบบ IT ที่ได้ระบุไว้แล้วใน IT Best Practice Phase 1 ซึ่งมีกรอบหลักการควบคุม IT 3 ด้าน[11] คือ Access Control, Security Management และ Availability Management นอกจากนี้ เพื่อให้ ธพ. เกิดความเข้าใจอย่างต่อเนื่องและสะดวกในการนำไปใช้งาน จึงได้นำแนวปฏิบัติที่ดีในส่วนของระบบ Internet Banking Security ของ IT Best Practice Phase 1 มาแสดงไว้ใน Appendix A ของฉบับนี้ด้วย

แนวปฏิบัติที่ดีสำหรับการบริหารจัดการภัยคุกคามทางไซเบอร์ สามารถแบ่งได้เป็น 3 ระดับชั้น คือ

(1) Cybersecurity Governance : การกำกับดูแลความเสี่ยงในระดับองค์กร (Enterprise-Wide) ให้ครอบคลุมความเสี่ยงด้านภัยคุกคามทางไซเบอร์ โดยคณะกรรมการและผู้บริหารระดับสูง เพื่อให้การกำกับดูแลความเสี่ยงขององค์กร (Enterprise-Wide) ครอบคลุมภัยคุกคามทางไซเบอร์ใหม่ ๆ ที่เกิดขึ้น

(2) Cybersecurity Risk Management : การกำหนดกรอบนโยบายการบริหารความเสี่ยงด้านภัยคุกคามทางไซเบอร์และการประสานความร่วมมือทั้งภายในและภายนอกองค์กร เพื่อให้พร้อมรับมือและกำหนดแนวทางป้องกันภัยคุกคามทางไซเบอร์ใหม่ ๆ ที่เกิดขึ้น

(3) Cybersecurity Operation : การกำหนดกระบวนการและเครื่องมือเพื่อเพิ่มประสิทธิภาพในการระบุความเสี่ยงจากภัยคุกคามทางไซเบอร์ การป้องกัน การตรวจพบ การรับมือ และการกู้คืน

[11] *กรอบหลักการควบคุมด้าน IT ด้าน คือ (1) Access Control คือ การควบคุมระบบ IT เพื่อป้องกันการถูกบุกรุกและเข้าถึงโดยไม่ได้รับอนุญาต (2) Security Management คือ การบริหารจัดการระบบ IT ให้มีความปลอดภัย เพื่อให้ระบบและข้อมูลมีความถูกต้อง และ (3) Availability Management คือ การบริหารจัดการระบบ IT ให้มีความพร้อมในการรองรับการทำธุรกรรมอย่างต่อเนื่อง*

ตารางการควบคุมที่สำคัญ

กรอบการบริหารจัดการภัยคุกคามทางไซเบอร์ **Cyber Security**		
วัตถุประสงค์ เพื่อให้ ธพ. มีการกำกับดูแล นโยบาย กระบวนการ และเครื่องมือในการบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ ที่สามารถระบุความเสี่ยง ป้องกัน ตรวจพบ รับมือ และกู้คืนกลับสู่สภาวะปกติสอดคล้องตามหลักการบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์สากล เพื่อให้การบริหารความเสี่ยงและความมั่นคงปลอดภัยของการให้บริการทางอิเล็กทรอนิกส์ มีความครอบคลุมและสามารถป้องกันความเสียหายได้อย่างทันท่วงที		
ขั้นตอน		**แนวปฏิบัติที่ดี**
Cyber Security Governance **1. การกำกับดูแลความเสี่ยงด้านภัยคุกคามทางไซเบอร์**		
การกำกับดูแลโดยคณะกรรมการและผู้บริหารระดับสูง	1.1	Board and Senior Management Role & Responsibility มีการมอบหมายบทบาทหน้าที่ให้แก่คณะกรรมการและผู้บริหารระดับสูงของธนาคารในการกำกับดูแลความเสี่ยงด้านภัยคุกคามทางไซเบอร์ เพื่อสนับสนุนให้มีมาตรฐานการรักษาความปลอดภัยที่มีขีดความสามารถเพียงพอเหมาะสมตามปริมาณและความซับซ้อนของธุรกิจ ในการป้องกัน รับมือ และลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์ที่อาจกระทบต่อการให้บริการธุรกรรมทางอิเล็กทรอนิกส์
	1.2	Enterprise Risk Governance ▪ มีการนำกรอบการกำกับดูแลความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cyber Risk Governance) มาเป็นส่วนหนึ่งของการกำกับดูแลความเสี่ยงขององค์กรโดยรวม (Enterprise Risk Governance) รวมถึงมีการรายงานข้อมูลความเสี่ยงด้านภัยคุกคามทางไซเบอร์ให้คณะกรรมการและผู้บริหารระดับสูงที่ได้รับมอบหมายรับทราบเป็นประจำ ▪ ในกรณีเกิดเหตุการณ์ปัญหาที่กระทบต่อการให้บริการแก่ลูกค้าเป็นวงกว้าง ให้มีการรายงานให้คณะกรรมการและผู้บริหารระดับสูงของธนาคารรับทราบโดยเร็ว
	1.3	Resource Allocation มีการจัดสรรทรัพยากรในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทั้งด้านบุคลากรที่มีความเชี่ยวชาญ กระบวนการ และเทคโนโลยีที่เหมาะสมเพียงพอรองรับการติดตามและป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยกำหนดให้มีการรายงานผลการประเมินต่อคณะกรรมการและผู้บริหารระดับสูงที่ได้รับมอบหมายทราบเป็นประจำ
	1.4	Performance Measurement มีการประเมินประสิทธิภาพของมาตรการที่ใช้ในการรักษาความมั่นคงปลอดภัยการให้บริการผ่านช่องทางอิเล็กทรอนิกส์ โดยรายงานผลการประเมินต่อคณะกรรมการและผู้บริหารระดับสูงที่ได้รับมอบหมายทราบเป็นประจำ

