7. ความเสี่ยงด้านปฏิบัติการ

ความเสี่ยงด้านปฏิบัติการ (Operational Risk: OR) หมายถึง ความเสี่ยงที่จะเกิดความเสียหายอันเนื่องมาจากการขาดการกำกับดูแลกิจการที่ดีหรือขาดธรรมาภิบาลในองค์กรและการขาดการควบคุมที่ดี โดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน คน ระบบงาน หรือเหตุการณ์ภายนอก และส่งผลกระทบต่อฐานะการเงิน รายได้ เงินกองทุน และชื่อเสียงของสถาบันการเงิน ทั้งนี้ ความเสี่ยงด้านปฏิบัติการนับรวมถึงความเสี่ยงด้านกฎหมายด้วย

แนวทางการกำกับดูแลของธนาคารแห่งประเทศไทย

1. การบริหารความเสี่ยงด้านปฏิบัติการ
2. การใช้บริการจากผู้ให้บริการรายอื่น (Outsourcing)
3. การใช้เทคโนโลยีสารสนเทศของธนาคารพาณิชย์
4. การจัดทำแผนฉุกเฉิน (Contingency Plan)
5. การป้องกันปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย (AML/CFT)

1. การบริหารความเสี่ยงด้านปฏิบัติการ

เพื่อส่งเสริมให้ธนาคารพาณิชย์พัฒนาการบริหารความเสี่ยงด้านนี้และเตรียมความพร้อมเพื่อรองรับการกำกับดูแลความเสี่ยงด้านปฏิบัติการตาม Basel II ธปท. ได้กำหนดแนวนโยบายในการบริหารความเสี่ยงด้านปฏิบัติการใน 4 เรื่อง ได้แก่

(1) การสร้างและการพัฒนา Operational Risk Management Environment ที่เน้นบทบาทหน้าที่ของคณะกรรมการธนาคารพาณิชย์ เช่น การกำหนดกรอบนโยบาย กลยุทธ์ คำจำกัดความของความเสี่ยงด้านปฏิบัติการที่เหมาะสม การอนุมัตินโยบาย แผนงานและกระบวนการการบริหารความเสี่ยงด้านปฏิบัติการ (Operational Risk Management: ORM) การจัดให้มี ORM Unit และการจัดโครงสร้างองค์กรที่เหมาะสม และเอื้อต่อการบริหาร OR เป็นต้น และบทบาทหน้าที่ของผู้บริหารระดับสูง เช่น การนำกรอบนโยบาย OR มาพัฒนาให้เกิดระเบียบ กฎเกณฑ์ หรือขั้นตอนการปฏิบัติงานในองค์กร การสื่อสารให้พนักงานขององค์กรเห็นความสำคัญและหน้าที่ของทุกคนในเรื่อง OR และการควบคุมให้มีการปฏิบัติตามนโยบาย กฎ ระเบียบที่กำหนดอย่างเคร่งครัด เป็นต้น

(2) ระบบบริหารความเสี่ยงด้านปฏิบัติการ ควรมีองค์ประกอบ คือ มีการระบุความเสี่ยง (Risk Identification) การประเมินความเสี่ยง (Risk Assessment) การติดตามความเสี่ยง (Risk Monitoring) การควบคุมและลดความเสี่ยง (Risk Control/ Mitigation) การจัดเก็บข้อมูลและรายงานความเสี่ยงด้านปฏิบัติการ และการจัดทำแผนฉุกเฉิน

(3) มีการเปิดเผยข้อมูลการบริหารความเสี่ยงด้านปฏิบัติการต่อสาธารณชน รวมทั้งผู้ฝากเงินและผู้มีส่วนได้เสียอย่างเพียงพอ โดยขึ้นกับขนาด ความซับซ้อนของการทำธุรกิจ และความเสี่ยงของธนาคารพาณิชย์แต่ละแห่ง

(4) เพื่อพัฒนาระบบข้อมูลความเสี่ยงด้านปฏิบัติการดังกล่าวและเพื่อเตรียมความพร้อมรองรับ Basel II ธปท. จึงได้ออกหนังสือเวียน เรื่อง การจัดเก็บข้อมูลความเสียหายที่เกิดจากความเสี่ยงด้านปฏิบัติการเพื่อประโยชน์ในการติดตามและบริหารความเสี่ยงด้านปฏิบัติการขององค์กร และเตรียมความพร้อมในการสร้างแบบจำลองทางสถิติในอนาคต

ประกาศและหนังสือเวียนที่เกี่ยวข้อง

1. การจัดเก็บข้อมูลความเสียหายที่เกิดจากความเสี่ยงด้านปฏิบัติการ (17 ส.ค. 2547)
2. Sound Practices for the Management and Supervision of Operational Risk (30 พ.ค. 2546)

2. การใช้บริการจากผู้ให้บริการรายอื่น (Outsourcing)

2.1 การใช้บริการด้านงานหลักจากผู้ให้บริการอื่น

โดยหลักการแล้ว งานหลัก (Core Function) และงานสำคัญ (Material Activity) จะต้องดำเนินการโดยสถาบันการเงินเอง เนื่องจากเป็นงานที่ต้องใช้ความเชี่ยวชาญของการเป็นสถาบันการเงิน หรือเป็นงานที่มีผลกระทบโดยตรงต่อทิศทางการดำเนินธุรกิจและการแข่งขันในระบบสถาบันการเงิน หรือเป็นงานด้านสถาบันการเงินที่มีความสำคัญทางธุรกิจ และหากงานดังกล่าวมีการหยุดชะงักอันเนื่องมาจากผู้ให้บริการรายอื่นไม่สามารถให้บริการได้อย่างต่อเนื่อง จะเกิดผลกระทบรุนแรงต่อการดำเนินธุรกิจของสถาบันการเงิน

อย่างไรก็ดี เพื่อเป็นการอำนวยความสะดวกและเพิ่มช่องทางการใช้บริการให้ประชาชนได้มากขึ้น ธปท.ไม่ขัดข้องหากสถาบันการเงินจะแต่งตั้งผู้ให้บริการอื่นดำเนินการในขอบเขตธุรกรรมดังต่อไปนี้

