ธนาคารแห่งประเทศไทย

31 มกราคม 2560

เรียน ผู้จัดการ

สถาบันการเงินทุกแห่ง

ที่ ฝนส.(01)ว. 01 /2560 เรื่อง นำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน

ธนาคารแห่งประเทศไทยขอนำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน ลงวันที่ 28 ธันวาคม 2559 ซึ่งได้ประกาศในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป เล่ม 134 ตอนพิเศษ 28 ง ลงวันที่ 25 มกราคม 2560 แล้ว และมีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

สาระสำคัญของการปรับปรุงประกาศ คือ

(1) กำหนดคำจำกัดความของ "การใช้บริการ Cloud Computing" และกำหนดหลักเกณฑ์การแจ้งหรือขออนุญาตการใช้บริการ Cloud Computing ตามลักษณะของการใช้บริการ

(2) เน้นย้ำและให้ความสำคัญกับการกำกับดูแลความเสี่ยงที่เกิดจากการใช้บริการ Cloud Computing เช่น การประเมินและการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นให้ครอบคลุมถึงการรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคล (data privacy) ความเสี่ยงอันเนื่องมาจากการพึ่งพิงการใช้บริการจากผู้ให้บริการภายนอกจนอาจทำให้การเปลี่ยนแปลงหรือยกเลิกการใช้บริการทำได้ยาก (vendor lock-in) และความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการในต่างประเทศ นอกจากนี้ สถาบันการเงินควรใช้บริการจากผู้ให้บริการ Cloud Computing ที่ได้รับการรับรองตามมาตรฐานสากลที่เกี่ยวข้อง

(3) อนุญาตให้สถาบันการเงินสามารถใช้ผลการตรวจสอบของผู้ให้บริการภายนอกที่ได้รับการรับรองจากผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากลในการตรวจสอบด้านเทคโนโลยีสารสนเทศ เพื่อลดข้อจำกัดของสถาบันการเงินที่ไม่สามารถเข้าตรวจสอบผู้ให้บริการภายนอกได้

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นางสาวเมทินี ศุภสวัสดิ์กุล)
ผู้อำนวยการอาวุโส ฝ่ายนโยบายการกำกับสถาบันการเงิน
ผู้ว่าการแทน

ฝนสว00-คส52001-2560031

คส520	วันที่ 31 ม.ค. 2560

สิ่งที่ส่งมาด้วย ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 19/2559 เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน ลงวันที่ 28 ธันวาคม 2559

ฝ่ายนโยบายการกำกับสถาบันการเงิน
โทรศัพท์ 0 2283 6938, 0 2283 5869

หมายเหตุ [ ] ธนาคารจะจัดให้มีการประชุมชี้แจงในวันที่ ..... ณ .....
[x] ไม่มีการประชุมชี้แจง

ธนาคารแห่งประเทศไทย

ประกาศธนาคารแห่งประเทศไทย
ที่ สนส. 19 /2559
เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing)
ในการประกอบธุรกิจของสถาบันการเงิน

---

1. เหตุผลในการออกประกาศ

ธนาคารแห่งประเทศไทยอนุญาตให้สถาบันการเงินสามารถใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ทั้งในประเทศและต่างประเทศได้ เพื่อส่งเสริมให้เกิดประสิทธิภาพในด้านการดำเนินงานและการบริหารต้นทุน และเพิ่มศักยภาพในการพัฒนาการให้บริการทางการเงินให้ทันต่อเทคโนโลยีที่มีการเปลี่ยนแปลงอย่างรวดเร็ว โดยสถาบันการเงินต้องรับผิดชอบต่อการให้บริการอย่างต่อเนื่องแก่ผู้ใช้บริการของสถาบันการเงิน ต้องคงความน่าเชื่อถือของการให้บริการเช่นเดียวกับกรณีที่สถาบันการเงินเป็นผู้ดำเนินการเอง และต้องคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นต่อสถาบันการเงินในรูปแบบที่เปลี่ยนแปลงไปจากการดำเนินงานปกติที่ดำเนินการโดยสถาบันการเงินเอง เช่น ความเสี่ยงด้านปฏิบัติการ (operational risk) จากการดำเนินงานของผู้ให้บริการภายนอก ความเสี่ยงด้านกลยุทธ์ (strategic risk) ในการวางแผนการดำเนินธุรกิจ ความเสี่ยงด้านชื่อเสียง (reputational risk) และความเสี่ยงด้านกฎหมาย (legal risk) โดยเฉพาะการรักษาความลับของข้อมูลของผู้ใช้บริการของสถาบันการเงิน รวมทั้ง สถาบันการเงินต้องมีการบริหารจัดการความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศอย่างเหมาะสม ภายใต้กรอบหลักการด้านเทคโนโลยีสารสนเทศที่สำคัญ 3 ประการ คือ การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (security) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (availability) นอกจากนี้ คณะกรรมการของสถาบันการเงินต้องมีการกำกับดูแลความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศอย่างเหมาะสม (board oversight) ทั้งนี้ ธนาคารแห่งประเทศไทยได้แบ่งการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศออกเป็น 2 ประเภท คือ การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน (Critical IT Outsourcing) และการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น (Other IT Outsourcing) รวมทั้ง กำหนดหลักเกณฑ์การกำกับดูแลให้สอดคล้องกับประเภทการใช้บริการดังกล่าว