ขั้นตอน		แนวปฏิบัติที่ดี
Cyber Security Management **2. การบริหารความเสี่ยงด้านภัยคุกคามทางไซเบอร์**		
	2.1	Security Policy & Procedure มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่ครอบคลุมถึงการระบุความเสี่ยงด้านภัยคุกคามทางไซเบอร์ การป้องกัน การตรวจพบ การรับมือ และการกู้คืน รวมทั้งควรมีการทบทวนนโยบายและมาตรการดังกล่าวอย่างสม่ำเสมอ เพื่อให้เท่าทันต่อการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศและภัยคุกคามใหม่ ๆ
	2.2	Change Management Process มีกระบวนการบริหารจัดการการเปลี่ยนแปลง เพื่อควบคุมการเปลี่ยนแปลงแก้ไขที่เกิดขึ้นกับข้อมูล ระบบงาน และอุปกรณ์สารสนเทศ เช่น การเปลี่ยนแปลงโปรแกรม การเปลี่ยนแปลงการตั้งค่าความปลอดภัย การเปลี่ยนแปลงแก้ไข Patch หรือ Software Update เป็นต้น ให้เป็นไปอย่างมีประสิทธิภาพ
	2.3	Secure System Development Life Cycle มีกระบวนการในการพัฒนาระบบงานอย่างมั่นคงปลอดภัย ไม่ว่าธนาคารจะทำการพัฒนาระบบเองหรือมีการว่าจ้างพัฒนาระบบโดยผู้ให้บริการภายนอก โดยในทุก ๆ ขั้นตอนของกระบวนการพัฒนาระบบงานควรนำแง่มุมของความปลอดภัยมาร่วมพิจารณาด้วย เช่น การคำนึงถึงความต้องการทางด้านความปลอดภัยของระบบงาน(Security Requirement) การออกแบบระบบงานอย่างปลอดภัย (Secure Design) การเขียนโปรแกรมอย่างปลอดภัย (Secure Coding) การสอบทานรหัสต้นฉบับ (Source Code Review) การทดสอบความปลอดภัยของระบบงาน (Security Testing) เป็นต้น
	2.4	Cyber Security Unit มีการกำหนดบทบาทและหน้าที่ความรับผิดชอบในการประเมิน ติดตามดูแล ป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ให้แก่ฝ่ายงานหรือบุคลากรภายในธนาคารอย่างชัดเจน
	2.5	Security Risk Assessment มีการประเมินความเสี่ยงด้านภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอจากฝ่ายงานที่มีความเชี่ยวชาญและเกี่ยวข้อง และพิจารณาแนวทางลดความเสี่ยงที่เหมาะสมตามระดับความเสี่ยงที่ยอมรับได้ (Cyber Risk Appetite)
	2.6	Security Awareness มีการเสริมสร้างความรู้ความเข้าใจเกี่ยวกับภัยคุกคามด้านไซเบอร์ต่าง ๆ ที่อาจเกิดขึ้น รวมถึงมีการสื่อสารแนวทางการป้องกันและรับมือเหตุการณ์ภัยคุกคามต่าง ๆ ให้แก่พนักงานและผู้เกี่ยวข้องได้รับทราบ เช่น ผู้ให้บริการภายนอก ลูกค้า เป็นต้น เพื่อจะได้ตระหนักถึงความจำเป็นในการรักษาความปลอดภัย และเข้าใจถึงผลกระทบที่อาจเกิดขึ้น