	ธุรกรรม	ผู้ว่าจ้าง	ผู้เป็นตัวแทน
1.	การรับฝากเงินในบัญชีที่เปิดไว้แล้ว	ธพ. และ บง.	ธพ. ไปรษณีย์ และบริษัทร่วมทุนของไปรษณีย์
2.	การถอนเงินในบัญชีที่เปิดไว้แล้ว	ธพ.	ธพ. ไปรษณีย์ และบริษัทร่วมทุนของไปรษณีย์
3.	การรับชำระสินเชื่อและค่าใช้จ่าย	ธพ. และ บง.	ธพ. ไปรษณีย์ และผู้ให้บริการด้านการโอนเงิน
4.	การจ่ายเงิน (Paying Agent)	ธพ.	ธพ.
5.	การบริหารสินทรัพย์ด้อยคุณภาพ	ธพ. บง. และบค.	บบส.

2.2 การใช้บริการด้านงานสนับสนุนจากผู้ให้บริการรายอื่น

โดยหลักการแล้ว งานด้านสนับสนุนหมายถึง งานปฏิบัติการที่เป็นการเอื้ออำนวยการดำเนินงานตามปกติ รวมถึงงานบัญชีและการเงิน งานเทคโนโลยีสารสนเทศ งานตรวจสอบภายใน งานด้านการกำกับดูแลการปฏิบัติตามกฎหมาย (Compliance) งานบริหารจัดการในการแปลงสินทรัพย์เป็นหลักทรัพย์ ฯลฯ ดังนั้น เพื่อให้เกิดประโยชน์ทางด้านเศรษฐกิจสูงสุด (Economy of scale) แล้ว ธปท. เห็นควรเปิดให้สถาบันการเงินใช้บริการด้านงานสนับสนุนจากผู้ให้บริการรายอื่น โดยให้คณะกรรมการสถาบันการเงินเป็นผู้ให้ความเห็นชอบในการกำหนดนโยบายการใช้บริการดังกล่าว

โดยสถาบันการเงินต้องให้ความสำคัญกับการบริหารความเสี่ยงที่เกี่ยวข้อง และการทำความเข้าใจกับบุคคลที่สามที่เกี่ยวข้องว่าผู้ให้บริการรายนั้นเป็นเพียงผู้รับช่วงการให้บริการ และไม่เข้าข่ายเป็นการเลี่ยงการเปิดสาขา

ทั้งนี้ ธปท. อยู่ระหว่างพิจารณากำหนดแนวปฏิบัติเกี่ยวกับการใช้บริการด้านงานสนับสนุนจากผู้ให้บริการรายอื่นเพื่อความชัดเจนในธุรกรรมที่สามารถกระทำได้

ประกาศและหนังสือเวียนที่เกี่ยวข้อง

1. การใช้บริการด้านงานสนับสนุนจากผู้ให้บริการรายอื่น (Outsourcing) และการแต่งตั้งตัวแทน (ธพ. 5 ก.ย. 2550)
2. การใช้บริการด้านงานสนับสนุนจากผู้ให้บริการรายอื่น (Outsourcing) และการแต่งตั้งตัวแทน (บง. 5 ก.ย. 2550)
3. การใช้บริการด้านงานสนับสนุนจากผู้ให้บริการรายอื่น (Outsourcing) และการแต่งตั้งตัวแทน (บค. 5 ก.ย. 2550)
4. การแต่งตั้งธนาคารพาณิชย์แห่งอื่นเป็นตัวแทนจ่ายเงิน (Paying agent) (24 มี.ค. 2551)
5. การแต่งตั้งตัวแทนรับฝากและถอนเงินของธนาคารพาณิชย์ (5 พ.ย. 2546)

2.3 การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

ปัจจุบัน ธนาคารพาณิชย์มีการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นอย่างแพร่หลายมากขึ้น เพื่อลดต้นทุน เพิ่มขีดความสามารถในการดำเนินงานและพัฒนาศักยภาพการให้บริการให้ทันต่อพัฒนาการของเทคโนโลยีที่มีการเปลี่ยนแปลงอย่างรวดเร็ว ดังนั้น เพื่อให้การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และเป็นการพิทักษ์รักษาประโยชน์ของประชาชนผู้ใช้บริการ ธปท. ได้กำหนดแนวปฏิบัติในการใช้บริการ ฯ ดังนี้

(1) ธนาคารพาณิชย์ยังคงมีความรับผิดชอบต่อการให้บริการอย่างต่อเนื่องแก่ลูกค้า รวมทั้งยังต้องคงความน่าเชื่อถือของการให้บริการเสมือนธนาคารพาณิชย์เป็นผู้ดำเนินการเอง

(2) ควรคำนึงถึงความเสี่ยงด้านกลยุทธ์ และความต่อเนื่องในการพัฒนาศักยภาพในระยะยาวสำหรับการทำธุรกิจหลักของธนาคารพาณิชย์และในกรณีที่ผู้ให้บริการอยู่ต่างประเทศ ควรคำนึงถึงความเสี่ยงด้านกฎหมาย โดยเฉพาะในเรื่องการรักษาความลับข้อมูลของลูกค้า

และความเสี่ยงด้านปฏิบัติการอันเนื่องมาจากความแตกต่างของกฎหมายและกฎระเบียบในแต่ละประเทศที่เกี่ยวกับธุรกรรมข้ามพรมแดน (Cross Border) ด้วย

(3) ต้องจัดให้มีข้อมูลอยู่ในประเทศที่พร้อมสำหรับการดำเนินธุรกิจภายในประเทศ รวมทั้งมีหนังสือยินยอมให้ ธปท. เข้าตรวจสอบการดำเนินงานในส่วนที่เกี่ยวข้องกับการให้บริการด้วย