เนื่องจากปัจจุบันสถาบันการเงินมีความต้องการใช้งานเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอกมากขึ้น โดยเฉพาะการใช้บริการ Cloud Computing ซึ่งมีความเกี่ยวข้องกับการจัดสรรทรัพยากรด้านงานเทคโนโลยีสารสนเทศ เพื่อการจัดเก็บข้อมูล การประมวลผล หรือการดำเนินการใด ๆ เกี่ยวกับข้อมูลของสถาบันการเงิน ซึ่งที่ผ่านมาธนาคารแห่งประเทศไทยกำหนดให้สถาบันการเงิน

ฝนสป00-คส52001-25591228

คส520	วันที่ 28 ธ.ค. 2559

ต้องหารือกับธนาคารแห่งประเทศไทยทุกกรณีก่อนเริ่มใช้บริการ Cloud Computing จึงอาจมีข้อจำกัดในทางปฏิบัติค่อนข้างมาก ดังนั้น เพื่อให้การกำกับดูแลสอดคล้องกับความเสี่ยงของการใช้บริการ Cloud Computing และเพื่อเพิ่มความยืดหยุ่นในการปฏิบัติตามหลักเกณฑ์ ธนาคารแห่งประเทศไทยจึงเห็นควรปรับปรุงหลักเกณฑ์การใช้บริการ Cloud Computing จากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ โดยเน้นการบริหารจัดการความเสี่ยงจากการใช้บริการ Cloud Computing และปรับปรุงหลักเกณฑ์การขออนุญาตการใช้บริการ Cloud Computing ให้เหมาะสมกับประเภทของ Cloud Computing ที่ธนาคารแห่งประเทศไทยกำหนดตามลักษณะของการใช้บริการ คือ Private Cloud และ Public Cloud ซึ่งสาระสำคัญของการปรับปรุงมีดังนี้

(1) การแจ้งหรือขออนุญาตการใช้บริการ Cloud Computing

กำหนดคำจำกัดความของ “การใช้บริการ Cloud Computing” และกำหนดหลักเกณฑ์การแจ้งหรือขออนุญาตการใช้บริการ Cloud Computing ตามลักษณะของการใช้บริการ โดยในกรณีที่สถาบันการเงินประสงค์จะใช้บริการ (1) Private Cloud จากบริษัทนอกกลุ่มธุรกิจเดียวกัน หรือ (2) Public Cloud ในงานประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน (Critical IT Outsourcing) ให้สถาบันการเงินแจ้งการใช้บริการตาม (1) หรือขออนุญาตการใช้บริการตาม (2) มายังธนาคารแห่งประเทศไทย ล่วงหน้าอย่างน้อย 30 วันก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

(2) การกำกับดูแลความเสี่ยงจากการใช้บริการ Cloud Computing

เน้นย้ำและให้ความสำคัญกับการกำกับดูแลความเสี่ยงที่เกิดจากการใช้บริการ Cloud Computing มากขึ้น เช่น การประเมินและการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นให้ครอบคลุมถึงการรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคล (data privacy) ความเสี่ยงอันเนื่องมาจากการพึ่งพิงการใช้บริการจากผู้ให้บริการภายนอกและเปลี่ยนแปลงการใช้บริการได้ยาก (vendor lock-in) ความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการในต่างประเทศ เช่น ความเสี่ยงจากการไม่สามารถเข้าถึงข้อมูลอันเนื่องมาจากการขัดข้องหรือการปิดกั้นเครือข่ายสื่อสารหรือระบบสื่อสารระหว่างประเทศ (information access risk) ความเสี่ยงด้านกฎหมายที่เกี่ยวข้องกับการปฏิบัติตามหลักเกณฑ์ของต่างประเทศ (cross-border compliance) นอกจากนี้ สถาบันการเงินควรใช้บริการจากผู้ให้บริการ Cloud Computing ที่ได้รับการรับรองตามมาตรฐานสากลที่เกี่ยวข้อง