ขั้นตอน		แนวปฏิบัติที่ดี
	2.7	Security Collaboration ■ มีช่องทางและกระบวนการประสานงานระหว่างหน่วยงานต่าง ๆ ภายในองค์กร รวมถึงการประสานงานกับองค์กรภายนอกที่ชัดเจน เช่น สถาบันการเงินอื่น ผู้ให้บริการด้านการสื่อสาร ผู้ให้บริการด้านอุปกรณ์ระบบงานหรือระบบรักษาความปลอดภัย หน่วยงานของทางการ เป็นต้น เพื่อกำหนดแนวทางในการรับมือและแก้ไขเหตุการณ์ทางด้านความปลอดภัยได้อย่างมีประสิทธิภาพและทันท่วงที ■ มีการแลกเปลี่ยนข้อมูลทางด้านความปลอดภัยทางไซเบอร์ กับองค์กรภายนอกเพื่อให้รู้เท่าทันสถานการณ์ภัยคุกคามใหม่ ๆ เพื่อการปรับปรุงนโยบายและมาตรการทางด้านการรักษาความปลอดภัยให้ทันกับความเสี่ยงทางไซเบอร์ที่เปลี่ยนแปลง
	2.8	Communications มีกระบวนการสื่อสารกับประชาชนและองค์กรภายนอกที่ชัดเจน เมื่อเกิดเหตุการณ์ทางด้านความมั่นคงปลอดภัย โดยควรครอบคลุมเรื่องดังต่อไปนี้ ■ การเตรียมแผนการสื่อสารเหตุการณ์ทางด้านความปลอดภัยกับสื่อ และลูกค้าผ่านทางช่องทางต่าง ๆ ของธนาคาร ■ การรายงานเหตุการณ์ปัญหาและการหยุดให้บริการ ที่มีนัยสำคัญและอาจส่งผลกระทบต่อลูกค้าในวงกว้าง ให้ ธปท. รับทราบ ตามข้อกำหนดของมาตรา 18 แห่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 ■ การจัดอบรมบุคลากรให้มีความรู้ ความเข้าใจถึงบทบาทหน้าที่ของตนในการสื่อสารกับสื่อต่าง ๆ เช่น หนังสือพิมพ์ สื่อ Online และ Social Network เป็นต้น รวมถึงผลกระทบที่อาจเกิดขึ้นกับองค์กรอันเป็นผลมาจากการสื่อสารที่ไม่มีประสิทธิภาพ
Cyber Security Operation **3. กระบวนการปฏิบัติงานด้านความมั่นคงปลอดภัยทางไซเบอร์**		
Security Prevention[12]	3.1	Asset Management มีการบริหารจัดการทรัพย์สินที่เกี่ยวข้องกับการให้บริการทางอิเล็กทรอนิกส์ โดยระบุทรัพย์สินที่เกี่ยวข้อง และมีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ (เช่น ประเภทอุปกรณ์ ชื่อและรุ่นของซอฟท์แวร์ที่ใช้งาน ผู้ดูแลทรัพย์สิน) อย่างครอบคลุมและชัดเจน ประเมินระดับความเสี่ยงของทรัพย์สิน และกำหนดแนวทางการรักษาความปลอดภัยแก่ทรัพย์สินที่เหมาะสมตามระดับความเสี่ยง
	3.2	Security Baseline Configuration มีการกำหนดมาตรฐานขั้นต่ำในการตั้งค่าความปลอดภัยของอุปกรณ์สารสนเทศและระบบงาน รวมทั้งมีการทบทวนและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

[12] *แนวทางควบคุมความเสี่ยงจากภัยคุกคามทางไซเบอร์ ปรากฏตาม Appendix B*

ขั้นตอน		แนวปฏิบัติที่ดี
	3.3	**Access Control** มีการควบคุมการเข้าถึงทรัพยากรเครือข่ายและระบบงานอย่างเข้มงวดด้วยวิธีการพิสูจน์ตัวตนที่ปลอดภัยเหมาะสมกับระดับความสำคัญของข้อมูลรวมถึงมีการบริหารจัดการบัญชีผู้ใช้งานและรหัสผ่านอย่างครบวงจรการใช้งานตั้งแต่การสร้างบัญชี การเปลี่ยนแปลง จนถึงการยกเลิกบัญชี
	3.4	**Data Security** มีการจัดระดับความสำคัญของข้อมูล โดยคำนึงถึงระเบียบและข้อบังคับทางกฎหมาย และมีมาตรการรักษาความปลอดภัยของข้อมูลที่เหมาะสมกับระดับความสำคัญ ทั้งในการจัดเก็บข้อมูล (Data at Rest) และระหว่างการนำส่งข้อมูล (Data in Transit) เพื่อป้องกันข้อมูลถูกเปิดเผยหรือเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต เช่น มีการเข้ารหัสข้อมูลที่มีความสำคัญด้วยอัลกอริทึมที่มีความมั่นคงแข็งแรง การส่งผ่านข้อมูลด้วยช่องทางที่มีความปลอดภัย เป็นต้น
	3.5	**System Maintenance** มีการบำรุงรักษาอุปกรณ์และซอฟต์แวร์ที่เกี่ยวข้องกับบริการอิเล็กทรอนิกส์อย่างสม่ำเสมอ โดยควรปฏิบัติตามคำแนะนำของผู้ผลิต เพื่อให้อุปกรณ์ดังกล่าวสามารถรองรับการดำเนินงานได้อย่างต่อเนื่อง และการบำรุงรักษาควรดำเนินการด้วยกระบวนการที่มีการควบคุมอย่างรัดกุม[13]
Security Monitoring	3.6	**Monitoring Process** มีกระบวนการติดตามเฝ้าระวัง และตรวจจับเหตุการณ์ภัยคุกคามด้านความปลอดภัยทาง ไซเบอร์อย่างต่อเนื่อง และมีการแจ้งเตือนสิ่งผิดปกติต่าง ๆ ที่เกิดขึ้นไปยังเจ้าหน้าที่ หรือบุคลากรที่มีหน้าที่รับผิดชอบได้อย่างทันท่วงที
	3.7	**Security Events** มีการติดตามเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นทั้งภายในและภายนอกธนาคาร และมีการวิเคราะห์ถึงจุดอ่อน หรือช่องโหว่ที่ก่อให้เกิดเหตุการณ์ภัยคุกคามต่าง ๆ รวมถึงมีกระบวนการประเมินช่องโหว่ (Vulnerability Assessment) และการทดสอบเจาะระบบเครือข่าย (Penetration Test) อย่างน้อยปีละครั้ง เพื่อป้องกันความเสี่ยงและผลกระทบที่อาจเกิดกับธนาคาร
Security Response and Recovery	3.8	**Incident Response Team** มีทีมงานเฉพาะซึ่งมีบทบาทหน้าที่ชัดเจนเพื่อการรับมือเหตุการณ์ผิดปกติทางไซเบอร์ได้อย่างทันท่วงที โดยทีมงานนี้ควรเป็นผู้ที่มีความเชี่ยวชาญด้านระบบการรักษาความปลอดภัยเป็นอย่างดี และมีการประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้องกับเหตุการณ์ดังกล่าวเพื่อระบุ ประเมินผลกระทบที่เกิดขึ้น และหามาตรการในการควบคุมความเสียหายร่วมกันอย่างทันท่วงที