(4) ต้องจัดให้มีการรักษาความปลอดภัยของข้อมูล และให้ผู้ให้บริการแยกฐานข้อมูลของลูกค้าของธนาคารพาณิชย์ออกจากข้อมูลของผู้ให้บริการหรือลูกค้ารายอื่นของผู้ให้บริการด้วย

(5) ต้องประเมินความเสี่ยงที่เกี่ยวข้องก่อนการใช้บริการ และแจ้งรายละเอียดการใช้บริการให้ ธปท. เพื่อทราบก่อนการเริ่มใช้บริการหรือก่อนวันที่มีการเปลี่ยนแปลงการใช้บริการเป็นเวลาไม่ต่ำกว่า 15 วัน

ประกาศและหนังสือเวียนที่เกี่ยวข้อง

1. การซักซ้อมความเข้าใจเกี่ยวกับแนวปฏิบัติในการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) (26 ก.ย. 2548)
2. แนวปฏิบัติในการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) (14 พ.ค. 2546)

3. การใช้เทคโนโลยีสารสนเทศของธนาคารพาณิชย์

ธนาคารพาณิชย์มีการใช้เทคโนโลยีสารสนเทศอย่างแพร่หลาย เพื่อลดต้นทุนการดำเนินงาน เพิ่มประสิทธิภาพ และสนับสนุนการให้บริการทางการเงินให้มีหลายช่องทาง เพิ่มความสะดวก รวดเร็ว และทันสมัย โดยจำแนกลักษณะการใช้เทคโนโลยีสารสนเทศของธนาคารพาณิชย์ได้ 2 ลักษณะ คือ

(1) การให้บริการการเงินทางอิเล็กทรอนิกส์

ธนาคารพาณิชย์ได้นำเทคโนโลยีสารสนเทศมาใช้ในการออกผลิตภัณฑ์ทางอิเล็กทรอนิกส์ เพื่อให้บริการแก่ลูกค้าผู้ใช้บริการ เช่น บริการ ATM บัตรเดบิต บัตรเครดิต บัตรเงินอิเล็กทรอนิกส์ (e-Money) การให้บริการผ่านเครือข่ายอินเทอร์เน็ต (Internet Banking) เป็นต้น

(2) การดำเนินงานของธนาคารพาณิชย์

ธนาคารพาณิชย์ได้มีการนำเทคโนโลยีสารสนเทศมาใช้เพื่อสนับสนุนการให้บริการแก่ลูกค้าและการดำเนินงานภายในของธนาคารพาณิชย์เอง ทั้งนี้ ธนาคารพาณิชย์สามารถใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น เพื่อลดต้นทุนและพัฒนาศักยภาพการให้บริการให้ทันต่อพัฒนาการของเทคโนโลยีที่มีการเปลี่ยนแปลงอย่างรวดเร็วได้ และในทางตรงข้ามธนาคารพาณิชย์สามารถให้บริการด้านงานสนับสนุนแก่บุคคลอื่นได้ เพื่อให้เกิดประโยชน์สูงสุดในการใช้ทรัพยากรที่มีอยู่

แนวทางการกำกับดูแลของธนาคารแห่งประเทศไทย

การใช้เทคโนโลยีที่หลากหลายมากขึ้น อาจก่อให้เกิดความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ (IT Risk) ซึ่งอาจส่งผลเสียหายต่อการให้บริการและการดำเนินงานของธนาคารพาณิชย์ ธปท. ได้กำหนดหลักเกณฑ์การกำกับดูแลการให้บริการและการดำเนินงานของธนาคารพาณิชย์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ดังนี้

3.1 การให้บริการการเงินทางอิเล็กทรอนิกส์

3.1.1 การให้บริการเครื่องอิเล็กทรอนิกส์

3.1.2 การให้บริการผ่านเครือข่ายอินเทอร์เน็ต

3.1.3 การให้บริการเงินอิเล็กทรอนิกส์

3.2 การดำเนินงานของธนาคารพาณิชย์

3.2.1 การโอนเงินทางอิเล็กทรอนิกส์

3.2.2 การรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์

3.2.3 การให้บริการด้านงานสนับสนุนแก่บุคคลอื่น

3.1 การให้บริการการเงินทางอิเล็กทรอนิกส์

3.1.1 การให้บริการเครื่องอิเล็กทรอนิกส์- เครื่อง ATM

ธนาคารพาณิชย์มีการให้บริการเครื่องอิเล็กทรอนิกส์ในการทำธุรกรรมทางการเงิน ได้แก่ เครื่อง ATM แก่ผู้ใช้บริการ ซึ่งเป็นการให้บริการที่นิยมใช้กันอย่างแพร่หลายมากขึ้น ทำให้ลูกค้ามีความคุ้นเคยกับการใช้บริการดังกล่าว และปัจจุบันธนาคารพาณิชย์ยังพัฒนาความสามารถการให้บริการทางการเงินผ่านเครื่อง ATM ได้หลากหลายรูปแบบมากขึ้น เช่น โอนเงิน ชำระเงินค่าสินค้าหรือบริการ เป็นต้น นอกจากนี้ ธนาคารพาณิชย์ยังให้บริการเครื่องอิเล็กทรอนิกส์เพื่อรับฝากเงิน หรือปรับสมุดบัญชีได้ด้วย โดย ธปท. ได้กำหนดแนวทางการกำกับดูแล ดังนี้

(1) ธปท. อนุญาตให้ธนาคารพาณิชย์เปิดบริการเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงินทั้งในและนอกสำนักงานธนาคารพาณิชย์ได้ตามวันและเวลาที่ต้องการ

(2) เครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงินที่ติดตั้งนอกสำนักงานธนาคารพาณิชย์ ตามกฎหมายถือว่ามีสภาพเป็นสาขาของธนาคารพาณิชย์