(3) การตรวจสอบผู้ให้บริการภายนอก

กรณีที่สถาบันการเงินไม่สามารถจัดให้มีการตรวจสอบผู้ให้บริการภายนอกได้ สถาบันการเงินอาจใช้ผลการตรวจสอบของผู้ให้บริการภายนอกที่ได้รับการรับรองจากผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากลในการตรวจสอบด้านเทคโนโลยีสารสนเทศ และรับทราบโดยคณะกรรมการของสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมายแล้วได้ โดยธนาคารแห่งประเทศไทยอาจพิจารณาสั่งการให้สถาบันการเงินจัดหาผู้ตรวจสอบภายนอกเข้าตรวจสอบผู้ให้บริการภายนอกดังกล่าวตามขอบเขตที่กำหนด และรายงานผลการตรวจสอบดังกล่าวให้ธนาคารแห่งประเทศไทยทราบโดยตรงด้วยก็ได้

นอกจากนี้ ตามที่ธนาคารแห่งประเทศไทยได้กำหนดให้สถาบันการเงินต้องนำส่งรายงานการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศให้ธนาคารแห่งประเทศไทยเป็นประจำทุกปีนั้น บัดนี้ ธนาคารแห่งประเทศไทยได้กำหนดรูปแบบรายงาน เพื่อให้สถาบันการเงินมีความสะดวกในการจัดทำรายงานดังกล่าวมากขึ้น โดยให้นำส่งตามกำหนดเวลาเดิม

2. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา 47 และมาตรา 71 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 ธนาคารแห่งประเทศไทยจึงออกหลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงินตามความในประกาศนี้

3. ยกเลิก/แก้ไข

ให้ยกเลิกประกาศและหนังสือเวียนธนาคารแห่งประเทศไทย ดังนี้

(1) ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 6/2557 เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน ลงวันที่ 14 กรกฎาคม 2557

(2) หนังสือเวียนที่ ฝนส.(01) ว. 17/2557 เรื่อง การนำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน ลงวันที่ 4 สิงหาคม 2557

4. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ใช้บังคับกับสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

5. เนื้อหา

5.1 คำจำกัดความ

"การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ" (IT Outsourcing) หมายความว่า การใช้บริการจากผู้ให้บริการภายนอก (service provider) ในการดำเนินการด้านงานเทคโนโลยีสารสนเทศให้แก่สถาบันการเงิน ซึ่งโดยปกติแล้วสถาบันการเงินต้องดำเนินการเอง

"ผู้ให้บริการภายนอก" (service provider) หมายความว่า บุคคลภายนอกทั้งในและต่างประเทศ รวมถึงบริษัทในกลุ่มธุรกิจเดียวกัน ซึ่งเข้าทำสัญญาหรือทำข้อตกลงในการให้บริการงานให้กับสถาบันการเงิน อันมีลักษณะที่โดยปกติแล้วสถาบันการเงินต้องดำเนินการเอง

"บริษัทในกลุ่มธุรกิจเดียวกัน"

(1) กรณีธนาคารพาณิชย์ที่จดทะเบียนในประเทศ หมายความว่า บริษัทในกลุ่มธุรกิจทางการเงินตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับแบบรวมกลุ่ม

(2) กรณีธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ หมายความว่า บริษัทในกลุ่มธุรกิจทางการเงินตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับแบบรวมกลุ่ม รวมถึงบริษัทที่มีความเกี่ยวข้องกับธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศนั้น

(3) กรณีสาขาของธนาคารพาณิชย์ต่างประเทศ หมายความว่า สำนักงานใหญ่สาขาที่อยู่ในประเทศอื่น สำนักงานภูมิภาคในต่างประเทศของสาขาของธนาคารพาณิชย์ต่างประเทศ รวมถึงบริษัทที่มีความเกี่ยวข้องกับธนาคารพาณิชย์ต่างประเทศนั้น

"บริษัทที่มีความเกี่ยวข้อง" หมายความว่า บริษัทแม่ บริษัทลูก และบริษัทร่วม โดยให้ใช้คำจำกัดความตามความในมาตรา 4 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 โดยอนุโลม

"งานเทคโนโลยีสารสนเทศ" (information technology – IT) หมายความว่า งานด้านเทคโนโลยีสารสนเทศ ที่ครอบคลุมถึง ระบบงาน (application) ข้อมูล (information) โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (infrastructure) และบุคลากรและกระบวนการที่จัดการด้านเทคโนโลยีสารสนเทศ (people and process)