[13] *อ้างอิงข้อ 2.1.1 การควบคุมการเข้าถึงศูนย์คอมพิวเตอร์ทางกายภาพ (Physical Access Control) ส่วนที่ 2 แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบ IT ที่สนับสนุนธุรกิจหลัก Phase 1 ธุรกรรมฝาก ถอนและโอนเงิน*

ขั้นตอน		แนวปฏิบัติที่ดี
	3.9	Incident Management มีแผนการรับมือกับเหตุการณ์หรือภัยคุกคามทางไซเบอร์และแนวทางการแก้ไขปัญหาเบื้องต้นสำหรับการให้บริการทางอิเล็กทรอนิกส์ โดยควรจัดทำขั้นตอนในการรับมือเหตุการณ์ (Response Plan) และแผนกู้คืนระบบ (Recovery Plan) ให้พร้อมดำเนินการเมื่อมีเหตุการณ์เกิดขึ้น
	3.10	Incident Response Process มีกระบวนการรับมือเหตุการณ์ภัยคุกคาม เหตุการณ์ปัญหาข้อขัดข้อง หรือการหยุดชะงักของบริการทางอิเล็กทรอนิกส์ ควรครอบคลุม 3 ด้าน ดังนี้ • **Cure:** กำหนดวิธีการเยียวยาลูกค้าที่ได้รับผลกระทบจากการถูกทุจริตหรือการหยุดชะงักของบริการทางอิเล็กทรอนิกส์ ที่ทันการณ์ เหมาะสม และเป็นธรรม • **Verification:** มีการกำหนดหน่วยงานเพื่อทำหน้าที่ตรวจสอบและวิเคราะห์หาสาเหตุของการทุจริตหรือหยุดชะงักของบริการทางอิเล็กทรอนิกส์เพื่อรายงานให้ผู้บริหารธนาคารและหน่วยงานที่เกี่ยวข้องรับทราบโดยทั่วกัน • **Prevention:** มีการนำ Lesson Learned จากเหตุการณ์ทุจริตหรือหยุดชะงักของบริการทางอิเล็กทรอนิกส์ที่เกิดขึ้นมากำหนดเป็นแนวทางป้องกันปัญหาที่อาจจะเกิดขึ้นอีกในอนาคต
	3.11	Business Continuity Plan มีการจัดทำแผนต่อเนื่องทางธุรกิจที่ครอบคลุมการดำเนินการในกรณีที่เกิดผลกระทบหรือเกิดความเสียหายจากเหตุการณ์ทางด้านความปลอดภัยทางไซเบอร์ รวมถึงควรมีการพิจารณาความต้องการทางด้านความปลอดภัยของการให้บริการในขั้นตอนการจัดทำแผน เพื่อให้สามารถรักษาระดับความปลอดภัยของการให้บริการได้อย่างต่อเนื่องเมื่อเกิดเหตุการณ์ความเสียหายขึ้น

Appendix A
แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงาน IT ที่สนับสนุนธุรกิจหลัก Phase 1 : ธุรกรรมฝากถอนและโอนเงิน ข้อ 2.4.6 Internet Banking Security