(3) ธนาคารพาณิชย์ต้องแจ้งให้ ธปท. ทราบล่วงหน้าเกี่ยวกับรายละเอียดการเปิดบริการเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงิน การเปลี่ยนแปลงสำนักงานที่ดูแลเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงินนอกสำนักงานธนาคารพาณิชย์ และการเปิดหรือหยุดบริการเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงินเป็นการชั่วคราวครั้งละไม่เกิน 90 วัน

(4) ธนาคารพาณิชย์ต้องมีระบบรักษาความปลอดภัยตามที่ ธปท. กำหนด และจัดให้มีการตรวจสอบด้านคอมพิวเตอร์อย่างน้อยปีละครั้ง พร้อมจัดส่งสำเนารายงานผลการตรวจสอบให้ ธปท. ทราบภายใน 45 วันนับจากวันที่เริ่มตรวจสอบ รวมทั้งควรพิจารณาค่าธรรมเนียมในการใช้บัตร ATM ให้เหมาะสม

(5) ธปท. อนุญาตให้ธนาคารพาณิชย์ให้บริษัทประกันภัยเปิดบริการประกันภัยผ่านเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงิน หรือผ่านระบบธนาคารทางโทรศัพท์หรือผ่านระบบธนาคารในสำนักงานได้เพื่ออำนวยความสะดวกให้ประชาชนสามารถทำประกันภัยได้โดยสะดวกขึ้นโดยแจ้งให้ ธปท. ทราบล่วงหน้าตามหลักเกณฑ์ที่ ธปท.กำหนด

นอกจากนี้ ในปัจจุบันปัญหาการทุจริตที่เกิดขึ้นกับการให้บริการผ่านเครื่อง ATM มีเพิ่มขึ้น โดยวิธีการทุจริตที่แพร่หลายได้แก่ การใช้เครื่องบันทึกข้อมูลในแถบแม่เหล็ก (Skimmer)

ติดไว้บริเวณช่องสอดบัตรของเครื่อง ATM เพื่อบันทึกข้อมูลต่าง ๆ ของบัตร และนำไปทำบัตรปลอม ประกอบกับการใช้วิธีการเพื่อให้เจ้าของบัตรเปิดเผยรหัสผ่านหรือลักลอบติดตั้งเครื่องมือเพื่อให้ได้รหัสผ่าน และนำไปใช้ควบคู่กับบัตรปลอมที่ทำขึ้น ซึ่งทำให้ผู้กระทำทุจริตสามารถทำรายการถอนเงินหรือโอนเงินจากบัญชีของเจ้าของบัตรได้

ธปท. ตระหนักถึงปัญหาการทุจริตที่เกิดขึ้น และให้ธนาคารพาณิชย์มีแนวทางป้องกันการทุจริตดังกล่าว ดังนี้

(1) การเพิ่มความระมัดระวังและจัดให้มีมาตรการรักษาความปลอดภัยสำหรับการให้บริการทางการเงินผ่านเครื่อง ATM ให้มีความเหมาะสมกับระดับความเสี่ยงและพื้นที่ที่ ATM ตั้งอยู่ เช่น การจัดให้มีเจ้าหน้าที่ออกไปตรวจสอบเครื่อง ATM อย่างสม่ำเสมอ โดยเฉพาะเครื่อง ATM ที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงต่อการกระทำทุจริต เพื่อป้องกันการลักลอบดัดแปลงหรือติดตั้งเครื่องมือที่ใช้กระทำทุจริตต่าง ๆ ที่เครื่อง ATM หรือการพิจารณาติดตั้งกล้องโทรทัศน์วงจรปิดที่เครื่อง ATM เป็นต้น

(2) การให้ข้อมูลและคำแนะนำที่เป็นประโยชน์แก่ลูกค้า เพื่อให้ลูกค้าสามารถใช้บริการทางการเงินผ่านเครื่อง ATM ได้อย่างปลอดภัย

(3) การจัดให้มีช่องทางในการรับแจ้งปัญหาและข้อร้องเรียนจากลูกค้า

(4) การดูแลและรับผิดชอบลูกค้าให้ได้รับความคุ้มครองจากความสูญเสียที่เกิดจากการกระทำทุจริตโดยบุคคลอื่น ในกรณีเกิดรายการโอนเงินทางอิเล็กทรอนิกส์โดยมิชอบและมิใช่ความผิดของผู้ใช้บริการ หากลูกค้าผู้ใช้บริการดำเนินการตามขั้นตอนปกติและต้องสูญเสียเงิน จากการที่บุคคลภายนอกผู้กระทำทุจริตใช้เครื่อง Skimmer ติดกับเครื่อง ATM และลักลอบบันทึกข้อมูลในแถบแม่เหล็ก เป็นเหตุให้เกิดความสูญเสียต่อลูกค้า สถาบันการเงินย่อมต้องรับผิดชดใช้ความสูญเสียให้แก่ลูกค้ารายนั้นด้วย

(5) การนำแนวทางป้องกันข้างต้นไปประยุกต์ใช้กับการให้บริการการเงินทางอิเล็กทรอนิกส์ประเภทอื่นที่มีความเสี่ยงในลักษณะเดียวกัน

ประกาศและหนังสือเวียนที่เกี่ยวข้อง

1. แนวทางป้องกันการทุจริตโดยการใช้เครื่องบันทึกข้อมูลในแถบแม่เหล็ก (Skimming) ดึงข้อมูลบัตรลูกค้าจากเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงิน (เครื่อง ATM) เพื่อทำบัตรปลอม (26 ก.พ. 2547)
2. การเปิดบริการเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงิน (21 ต.ค. 2535)
3. การให้บริษัทประกันภัยเปิดบริการผ่านเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงินและเครื่องอิเล็กทรอนิกส์อื่น (6 ก.ย. 2532)
4. การส่งรายงานการตรวจสอบด้านคอมพิวเตอร์ ตามหลักเกณฑ์และเงื่อนไขในการอนุญาตให้ธนาคารพาณิชย์เปิดบริการด้วยเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงิน (30 ก.ค. 2529)
5. การให้บริการเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงินโดยบริษัททั่วไปซึ่งมิใช่ธนาคารพาณิชย์ (2 พ.ค. 2528)