"การใช้บริการ Cloud Computing" หมายความว่า การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศในงานด้านโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศหรือระบบงานด้านเทคโนโลยีสารสนเทศที่มีการนำเทคโนโลยี Cloud Computing มาใช้ในการให้บริการผ่านเครือข่ายอินเตอร์เน็ต เพื่อประโยชน์ในการจัดเก็บข้อมูล การประมวลผล หรือการดำเนินการใด ๆ เกี่ยวกับข้อมูลหรือระบบงานให้แก่สถาบันการเงิน ซึ่งการใช้บริการดังกล่าวสามารถปรับเปลี่ยนได้ตามความต้องการของผู้ใช้บริการ

"คณะกรรมการของสถาบันการเงิน" หมายความว่า คณะกรรมการของสถาบันการเงินที่จดทะเบียนในประเทศไทย หรือคณะผู้บริหารที่มีอำนาจหน้าที่รับผิดชอบที่เกี่ยวข้องของสาขาของธนาคารพาณิชย์ต่างประเทศ

5.2 การอนุญาตให้สถาบันการเงินใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

ธนาคารแห่งประเทศไทยอนุญาตให้สถาบันการเงินใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงินได้ ภายใต้หลักเกณฑ์และเงื่อนไขตามที่กำหนดไว้ในประกาศนี้ อย่างไรก็ดี สถาบันการเงิน โดยเฉพาะสถาบันการเงินไทยต้องพิจารณาถึงความสอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจ และควรให้ความสำคัญต่อการลงทุนในระบบเทคโนโลยีสารสนเทศเพื่อส่งเสริมศักยภาพในการแข่งขัน (competitiveness) ด้วย

ทั้งนี้ หลักการสำคัญของการอนุญาตให้สถาบันการเงินใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ คือ

(1) สถาบันการเงินต้องรับผิดชอบต่อการให้บริการอย่างต่อเนื่องแก่ผู้ใช้บริการของสถาบันการเงิน ต้องคงความน่าเชื่อถือของการให้บริการเช่นเดียวกับกรณีที่สถาบันการเงินเป็น

ผู้ดำเนินการด้านเทคโนโลยีสารสนเทศด้วยตนเอง และต้องคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นต่อสถาบันการเงินในรูปแบบที่เปลี่ยนแปลงไปจากการดำเนินงานปกติที่กระทำโดยสถาบันการเงินเอง

ในกรณีที่ผู้ให้บริการภายนอกมีการให้ผู้ให้บริการภายนอกรายอื่นรับช่วงจัดการงานด้านเทคโนโลยีสารสนเทศที่ให้บริการแก่สถาบันการเงินต่อ (sub-contract) สถาบันการเงินต้องมั่นใจว่าผู้ให้บริการภายนอกจะรับผิดชอบต่อการให้บริการด้านงานเทคโนโลยีสารสนเทศแก่สถาบันการเงินเสมือนกับที่ผู้ให้บริการภายนอกเป็นผู้ให้บริการด้วยตนเอง

(2) สถาบันการเงินต้องมีแนวทางบริหารความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศที่สอดคล้องกับความเสี่ยงที่อาจเกิดขึ้น ภายใต้กรอบหลักการด้านเทคโนโลยีสารสนเทศที่สำคัญ 3 ประการ คือ การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (security) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (availability)

(3) สถาบันการเงินต้องมีการกำกับดูแลความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศอย่างเหมาะสม โดยต้องมีการประเมินตนเอง (self-assessment) ควบคุม และจัดการความเสี่ยงอย่างมีประสิทธิภาพ ภายใต้การกำกับดูแลของคณะกรรมการของสถาบันการเงิน (board oversight)

5.3 การแบ่งประเภทการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

สถาบันการเงินต้องพิจารณาประเภทการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ ดังนี้

5.3.1 การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน (Critical IT Outsourcing)

การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน หมายถึง การใช้บริการในงานเทคโนโลยีสารสนเทศที่อาจก่อให้เกิด

(1) ความเสี่ยงและผลกระทบต่อสถาบันการเงินในวงกว้าง (bank wide impact) เช่น การหยุดชะงักของการให้บริการแก่ผู้ใช้บริการของสถาบันการเงินและประชาชนทั่วไปในวงกว้าง หรือ

(2) ความเสี่ยงและผลกระทบต่อระบบสถาบันการเงิน หรือธุรกิจอื่นในวงกว้าง (banking system wide impact) เช่น การหยุดชะงักของระบบงานที่เชื่อมต่อกับระบบการชำระเงิน

ทั้งนี้ ตัวอย่างการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน เช่น การใช้บริการระบบประมวลผลกลาง (core banking) ศูนย์คอมพิวเตอร์ (data center) และระบบเครือข่ายสื่อสาร (network)

5.3.2 การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น (Other IT Outsourcing)

การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น หมายถึง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศที่ไม่เข้าข่ายเป็นการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน ตามข้อ 5.3.1