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[14] 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
- มีการประเมินความเสี่ยงและช่องโหว่ของ Internet Banking Application อย่างสม่ำเสมอ หรือเมื่อมีภัยใหม่ ๆ และมีการปรับปรุงแก้ไข Application หรือเพิ่มการควบคุมที่จำเป็นอย่างทันท่วงที

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

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
- กำหนดให้ผู้ใช้บริการตั้งค่ารหัสผ่านให้มีความซับซ้อนและยากต่อการคาดเดา โดยรหัสผ่านต้องประกอบไปด้วยตัวอักษร ตัวอักขระพิเศษและตัวเลข
- มีการบังคับให้ผู้ใช้บริการเปลี่ยนรหัสผ่านเมื่อเข้าใช้ระบบงานครั้งแรก หรือได้รับรหัสผ่านใหม่
- หากลูกค้าลืมรหัสผู้ใช้งาน หรือรหัสผ่านต้องมีการพิสูจน์ตัวตนของลูกค้าโดยวิธี Two-Factor Authentication ก่อนให้ลูกค้าทำการ Reset รหัสผ่าน

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)[15] เพื่อยืนยันตัวตนผู้ใช้บริการ ควรกำหนดอายุการใช้งาน OTP ให้มีระยะเวลาไม่เกิน 5 นาที ซึ่ง OTP ที่ถูกสร้างขึ้นมาต้องใช้สำหรับการทำธุรกรรมรายการใดรายการหนึ่งเท่านั้น โดยไม่สามารถใช้กับรายการธุรกรรมอื่น ๆ ได้ โดยในการสร้าง OTP ควรมีการใช้ข้อมูลเกี่ยวกับธุรกรรม เช่น หมายเลขบัญชี จำนวนเงินที่ทำธุรกรรม เป็นต้น มาเป็นส่วนประกอบหนึ่งของการสร้าง OTP ด้วย[16]
- 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

[15] OTP หรือ One Time Password คือ รหัสผ่านที่ใช้เพียงครั้งเดียวสำหรับยืนยันการทำธุรกรรมผ่านทาง Internet/Mobile Banking

[16] ผู้จัดทำได้ตัดข้อความเกี่ยวกับ OTP Transaction Signing ออกจากที่ระบุอยู่ในการควบคุม IT Best Practice - Phase 1 เพื่อความถูกต้องเหมาะสม

Appendix B
ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

แบ่งเป็น 2 รูปแบบ คือ แบบ Technical Threats และแบบ Non-Technical Threats

1. รูปแบบภัยคุกคามในลักษณะ Technical Threats

Phishing

Phishing คือเทคนิคการหลอกลวงด้วยวิธีการส่งอีเมล์หรือ SMS ที่มีเนื้อหาล่อลวงให้ลูกค้าทำการเชื่อมต่อไปยังหน้าเว็บไซต์ปลอมที่ทำเลียนแบบเว็บไซต์ของธนาคาร เพื่อให้ได้มาซึ่งข้อมูลส่วนตัวของผู้ใช้งาน เช่น ชื่อผู้ใช้ รหัสผ่าน เป็นต้น ทั้งนี้ ธนาคารควรมีมาตรการป้องกันภัยคุกคามจาก Phishing โดยการเสริมสร้างความรู้ความเข้าใจ (Awareness) เกี่ยวกับภัยจาก Phishing รวมถึงมีการแนะนำวิธีป้องกันแก่ผู้ใช้บริการรับทราบ นอกจากนี้ ธนาคารอาจมีการใช้ระบบหรือกระบวนการที่สามารถตรวจหาเว็บไซต์ที่ทำเลียนแบบเว็บไซต์ของธนาคาร และมีการประสานงานเพื่อปิดกั้นการเข้าถึงเว็บไซต์ Phishing ที่ตรวจพบ

Malicious Software (Malware)

โดยทั่วไปคำว่า Malware หมายรวมถึง ไวรัส โทรจัน หรือ Worm ซึ่งเป็นโปรแกรมคอมพิวเตอร์ที่มีจุดประสงค์ร้ายต่อทั้งระบบคอมพิวเตอร์ของธนาคารและเครื่องคอมพิวเตอร์ส่วนตัวของลูกค้า โดย Malware จะเข้ามาแอบแฝงในเครื่องคอมพิวเตอร์เพื่อหวังจะขโมยข้อมูลสำคัญหรือสร้างความเสียหายให้กับข้อมูลในระบบคอมพิวเตอร์ นอกจากนั้น Malware ยังสามารถแพร่กระจายไปยังระบบคอมพิวเตอร์อื่น ๆ ที่เชื่อมต่อกันในเครือข่ายจนก่อให้เกิดความเสียหายในวงกว้างได้ ทั้งนี้ ธนาคารควรมีมาตรการป้องกันภัยคุกคามจาก Malware โดยมีการติดตั้งโปรแกรมป้องกันมัลแวร์ให้ครอบคลุมทั้งเครื่องประมวลผลและเครื่องคอมพิวเตอร์ พร้อมทั้งควรปรับปรุงโปรแกรมป้องกันมัลแวร์ให้เป็นปัจจุบัน