3.1.2 การให้บริการผ่านเครือข่ายอินเทอร์เน็ต

การใช้บริการเครือข่ายอินเทอร์เน็ตในการประกอบธุรกิจ ธนาคารพาณิชย์ต้องขออนุญาตจาก ธปท. ตามความในมาตรา 9 ทวิ แห่ง พ.ร.บ. การธนาคารพาณิชย์ พ.ศ. 2505 และที่แก้ไขเพิ่มเติม (ดูรายละเอียดที่ การประกอบธุรกิจผ่านเครือข่ายอินเทอร์เน็ต (Internet))

ในปัจจุบันได้เกิดปัญหาการทุจริตบนเครือข่าย Internet ด้วยวิธี Phishing คือการโจมตีในรูปแบบของการปลอมแปลง e-mail (e-mail Spoofing) และสร้าง Website ปลอมเพื่อทำการหลอกลวงให้เหยื่อผู้รับ e-mail เปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนบุคคลอื่น ๆ ซึ่งจะสร้างความเสียหายทางการเงินต่อลูกค้าและธนาคารพาณิชย์

ธปท. ได้ออกหนังสือเวียนถึงธนาคารพาณิชย์เพื่อให้ตระหนักถึงปัญหาการทุจริตที่เกิดขึ้น รวมทั้งจัดให้มีมาตรการป้องกันและแจ้งเตือนลูกค้าเกี่ยวกับการทุจริตที่อาจเกิดขึ้น ดังนี้

(1) การเพิ่มความระมัดระวังและจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับการให้บริการทางการเงิน เช่น ในกรณีที่สถาบันการเงินมีการให้บริการส่ง e-mail ไปยังลูกค้า สถาบันการเงินต้องไม่แนบลิงค์เพื่อเชื่อมโยง Website ของสถาบันการเงิน หรือแบบฟอร์มการสอบถามข้อมูลส่วนบุคคลไปให้ลูกค้า หรือสถาบันการเงินควรพิจารณากำหนดวงเงินสูงสุดในการโอนเงินที่เหมาะสม

(2) การให้ข้อมูลและคำแนะนำที่เป็นประโยชน์แก่ลูกค้า เพื่อให้ลูกค้าสามารถใช้บริการการเงินทางอิเล็กทรอนิกส์ได้อย่างปลอดภัย

(3) การจัดให้มีช่องทางในการรับแจ้งปัญหาและข้อร้องเรียนจากลูกค้า โดยอย่างน้อยควรจัดให้มีหมายเลขโทรศัพท์ที่ลูกค้าสามารถติดต่อได้ ในกรณีที่พบเหตุการณ์หรือรายการผิดปกติต่าง ๆ

ประกาศและหนังสือเวียนที่เกี่ยวข้อง

1. แนวทางการป้องกันการทุจริตผ่านเครือข่ายอินเทอร์เน็ตด้วยวิธี Phishing (12 เม.ย. 2548)
2. การใช้บริการเครือข่ายอินเทอร์เน็ต (Internet) ในการประกอบธุรกิจของธนาคารพาณิชย์ (15 พ.ย. 2543)

3.1.3 การให้บริการเงินอิเล็กทรอนิกส์

การให้บริการเงินอิเล็กทรอนิกส์ ธนาคารพาณิชย์ต้องขออนุญาตจาก ธปท. ตามความในมาตรา 9 ทวิ แห่ง พ.ร.บ. การธนาคารพาณิชย์ พ.ศ. 2505 และที่แก้ไขเพิ่มเติม (ดูรายละเอียดที่ การให้บริการเงินอิเล็กทรอนิกส์ (Electronic Money))

ประกาศและหนังสือเวียนที่เกี่ยวข้อง

1. แนวนโยบายการกำกับดูแลการให้บริการเงินอิเล็กทรอนิกส์ (Electronic Money) (10 ก.พ. 2547)

3.2 การดำเนินงานของธนาคารพาณิชย์

3.2.1 การโอนเงินทางอิเล็กทรอนิกส์

การโอนเงินทางอิเล็กทรอนิกส์ หมายถึง การโอนเงินที่กระทำผ่านเครื่องเทอร์มินอลหรืออุปกรณ์สื่อสารทางอิเล็กทรอนิกส์ หรือเครื่องคอมพิวเตอร์ หรือสื่อบันทึกข้อมูลคอมพิวเตอร์เพื่อสั่งให้ธนาคารพาณิชย์โอนเงินเข้าหรือออกจากบัญชี เช่น เครื่อง ATM เครื่องรูดบัตรเครดิต Internet Banking เป็นต้น

การให้บริการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าว อาจทำให้เกิดความเสี่ยงในรูปแบบต่าง ๆ ที่ก่อให้เกิดความเสียหายได้ง่าย และมีหลักฐานที่แตกต่างจากการโอนเงินทางตราสาร ซึ่งเป็นสาเหตุของปัญหาและข้อโต้แย้งที่อาจเกิดขึ้นได้ระหว่างธนาคารพาณิชย์และลูกค้า

ผู้ใช้บริการ โดยส่วนหนึ่งมักเกิดจากการขาดเอกสารหลักฐานเพื่อยืนยันข้อเท็จจริง และไม่ทราบขั้นตอนการปฏิบัติที่ถูกต้อง

ธปท. ได้กำหนดหลักเกณฑ์การให้บริการโอนเงินทางอิเล็กทรอนิกส์ เพื่อให้ธนาคารพาณิชย์ใช้เป็นแนวทางและวิธีปฏิบัติ เพื่อให้เกิดความเป็นธรรมแก่ทุกฝ่ายที่เกี่ยวข้อง และเพิ่มความเชื่อมั่นต่อสาธารณชนมากยิ่งขึ้น สรุปได้ดังนี้