ทั้งนี้ หากสถาบันการเงินมีข้อสงสัยเกี่ยวกับการพิจารณาประเภทการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ ให้สถาบันการเงินหารือมาที่ **ฝ่ายตรวจสอบเทคโนโลยีสารสนเทศ สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน** ธนาคารแห่งประเทศไทยก่อนดำเนินการ

5.4 แนวทางการกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

ธนาคารแห่งประเทศไทยกำหนดแนวทางการกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ ตามประเภทของการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศตามข้อ 5.3 ดังนี้

5.4.1 สถาบันการเงินที่ใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน (Critical IT Outsourcing) ต้องปฏิบัติตามทั้งหลักเกณฑ์การควบคุมทั่วไป (general control) และหลักเกณฑ์การควบคุมเฉพาะสำหรับงานเทคโนโลยีสารสนเทศที่มีความสำคัญอย่างยิ่ง (specific control) โดยให้พิจารณาตามความเหมาะสมกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ

5.4.2 สถาบันการเงินที่ใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น (Other IT Outsourcing) ต้องปฏิบัติตามหลักเกณฑ์การควบคุมทั่วไป (general control) โดยให้พิจารณาตามความเหมาะสมกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ

5.5 หลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

สถาบันการเงินต้องปฏิบัติตามกฎหมาย ข้อบังคับของทางการ หรือมาตรฐานสากลที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศที่ใช้บริการ รวมถึงหลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ ดังนี้

5.5.1 หลักเกณฑ์การควบคุมทั่วไป (general control)

สถาบันการเงินที่มีการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศทั้งสองประเภทตามข้อ 5.3 ต้องให้ความสำคัญในเรื่องการกำหนดนโยบาย การบริหารความเสี่ยง การบริหารจัดการผู้ให้บริการภายนอก (service provider management) การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (security) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (integrity)

ความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (availability) และการคุ้มครองผู้ใช้บริการของสถาบันการเงิน (consumer protection) โดยให้พิจารณาตามความเหมาะสมกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ ดังนี้

(1) นโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

ในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ รวมถึงการใช้บริการ Cloud Computing สถาบันการเงินต้องกำหนดกลยุทธ์และนโยบายการใช้บริการดังกล่าว ดังนี้

(1.1) สถาบันการเงินต้องกำหนดกลยุทธ์ที่ชัดเจนสำหรับการตัดสินใจใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ เช่น เหตุผลความจำเป็นทางธุรกิจ รวมถึงประโยชน์และต้นทุน ทั้งนี้ สถาบันการเงินต้องมั่นใจว่า การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศนั้น ไม่ขัดต่อกฎหมายและข้อบังคับของทางการของประเทศไทยและประเทศของผู้ให้บริการภายนอกในกรณีที่ผู้ให้บริการภายนอกประกอบธุรกิจในต่างประเทศ ไม่ก่อให้เกิดช่องโหว่ที่นำไปสู่การเกิดการทุจริตที่ร้ายแรงหรือก่อให้เกิดภัยคุกคามด้านเทคโนโลยีสารสนเทศทั้งจากภายในและภายนอกจนอาจส่งผลกระทบต่อธุรกิจอย่างร้ายแรง และไม่ส่งผลกระทบต่อเสถียรภาพของระบบสถาบันการเงินและระบบการเงินของประเทศไทยอย่างร้ายแรง

(1.2) สถาบันการเงินต้องกำหนดนโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศอย่างชัดเจนและเป็นลายลักษณ์อักษร โดยต้องสอดคล้องกับนโยบายในการใช้บริการจากบุคคลภายนอก (outsourcing policy) และต้องคำนึงถึงความสอดคล้องกับกลยุทธ์ทางธุรกิจและความสามารถในการแข่งขัน ซึ่งนโยบายดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการของสถาบันการเงิน ทั้งนี้ นโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศควรครอบคลุมเรื่อง การแบ่งประเภทของการใช้บริการ การบริหารความเสี่ยงที่เกิดจากการใช้บริการ การบริหารจัดการผู้ให้บริการภายนอก การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล การรักษาความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล การรักษาความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ การคุ้มครองผู้ใช้บริการของสถาบันการเงิน การกำกับดูแลเพิ่มเติมกรณีการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน (Critical IT Outsourcing) และการรายงานและการตรวจสอบ เป็นต้น

(1.3) สถาบันการเงินต้องมีการทบทวนนโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับกลยุทธ์ของสถาบันการเงินที่อาจเปลี่ยนแปลงไป