Distributed Denial of Service (DDoS)

DDoS คือวิธีการโจมตีระบบการให้บริการของธนาคารผ่านเครือข่ายอินเตอร์เน็ต ทำให้เครื่องคอมพิวเตอร์ปลายทางหยุดทำงานโดยอาศัยการโจมตีจากเครื่องคอมพิวเตอร์จำนวนมากที่ติดไวรัส (Zombie) ซึ่งถูกควบคุมโดยเครื่องคอมพิวเตอร์ของผู้สั่งการ (Command and Control Center) ทั้งนี้ในการควบคุมความเสี่ยงจากการโจมตีแบบ DDoS ธนาคารควรมีแผนการรับมือเหตุการณ์ (Response Plan) และแผนกู้คืนระบบ (Recovery Plan) ประกอบกับควรมีการประสานงานกับผู้ให้บริการอินเตอร์เน็ต (ISP) ในการบริหารจัดการ Traffic เมื่อมีการโจมตีด้วย DDoS เกิดขึ้น นอกจากนี้ควรมีกระบวนการประเมินช่องโหว่ของเครือข่ายและระบบงาน (Vulnerability Assessment) อย่างสม่ำเสมอด้วย

Website Defacement

Website Defacement คือ การโจมตีเว็บไซต์ของธนาคารโดยผู้ไม่หวังดี เพื่อเปลี่ยนแปลงข้อมูลที่เผยแพร่บนหน้าเว็บไซต์ให้มีเนื้อหาเป็นไปตามที่ผู้ไม่หวังดีต้องการโดยมีจุดประสงค์เพื่อต้องการทำลายความน่าเชื่อถือของหน่วยงานเจ้าของเว็บไซต์ ทั้งนี้ธนาคารควรมีการคำนึงถึงความปลอดภัยของระบบงาน Web Application ในขั้นตอนการออกแบบและพัฒนา Web Application รวมถึงมีการทดสอบเจาะระบบ (Penetration Testing) และการประเมินช่องโหว่ (Vulnerability Assessment) ของ Web Application ที่เชื่อมต่อกับอินเตอร์เน็ตโดยผู้เชี่ยวชาญอย่างสม่ำเสมอ

Hacking

Hacking คือ การโจมตีระบบเครือข่ายและระบบงานประมวลผลของธนาคารโดยผู้ไม่หวังดีที่มีความเชี่ยวชาญด้านคอมพิวเตอร์ซึ่งอาศัยช่องโหว่จากระบบ IT ของธนาคารโดยมีจุดประสงค์เพื่อลักลอบขโมยข้อมูลความลับของธนาคาร ข้อมูลส่วนตัวลูกค้า หรือทำลายข้อมูลเพื่อให้เกิดความเสียหายต่อธนาคาร ทั้งนี้ธนาคารควรมีการควบคุมความเสี่ยงจาก Hacking โดยการจัดระบบเครือข่ายโดยแยกตามลำดับความเสี่ยงและความสำคัญของข้อมูล ประกอบกับมีการติดตั้งอุปกรณ์รักษาความปลอดภัยที่มีความสามารถในการควบคุมการบุกรุกระบบเครือข่าย นอกจากนี้ ธนาคารควรมีการทดสอบเจาะระบบ (Penetration Testing) และการประเมินช่องโหว่ของเครือข่ายและระบบงาน (Vulnerability Assessment) ที่เชื่อมต่อกับอินเตอร์เน็ตโดยผู้เชี่ยวชาญอย่างสม่ำเสมอ

2. รูปแบบภัยคุกคามในลักษณะ Non-Technical Threats

Identity Theft

Identity Theft คือ การที่คนร้ายสวมรอยเป็นเหยื่อโดยการลักลอบเอาข้อมูลส่วนตัวของเหยื่อไปใช้โดยไม่ได้รับความยินยอม เช่น นำข้อมูลไปเปิดบัญชีธนาคาร สมัครบัตรเครดิต ทำธุรกรรมการเงิน ขอรับ SIM Card ใหม่ เป็นต้น ธนาคารสามารถลดความเสี่ยงจาก Identity Theft โดยการมีกระบวนการตรวจสอบข้อมูลเอกสารยืนยันตัวตนลูกค้าที่เข้มงวดรัดกุมครอบคลุมช่องทางการให้บริการต่าง ๆ รวมถึงมีการส่งเสริมความรู้ความเข้าใจและฝึกอบรมพนักงานเกี่ยวกับรูปแบบการทุจริตใหม่ ๆ