(1) การโอนเงินจะเสร็จสมบูรณ์ต่อเมื่อผู้รับโอนหรือผู้รับประโยชน์ได้รับเงินสดหรือได้รับเครดิตบัญชีให้ครบถ้วนตามจำนวนเงินที่โอนเข้าบัญชีของผู้รับเงินจากธนาคารผู้โอนหรือธนาคารผู้รับโอนเรียบร้อยแล้ว และผู้รับโอนสามารถใช้เงินนั้นได้

(2) ต้องจัดทำข้อตกลงหรือสัญญาการให้บริการโอนเงินทางอิเล็กทรอนิกส์กับผู้ใช้บริการเป็นลายลักษณ์อักษรอย่างน้อย 2 ฉบับ และมอบให้ผู้ใช้บริการเก็บไว้เป็นหลักฐาน 1 ฉบับ

(3) ธนาคารพาณิชย์จะออกเครื่องมือโอนเงิน เช่น บัตร ATM บัตรเครดิตให้แก่ผู้ใช้บริการได้ในกรณีได้รับคำขอจากผู้ใช้บริการ หรือเพื่อทดแทนเครื่องมือโอนเงินเดิมที่ขาดชำรุด สูญหาย หรือถูกโจรกรรม หรือครบกำหนดเวลาที่ต้องเปลี่ยนแทน

(4) ต้องจัดทำคู่มือหรือเอกสารเพื่ออธิบายขั้นตอน หรือวิธีการใช้บริการให้ผู้ใช้บริการทราบ

(5) ให้จัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานที่สามารถเรียกใช้และเข้าใจได้ง่าย

(6) ต้องดำเนินการอายัดหรือระงับการใช้เครื่องมือโอนเงินหรือการโอนเงินที่มีข้อตกลงล่วงหน้าพร้อมทั้งจัดทำหลักฐานการรับแจ้งไว้ทันที เมื่อผู้ใช้บริการแจ้งอายัดและผู้ใช้บริการไม่ต้องรับผิดชอบความเสียหายต่าง ๆ ที่เกิดขึ้นภายหลังการแจ้งอายัด

(7) ต้องจัดทำและมอบใบบันทึกรายการให้ผู้ใช้บริการทันทีและทุกครั้งของการทำรายการ ภายหลังจากที่ผู้ใช้บริการทำรายการโอนเงินเสร็จสิ้นสมบูรณ์ตามขั้นตอนที่กำหนดไว้ทุกรายการ เว้นแต่ธนาคารพาณิชย์ได้แจ้งให้ลูกค้าทราบเป็นการล่วงหน้าแล้วหรือเป็นเหตุสุดวิสัย

(8) ต้องดำเนินการสอบสวนข้อผิดพลาดในการโอนเงินที่ได้รับแจ้งจากผู้ใช้บริการพร้อมทั้งดำเนินการแก้ไขข้อผิดพลาดให้เสร็จสิ้นภายใน 30 วันนับแต่วันที่ได้รับแจ้ง และต้องแจ้งให้ผู้ใช้บริการหรือเจ้าของบัญชีทราบภายใน 7 วัน นับแต่วันที่ทราบผลการสอบสวนนั้น

(9) กรณีที่จะแก้ไขเปลี่ยนแปลงข้อกำหนดหรือเงื่อนไขใด ๆ ในข้อตกลงหรือสัญญาการให้บริการธนาคารพาณิชย์ต้องแจ้งให้ผู้ใช้บริการทราบล่วงหน้าไม่น้อยกว่า 15 วัน

ประกาศและหนังสือเวียนที่เกี่ยวข้อง

1. หลักเกณฑ์การให้บริการโอนเงินทางอิเล็กทรอนิกส์ (5 ก.ค. 2537)

3.2.2 การรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์

การให้บริการทางการเงินผ่านสื่ออิเล็กทรอนิกส์ต่าง ๆ มากขึ้น เพื่อให้สามารถลดต้นทุน ตอบสนองความต้องการของผู้ใช้บริการได้อย่างรวดเร็ว และเพิ่มประสิทธิภาพในการแข่งขัน ทำให้เกิดความเสี่ยงด้านความปลอดภัยของข้อมูล ระบบ และเครือข่ายที่ใช้ในการให้บริการ

ธปท. ได้กำหนดแนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ เพื่อให้ธนาคารพาณิชย์ใช้เป็นแนวทางในการกำหนดนโยบายและกระบวนการในการรักษาความปลอดภัยสำหรับการให้บริการการเงินทางอิเล็กทรอนิกส์ ดังนี้

(1) คณะกรรมการธนาคารพาณิชย์มีหน้าที่กำหนดนโยบายการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ที่เป็นลายลักษณ์อักษรและอนุมัติกระบวนการรักษาความปลอดภัยที่ฝ่ายจัดการเสนอ และคณะกรรมการต้องกำหนดให้มีผู้บริหารและพนักงานที่รับผิดชอบในการดำเนินการให้เป็นไปตามนโยบายและกระบวนการที่ได้รับการอนุมัติ นอกจากนั้น คณะกรรมการต้องจัดให้มีการประเมินประสิทธิภาพของนโยบายและกระบวนการรักษาความปลอดภัยอย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัย

(2) กระบวนการหลักในการรักษาความปลอดภัย ประกอบด้วย กระบวนการควบคุมการเข้าถึงระบบให้บริการและข้อมูล (Access Control) การตรวจสอบตัวตนลูกค้าและการป้องกันการปฏิเสธความรับผิด (Authentication & Non-repudiation) การรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการและข้อมูล การรักษาความลับของข้อมูล (System and Data Integrity) การรักษาความพร้อมใช้ของระบบให้บริการ (System Availability) การติดตามตรวจสอบความผิดปกติและความล่อแหลมของระบบให้บริการ (System Detection) และการแก้ไขปัญหาและการรายงานในกรณีระบบให้บริการได้รับความเสียหายจากภัยคุกคาม (Incident Response & Report)