(2) การบริหารความเสี่ยง

ในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ รวมถึงการใช้บริการ Cloud Computing สถาบันการเงินต้องมีแนวทางในการบริหารความเสี่ยงที่เกี่ยวข้องกับการใช้บริการดังกล่าว ดังนี้

(2.1) สถาบันการเงินต้องกำหนดนโยบายการบริหารความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศอย่างชัดเจนและเป็นลายลักษณ์อักษร โดยต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงโดยรวมของสถาบันการเงิน รวมถึง ขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ และ **นโยบายการบริหารความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศดังกล่าว**ต้องได้รับความเห็นชอบจากคณะกรรมการของสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมาย **นอกจากนี้ สถาบันการเงิน**ต้องมีการกำหนดแนวทาง วิธีการ และผู้รับผิดชอบในการบริหารความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศอย่างชัดเจนและเป็นลายลักษณ์อักษร ต้องประเมินผลการปฏิบัติตามแนวทางและวิธีการที่กำหนดอย่างสม่ำเสมอและต้องมีการรายงานผลการปฏิบัติดังกล่าวให้คณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสม

(2.2) สถาบันการเงินต้องมีความรู้ความเข้าใจในงานเทคโนโลยีสารสนเทศที่ใช้บริการจากผู้ให้บริการภายนอกตามสมควร ต้องสามารถประเมินระดับความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ และต้องจัดให้มีระบบการประเมิน ควบคุม และบริหารจัดการความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศให้ครอบคลุมความเสี่ยงที่สำคัญที่อาจเกิดขึ้น (เช่น ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านกฎหมาย และความเสี่ยงด้านเทคโนโลยีสารสนเทศ) โดยควรสอดคล้องกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ

ทั้งนี้ ในการประเมินความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ รวมถึงการใช้บริการ Cloud Computing ควรครอบคลุมถึงความเสี่ยงที่เกี่ยวข้องกับการรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคล (data privacy) การพึ่งพิงการใช้บริการจากผู้ให้บริการภายนอกจนอาจทำให้การเปลี่ยนแปลงหรือยกเลิกการใช้บริการทำได้ยาก (vendor lock-in) และผลกระทบต่อระบบงานที่สำคัญของสถาบันการเงิน นอกจากนี้ ในกรณีที่สถาบันการเงินมีการใช้บริการจากผู้ให้บริการภายนอกในต่างประเทศ โดยเฉพาะการจัดเก็บข้อมูล การประมวลผล หรือการดำเนินการใด ๆ เกี่ยวกับข้อมูล สถาบันการเงินต้องมีการประเมินความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการในต่างประเทศนั้น เช่น ความเสี่ยงจากการไม่สามารถเข้าถึงข้อมูลอันเนื่องมาจากการขัดข้องหรือการปิดกั้นเครือข่ายสื่อสารหรือระบบสื่อสารระหว่างประเทศ (information access risk) และความเสี่ยงด้านกฎหมายที่เกี่ยวข้องกับการปฏิบัติตามหลักเกณฑ์ของต่างประเทศ (cross-border compliance)

(2.3) สถาบันการเงินต้องจัดให้มีแนวทางในการติดตามประสิทธิภาพในการให้บริการของผู้ให้บริการภายนอกอย่างต่อเนื่อง แนวทางในการรับทราบการเปลี่ยนแปลงที่เกิดขึ้นกับผู้ให้บริการภายนอก รวมถึงแนวทางในการรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นจากการให้บริการของผู้ให้บริการภายนอก (day-to-day incident) อย่างสม่ำเสมอ ทั้งนี้ สถาบันการเงินต้องมีส่วนร่วมในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติ หากสถาบันการเงินประเมินว่า เหตุการณ์ผิดปกติที่เกิดขึ้นนั้นอาจกระทบต่อการดำเนินธุรกิจของสถาบันการเงินอย่างมีนัยสำคัญ นอกจากนี้ สถาบันการเงินต้องมีการทบทวนและประเมิน

ประสิทธิภาพในการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ และมีการรายงานผลการประเมินดังกล่าวให้คณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสม

(2.4) สถาบันการเงินต้องจัดให้มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity plan) ที่ครอบคลุมถึงการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ โดยควรสอดคล้องกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการและความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ รวมถึงผลกระทบของการใช้บริการที่มีต่อการดำเนินธุรกิจของสถาบันการเงิน และต้องจัดให้มีแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (disaster recovery plan) เพื่อรองรับกรณีการเกิดปัญหาหรือเหตุการณ์ผิดปกติจากการใช้บริการจากผู้ให้บริการภายนอกและเพื่อลดผลกระทบที่อาจเกิดขึ้น โดยสถาบันการเงินต้องมั่นใจว่า สถาบันการเงินมีข้อมูลพร้อมใช้ภายในประเทศสำหรับการดำเนินธุรกิจและการให้บริการแก่ลูกค้าอย่างต่อเนื่อง รวมทั้ง ต้องมีการทบทวนและทดสอบการปฏิบัติตามแผนรองรับการดำเนินธุรกิจและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอเพื่อให้สามารถปฏิบัติงานได้จริง รวมทั้ง ต้องจัดให้มีกระบวนการในการบริหารจัดการปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการใช้บริการ และมีการรายงานปัญหาหรือเหตุการณ์ผิดปกติและการจัดการปัญหาหรือเหตุการณ์ผิดปกติดังกล่าว ให้คณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสม

(3) การบริหารจัดการผู้ให้บริการภายนอก (service provider management)

ในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ รวมถึงการใช้บริการ Cloud Computing สถาบันการเงินต้องมีการบริหารจัดการผู้ให้บริการภายนอก ดังนี้

(3.1) สถาบันการเงินต้องกำหนดกระบวนการและหลักเกณฑ์ในการคัดเลือกผู้ให้บริการภายนอกที่ชัดเจน และมีการตรวจสอบความพร้อมและพิจารณาความเหมาะสมของผู้ให้บริการภายนอกเพื่อให้มั่นใจว่า ผู้ให้บริการภายนอกจะสามารถให้บริการได้อย่างต่อเนื่อง และสามารถตอบสนองความต้องการของสถาบันการเงินได้ โดยควรคำนึงถึงปัจจัยที่สำคัญ เช่น ความรู้ในเทคโนโลยีสารสนเทศ ประสบการณ์ ระบบการบริหารงานภายใน ศักยภาพและความสามารถในการให้บริการทั้งในภาวะปกติและไม่ปกติ โดยเฉพาะอย่างยิ่งกรณีที่ผู้ให้บริการภายนอกนั้นมีการให้บริการแก่ผู้ใช้บริการหลายราย (concentration risk)

ทั้งนี้ ในการพิจารณาคัดเลือกผู้ให้บริการ Cloud Computing สถาบันการเงินควรคำนึงถึงความพร้อมและมาตรฐานในการให้บริการของผู้ให้บริการดังกล่าว โดยผู้ให้บริการ Cloud Computing ควรได้รับการรับรองมาตรฐานสากลที่เกี่ยวข้อง เช่น มาตรฐานสากลในเรื่องการรักษาความปลอดภัยของระบบงานและข้อมูล

(3.2) สถาบันการเงินต้องมีการจัดทำสัญญาการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร หรือมีการจัดทำข้อตกลงการให้บริการ (service level agreement) เป็นลายลักษณ์อักษรกรณีที่ผู้ให้บริการภายนอกเป็นบริษัทในกลุ่มธุรกิจเดียวกัน และต้องระบุบทบาท หน้าที่ ความรับผิดชอบ เงื่อนไขการให้บริการของผู้ให้บริการภายนอก และความรับผิดต่อความเสียหายอย่างใด ๆ ในกรณีที่ผู้ให้บริการภายนอกไม่ปฏิบัติตามเงื่อนไขในการให้บริการ ไว้ในสัญญาหรือ

ข้อตกลงการให้บริการให้ชัดเจน ส่วนเนื้อหาของสัญญาและข้อตกลงการให้บริการควรครอบคลุมประเด็นสำคัญ เช่น

- ขอบเขตงานเทคโนโลยีสารสนเทศที่ใช้บริการและเงื่อนไขในการให้บริการของผู้ให้บริการภายนอก
- มาตรฐานของการปฏิบัติงานขั้นต่ำที่ต้องการจากผู้ให้บริการภายนอก (เช่น มาตรฐานด้านการรักษาความปลอดภัยและความลับของข้อมูล **การห้ามนำข้อมูลไปใช้นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงการให้บริการ** ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ)
- ระบบการควบคุมภายในของผู้ให้บริการภายนอก
- การจัดทำแผนฉุกเฉินสำหรับการให้บริการของผู้ให้บริการภายนอกที่ควรสอดคล้องกับแผนฉุกเฉินของสถาบันการเงิน
- การรายงานผลการปฏิบัติงานของผู้ให้บริการภายนอกซึ่งครอบคลุมถึงการรายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการให้บริการ
- ความรับผิดชอบของสถาบันการเงินและผู้ให้บริการภายนอกภาระผูกพันในกรณีที่เกิดปัญหาในการให้บริการ เงื่อนไขหรือแนวทางในการเปลี่ยนแปลงหรือยกเลิกสัญญา **เช่น การทำลายข้อมูลของผู้ใช้บริการของสถาบันการเงินและข้อมูลของสถาบันการเงินทั้งหมด เมื่อสิ้นสุดหรือยกเลิกการใช้บริการจากผู้ให้บริการภายนอก**
- สิทธิของสถาบันการเงิน ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก และธนาคารแห่งประเทศไทย ในการเรียกดูข้อมูลที่เกี่ยวข้องและเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของผู้ให้บริการภายนอกทั้งในกรณีที่ผู้ให้บริการภายนอกประกอบธุรกิจในประเทศและต่างประเทศ