Social Engineering

Social Engineering เป็นวิธีการหลอกลวงโดยใช้หลักการทางจิตวิทยาหลาย ๆ รูปแบบ เพื่อให้เหยื่อเปิดเผยข้อมูลซึ่งอาจไม่จำเป็นต้องใช้เทคโนโลยีเข้ามาเกี่ยวข้อง เช่น การโทรศัพท์เข้ามาหลอกลวงเหยื่อเพื่อให้เปิดเผยข้อมูลสำคัญหรือหลอกล่อให้เหยื่อกระทำการตามที่ผู้ไม่หวังดีต้องการ การล่อลวงผ่านการเข้าใช้งานเว็บบอร์ด อีเมล์ หรือการแชท เป็นต้น การหลอกลวงในลักษณะนี้ผู้ไม่หวังดีมักจะมีเป้าหมายเพื่อขโมยข้อมูลส่วนตัวที่สำคัญของเหยื่อ เช่น รหัสผ่านของบริการต่าง ๆ เป็นต้น ทั้งนี้ การควบคุมความเสี่ยงจาก Social Engineering นั้น จำเป็นต้องมีการเสริมสร้างความรู้ความเข้าใจเกี่ยวกับวิธีการล่อลวงรูปแบบใหม่ ๆ และมีข้อควรระวังแจ้งแก่ผู้ใช้บริการอย่างสม่ำเสมอ

Insider Fraud

เหตุการณ์ทุจริตที่เกิดขึ้นจากการกระทำของพนักงานหรือคนภายในองค์กร เช่น การนำข้อมูลความลับขององค์กรไปขายหรือส่งต่อให้กับบริษัทคู่แข่ง การลักลอบนำข้อมูลทางการเงินของลูกค้าไปทำทุจริตต่าง ๆ ทั้งนี้ การควบคุมความเสี่ยงจาก Insider Fraud ทำได้หลายแนวทาง ได้แก่ การกำหนดขั้นตอนการปฏิบัติงานของเจ้าหน้าที่ตามหลักการควบคุมที่ดี (เช่น การแบ่งแยกหน้าที่ การสอบทานโดยหัวหน้างาน การจำกัดสิทธิการเข้าถึงข้อมูล เป็นต้น) เพื่อป้องกันข้อมูลขององค์กรรั่วไหล

Appendix C
ตารางสรุปความหมายโดยย่อของคำศัพท์ที่สำคัญ

คำศัพท์	ความหมาย
บริการการเงินทางอิเล็กทรอนิกส์ (E-Banking)	การให้บริการทางการเงินผ่านสื่ออิเล็กทรอนิกส์ต่าง ๆ ซึ่งลูกค้าผู้ใช้บริการสามารถทำรายการได้เอง โดยสำหรับ E-banking ใน IT Best Practice ฉบับนี้ ครอบคลุมถึงธุรกรรมที่ให้บริการผ่านทาง electronic สำหรับลูกค้ารายย่อย ได้แก่ การทำธุรกรรมผ่าน Internet Banking / Mobile banking
การชำระเงินทางอิเล็กทรอนิกส์ (E-Payment)	การโอนสิทธิการถือครองเงินหรือการโอนสิทธิการถอนเงิน หรือหักเงินจากบัญชีเงินฝากของผู้ใช้บริการที่เปิดไว้กับผู้ให้บริการด้วยวิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือบางส่วน
Internet Banking	เป็นบริการที่ให้ลูกค้าสามารถทำธุรกรรมทางการเงินผ่านเครือข่ายอินเทอร์เน็ตด้วยตนเอง โดยอาศัยอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ เช่น เครื่องคอมพิวเตอร์ โทรศัพท์มือถือ หรือสื่ออื่น ๆ ที่ช่วยให้ลูกค้าสามารถทำรายการทางการเงินในลักษณะโต้ตอบกับระบบงานของธนาคารได้เองโดยอัตโนมัติ
Mobile Banking	เป็นบริการอิเล็กทรอนิกส์ที่ลูกค้าสามารถทำธุรกรรมทางการเงินด้วยตนเองผ่านโทรศัพท์มือถือในลักษณะโต้ตอบกับระบบงานของธนาคารได้เองโดยอัตโนมัติ ซึ่งส่วนใหญ่จะใช้เพื่อการโอนเงินและชำระเงิน เพราะสะดวก และสามารถใช้บริการได้ตลอดเวลาที่ต้องการ
บริการเงินอิเล็กทรอนิกส์ (e-Money)	เงินสดที่อยู่ในรูปของสื่อการชำระเงินในรูปแบบต่าง ๆ เช่น บัตรพลาสติกหรือสื่ออิเล็กทรอนิกส์อื่น ๆ เพื่อใช้ในการซื้อสินค้าหรือบริการแทนการจ่ายชำระด้วยเงินสด ทั้งนี้ บัตรเงินสดอิเล็กทรอนิกส์ อาจเรียกเป็นอย่างอื่น เช่น Multipurpose Stored Value Card หรือ e-Purse หรือ e-Wallet หรือ Smart Card เป็นต้น โดยบัตรเงินสดอิเล็กทรอนิกส์จะมีลักษณะสำคัญ 3 ประการ คือ 1. ผู้บริโภคชำระเงินล่วงหน้าให้ผู้ออกบัตรเงินสดอิเล็กทรอนิกส์ (Prepaid) 2. มูลค่าเงินที่ชำระล่วงหน้าถูกบันทึกในสื่ออิเล็กทรอนิกส์ต่าง ๆ (Stored Value) เช่น บัตรพลาสติก หรือสื่อคอมพิวเตอร์อื่น 3. ผู้บริโภคสามารถนำไปใช้ซื้อสินค้าหรือบริการต่าง ๆ ได้จากร้านค้าที่ผู้ออกบัตรเงินสดอิเล็กทรอนิกส์กำหนด (Multipurpose)
บริการสวิตช์ชิ่งในการชำระเงิน (Transaction Switching/Switching)	บริการที่ทำหน้าที่เป็นตัวกลางหรือจุดเชื่อมต่อรับส่งข้อมูลรายการชำระเงินทางอิเล็กทรอนิกส์ให้แก่ผู้ให้บริการตามที่ตกลงกัน
บริการหักบัญชี (Clearing)	บริการรับส่ง ตรวจสอบ และยืนยันข้อมูลตามคำสั่งการชำระเงิน สำหรับนำไปคำนวณหายอดเงินแสดงความเป็นเจ้าหนี้ หรือลูกหนี้ของผู้ใช้บริการ เพื่อใช้ข้อมูลดังกล่าวไปทำการชำระดุลระหว่าง เจ้าหนี้และลูกหนี้ ทั้งนี้ รวมถึงการจัดการเพื่อให้กระบวนการชำระดุลสำเร็จลุล่วงด้วย
บริการชำระดุล (Settlement)	บริการระบบการชำระเงินที่ตกลงกันไว้ล่วงหน้าระหว่างผู้ใช้บริการกับผู้ให้บริการเพื่อให้ผู้ให้บริการปรับฐานะความเป็นเจ้าหนี้ หรือลูกหนี้ของผู้ใช้บริการโดยผู้ให้บริการจะทำการหักบัญชีเงินฝากของผู้ใช้บริการซึ่งมีฐานะเป็นลูกหนี้ หรือรับชำระหนี้โดยวิธีอื่นใดตามที่ตกลงกัน แล้วปรับบัญชีเงินฝากของผู้ใช้บริการซึ่งมีฐานะเป็นเจ้าหนี้ หรือชำระเงินด้วยวิธีอื่นใด เพื่อให้หนี้ดังกล่าวระงับไป