(3) ควรจัดให้มีการฝึกอบรมและให้ความรู้อย่างต่อเนื่องแก่ผู้บริหารและพนักงานทุกระดับที่เกี่ยวข้องกับการให้บริการ เพื่อให้สามารถปฏิบัติตามนโยบายและกระบวนการรักษาความปลอดภัยได้อย่างมีประสิทธิภาพ นอกจากนั้น ควรให้ข้อมูลและคำแนะนำที่เป็นประโยชน์แก่ลูกค้า รวมทั้งจัดให้มีกระบวนการควบคุมภายในที่เหมาะสมกับการให้บริการการเงินทางอิเล็กทรอนิกส์ ซึ่งจะช่วยเสริมให้นโยบายและกระบวนการรักษาความปลอดภัยมีประสิทธิภาพมากยิ่งขึ้น

ประกาศและหนังสือเวียนที่เกี่ยวข้อง

1. แนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ (19 พ.ย. 2546)

3.2.3 การให้บริการด้านงานสนับสนุนแก่บุคคลอื่น

ธปท. อนุญาตให้ธนาคารพาณิชย์ประกอบธุรกิจการให้บริการด้านงานสนับสนุนแก่บุคคลอื่นได้ ตามความในมาตรา 9 ทวิ แห่ง พ.ร.บ. การธนาคารพาณิชย์ พ.ศ. 2505 และที่แก้ไขเพิ่มเติม (ดูรายละเอียดที่ การให้บริการด้านงานสนับสนุนแก่บุคคลอื่น)

ประกาศและหนังสือเวียนที่เกี่ยวข้อง

1. การอนุญาตให้ธนาคารพาณิชย์ให้บริการด้านงานสนับสนุนแก่บุคคลอื่น (14 ธ.ค. 2549)

4. การจัดทำแผนฉุกเฉิน (Contingency Plan)

4.1 การบริหารความเสี่ยงต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM/Business Continuity Plan: BCP)

การบริหารความต่อเนื่องทางธุรกิจ (BCM/BCP) คือ แนวทางในการกำหนดนโยบาย มาตรฐาน และกระบวนการทำงานของทั้งองค์กรเพื่อให้มั่นใจว่าในกรณีที่มีเหตุการณ์ที่ทำให้การปฏิบัติงานตามปกติต้องหยุดชะงักลง โดยหน่วยงานที่สำคัญ (Critical Business Functions) จะสามารถดำเนินการได้อย่างต่อเนื่องหรือกลับมาดำเนินการในเวลาที่เหมาะสม

ธปท. ได้ออกแนวปฏิบัติ เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ของธนาคารพาณิชย์ โดยครอบคลุมแนวทางและประเด็นสำคัญสำหรับการบริหารความต่อเนื่องทางธุรกิจ และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของสถาบันการเงิน ซึ่งสถาบันการเงินแต่ละแห่งควรพิจารณานำไปปรับใช้และกำหนดรายละเอียดให้เหมาะสมกับประเภทและความซับซ้อนของธุรกิจของตนเอง

<u>ข้อกำหนดสำคัญที่สถาบันการเงินพึงปฏิบัติ</u>

- คณะกรรมการและผู้บริหารระดับสูงเป็นผู้รับผิดชอบในการกำหนดกลยุทธ์และนโยบายการบริหารความต่อเนื่องทางธุรกิจของธนาคารพาณิชย์ (Business Continuity Management) พร้อมทั้ง จัดสรรทรัพยากรเพื่อรองรับการดำเนินงานอย่างเพียงพอ และพิจารณาความเสี่ยงในด้านการบริหารและการควบคุมให้มีการปฏิบัติตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องดังกล่าว โดยถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงโดยรวมด้วย
- ธนาคารพาณิชย์ควรจัดให้มีการระบุธุรกรรมงานที่สำคัญ (Critical Business Functions) และประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการหยุดชะงักของธุรกรรมงานที่สำคัญ พร้อมทั้งกำหนดระยะเวลาหยุดดำเนินงานที่ยอมรับได้ และกลยุทธ์การกู้การดำเนินงานที่เสียหายให้กลับคืนสู่ภาวะปกติที่เหมาะสมกับแต่ละธุรกรรมงาน
- ธนาคารพาณิชย์ควรจัดให้มีการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) ที่เป็นลายลักษณ์อักษรให้ครอบคลุมทุกธุรกรรมงานที่สำคัญในองค์กร รวมถึงผู้ให้บริการหลักที่เกี่ยวข้องด้วย

- ธนาคารพาณิชย์ควรจัดให้มีการทดสอบและทบทวนแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องสำหรับธุรกรรมงานที่สำคัญอย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงปัจจัยที่มีผลต่อความเสี่ยงในการเกิดการหยุดชะงักของการดำเนินงานที่มีนัยสำคัญ
- หากมีการหยุดการให้บริการของธุรกรรมงานที่สำคัญธนาคารพาณิชย์ควรแจ้ง ธปท. ภายในโอกาสแรกที่ทำได้และไม่เกิน 24 ชั่วโมง พร้อมทั้งรายงานรายละเอียดของเหตุการณ์ที่เกิดขึ้น ขั้นตอนการดำเนินการและระยะเวลาที่คาดว่าจะใช้ในการแก้ไขปัญหา และเมื่อธุรกรรมงานที่สำคัญดังกล่าวกลับมาดำเนินการได้ตามปกติ ให้แจ้ง ธปท. รับทราบด้วย

ประกาศและหนังสือเวียนที่เกี่ยวข้อง

1. การบริหารความต่อเนื่องทางธุรกิจและการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (23 ม.ค. 2550)

4.2 การจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ (IT Contingency Plan)

ธนาคารพาณิชย์มีการใช้เทคโนโลยีสารสนเทศเพื่อสนับสนุนการดำเนินงานและการให้บริการอย่างกว้างขวาง เพื่อเพิ่มความสะดวก รวดเร็ว และประสิทธิภาพในการทำงาน รวมทั้ง มีการเชื่อมโยงเครือข่ายภายในและภายนอกองค์กร ทั้งในประเทศและต่างประเทศ ซึ่งหากมีเหตุการณ์ที่ส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศย่อมส่งผลกระทบต่อธุรกิจของธนาคารพาณิชย์ทำให้ไม่สามารถให้บริการลูกค้าได้อย่างต่อเนื่องและส่งผลกระทบเป็นวงกว้างต่อองค์กรอื่นที่มีเครือข่ายเชื่อมโยงกัน