คำศัพท์	ความหมาย
Payment Gateway	บริการเว็บไซต์ที่ทำหน้าที่เป็นตัวกลางในการชำระเงินระหว่างลูกค้าและเว็บไซต์ร้านค้า โดยรับข้อมูลการซื้อสินค้าและบริการจากเว็บไซต์ร้านค้า และลูกค้าจะเป็นผู้ทำรายการชำระเงินผ่านช่องทางการชำระเงินที่รองรับ (เช่น บัตรเครดิต หรือ Internet Banking) ด้วยตนเองด้วยตนเอง
การพาณิชย์อิเล็กทรอนิกส์ (E-Commerce)	การทำธุรกรรมทางเศรษฐกิจที่ผ่านสื่ออิเล็กทรอนิกส์ เช่น การซื้อขายสินค้าและบริการ การโฆษณาสินค้า การโอนเงินทางอิเล็กทรอนิกส์ เป็นต้น
การโอนเงินรายย่อยทีละรายการ (Single Payment)	เป็นบริการที่ผู้โอนเงินสามารถโอนเงินให้ผู้รับเงินที่มีบัญชีอยู่ต่างธนาคารได้ผ่านช่องทางต่าง ๆ เช่น เครื่อง ATM เคาน์เตอร์สาขาธนาคาร หรือบริการ Internet banking โดยผู้รับเงินจะสามารถเบิกเงินในบัญชีได้ทันทีภายหลังจากที่ผู้โอนเงินทำรายการสำเร็จ ทั้งนี้ การโอนเงินผ่านบริการดังกล่าว จะใช้ได้เฉพาะในกลุ่มของธนาคารที่เป็นสมาชิกของแต่ละระบบเท่านั้น
การโอนเงินครั้งละหลายรายการ (Bulk Payment)	บริการผ่านธนาคารเพื่อให้ลูกค้าผู้ใช้บริการโอนเงินให้กับบุคคลอื่น หรือเรียกเก็บเงินจากบุคคลอื่น โดยส่วนใหญ่มักจะมีมูลค่าไม่สูงมาก แต่มีปริมาณรายการมาก และมีรอบการชำระเงินแน่นอน

หมายเหตุ : ความหมายของคำศัพท์นี้เป็นความหมายโดยย่อที่จัดทำขึ้นเพื่อมุ่งเน้นให้ผู้อ่านสามารถเข้าใจได้ง่ายและใช้อ้างอิงเฉพาะในแนวปฏิบัติฉบับนี้

ธนาคารแห่งประเทศไทย

เพื่อความเป็นอยู่ที่ดี อย่างยั่งยืนของไทย