เพื่อให้ธนาคารพาณิชย์สามารถดำเนินธุรกิจได้อย่างต่อเนื่องหรือมีผลกระทบน้อยที่สุดหลังจากเกิดเหตุการณ์ที่ทำให้การดำเนินงานของระบบที่อาศัยเทคโนโลยีสารสนเทศหยุดชะงัก ธปท. ได้กำหนดให้ธนาคารพาณิชย์จัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ (แผนฉุกเฉินด้าน IT) และจัดให้มีระบบคอมพิวเตอร์สำรองนอกอาคารที่ตั้งศูนย์คอมพิวเตอร์หลัก รวมทั้งการหยุดให้บริการแก่ลูกค้าอันมีสาเหตุจากระบบคอมพิวเตอร์ขัดข้องหรือเสียหายจะหยุดเกิน 1 วันทำการไม่ได้ เว้นแต่จะได้รับอนุญาตจาก ธปท.

กระบวนการรองรับเหตุการณ์ความเสียหายเป็นสิ่งสำคัญที่ธนาคารพาณิชย์จะนำมาใช้เมื่อเกิดปัญหาขึ้น การเตรียมการที่ดีย่อมจะช่วยลดผลกระทบต่าง ๆ และช่วยฟื้นฟูระบบเทคโนโลยีสารสนเทศของธนาคารพาณิชย์กลับคืนสู่สภาพปกติได้ภายในเวลาที่ยอมรับได้

ธปท. ได้กำหนดแนวปฏิบัติในการจัดทำแผนฉุกเฉินด้าน IT ดังนี้

(1) บทบาทและความรับผิดชอบของคณะกรรมการธนาคารพาณิชย์ ในการกำหนดนโยบายและแนวทางในการจัดทำแผนฉุกเฉินด้าน IT

(2) การกำหนดนโยบายและแนวทางในการจัดทำแผนฉุกเฉินด้าน IT ซึ่งควรมีความสอดคล้องกับนโยบายการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและนโยบายการบริหารความเสี่ยง

(3) กระบวนการหลักในการจัดทำแผนฉุกเฉินด้าน IT ที่มีประสิทธิภาพและสามารถนำมาใช้รองรับเหตุการณ์ความเสี่ยงหายที่เกิดขึ้นได้

ประกาศและหนังสือเวียนที่เกี่ยวข้อง

1. แนวปฏิบัติในการจัดทำแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ (แผนฉุกเฉินด้าน IT) (12 ต.ค. 2548)
2. การจัดทำแผนฉุกเฉินและระบบคอมพิวเตอร์สำรอง (23 มิ.ย. 2531)

5. การป้องกันปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย (Anti-Money Laundering and Combating the Financing of Terrorism :AML/CFT)

การฟอกเงิน และการสนับสนุนทางการเงินแก่การก่อการร้าย ถือเป็นภัยร้ายแรงต่อระบบเศรษฐกิจ สังคม และความมั่นคงของชาติ สถาบันการเงินที่ตกเป็นเครื่องมือของการฟอกเงินหรือการสนับสนุนทางการเงินแก่การก่อการร้าย จะมีความเสี่ยงต่อฐานะการดำเนินงานและชื่อเสียง ซึ่งสามารถนำไปสู่ความเสียหายขั้นร้ายแรงได้ ธปท. ได้เล็งเห็นถึงความสำคัญของการมีมาตรการในการป้องกันปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย (Anti-Money Laundering and Combating the Financing of Terrorism :AML/CFT) ที่เป็นไปตามมาตรฐานสากล

แนวทางการกำกับดูแลของ ธปท.

เพื่อส่งเสริมให้สถาบันการเงินมีมาตรการในการป้องกันปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย (AML/CFT) ที่เป็นไปตามมาตรฐานสากล ธปท. ได้ออกหลักเกณฑ์และวิธีปฏิบัติในการรู้จักลูกค้า และการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (Know Your Customer / Customer Due Diligence : KYC/CDD) ซึ่งเป็นส่วนประกอบสำคัญของมาตรการ AML/CFT ให้สถาบันการเงินถือปฏิบัติโดยทั่วกัน โดยแนวปฏิบัติดังกล่าวครอบคลุมถึงธุรกิจทางการเงินทุกประเภทที่สถาบันการเงินให้บริการแก่ลูกค้า แนวปฏิบัติฯ นี้ประกอบด้วย 1) บทบาทและความรับผิดชอบของคณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงิน และ 2) การดำเนินมาตรการ AML/CFT ได้แก่ นโยบายในการรับลูกค้า (Customer Acceptance Policy) การแสดงตนของลูกค้าและการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (Customer Identification) การติดตามเฝ้าดูบัญชีลูกค้าอย่างต่อเนื่อง (On-going Monitoring of Accounts and Transactions) และการบริหารความเสี่ยง (Risk Management)

ประกาศและหนังสือเวียนที่เกี่ยวข้อง

1. มาตรการป้องกันปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย เรื่อง นโยบายการปฏิบัติตามหลักเกณฑ์การรู้จักลูกค้า/การตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าของสถาบันการเงิน และหน่วยธุรกิจหรือผู้ประกอบวิชาชีพที่ไม่ใช่สถาบันการเงิน (17 พ.ค. 2550)

2. มาตรการป้องกันปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย (Anti-Money Laundering and Combating the Financing of Terrorism: AML/CFT) ของสถาบันการเงิน (19 ม.ค. 2550)
3. การกำหนดให้ธนาคารพาณิชย์ปฏิบัติในเรื่องการรับฝากเงิน (24 ธ.ค. 2544)