นอกจากนี้ สถาบันการเงินต้องมีการเก็บสัญญาหรือข้อตกลงการให้บริการไว้ที่สถาบันการเงินเพื่อให้พร้อมสำหรับการตรวจสอบของธนาคารแห่งประเทศไทย และเมื่อธนาคารแห่งประเทศไทยร้องขอ

ทั้งนี้ ในกรณีที่ผู้ให้บริการภายนอกประกอบธุรกิจในต่างประเทศและหน่วยงานกำกับดูแลในประเทศนั้นมีข้อจำกัดเกี่ยวกับการเข้าตรวจสอบการดำเนินงานของผู้ให้บริการภายนอกดังกล่าว หรือมีข้อกฎหมาย หรือหลักเกณฑ์การกำกับดูแลที่แตกต่างจากที่ธนาคารแห่งประเทศไทยกำหนด ซึ่งทำให้สถาบันการเงินต้องปฏิบัติตามกฎหมาย ข้อกำหนด หรือหลักเกณฑ์การกำกับดูแลของหน่วยงานกำกับดูแลในประเทศนั้นด้วย ธนาคารแห่งประเทศไทยขอสงวนสิทธิในการพิจารณากำหนดหลักเกณฑ์การกำกับดูแล และ/หรือ เงื่อนไขอื่น เป็นรายกรณีตามความเหมาะสม

(4) การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (security)

ในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศรวมถึงการใช้บริการ Cloud Computing สถาบันการเงินต้องมีการรักษาความปลอดภัยและความลับของระบบงานและข้อมูล ดังนี้

(4.1) สถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกมีแนวทางหรือมาตรฐานในการรักษาความปลอดภัยและความลับของระบบงานและข้อมูล ทั้งข้อมูลของผู้ใช้บริการของสถาบันการเงินและข้อมูลของสถาบันการเงิน โดยควรมีความสอดคล้องกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ให้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการให้บริการ ทั้งนี้ สถาบันการเงินอาจกำหนดให้ผู้ให้บริการภายนอกมีการประยุกต์ใช้แนวทางการควบคุมด้านงานเทคโนโลยีสารสนเทศที่ดี เป็นมาตรฐานสากล และได้รับการยอมรับโดยทั่วไป ตามความเหมาะสม

ทั้งนี้ ในกรณีที่มีการใช้บริการ Cloud Computing สถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการ Cloud Computing มีแนวทางการรักษาความปลอดภัยข้อมูลสำคัญของผู้ใช้บริการของสถาบันการเงินและข้อมูลของสถาบันการเงินตามวิธีการและมาตรฐานสากล เช่น การเข้ารหัสข้อมูล (data encryption) การควบคุมกุญแจที่ใช้เข้าถึงและเข้ารหัสข้อมูลบนระบบ Cloud Computing (key management) เป็นต้น

(4.2) สถาบันการเงินต้องจัดให้มีกระบวนการ ขั้นตอน หรือ ระบบในการติดตาม ประเมินผล และตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่า ผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานด้านการรักษาความปลอดภัยและความลับของระบบงานและข้อมูลที่ได้ตกลงไว้กับสถาบันการเงิน

(4.3) สถาบันการเงินต้องจัดให้มีกระบวนการ ขั้นตอน หรือ ระบบในการดำเนินการนำข้อมูลของผู้ใช้บริการของสถาบันการเงินและข้อมูลของสถาบันการเงินทั้งหมดกลับมาจากผู้ให้บริการภายนอก และสถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกมีกระบวนการ ขั้นตอน หรือ ระบบในการดำเนินการทำลายข้อมูลของผู้ใช้บริการของสถาบันการเงินและข้อมูลของสถาบันการเงินทั้งหมด เมื่อมีการสิ้นสุดหรือยกเลิกการใช้บริการจากผู้ให้บริการภายนอก

(4.4) สถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกมีแนวทางหรือมาตรฐานในการดูแลและป้องกันข้อมูลสำคัญของผู้ใช้บริการของสถาบันการเงิน**และข้อมูลของสถาบันการเงิน** โดยควรสอดคล้องกับกฎหมาย ข้อบังคับที่เกี่ยวข้องของทางการ และมาตรฐานสากลที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศนั้น

(5) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (integrity)

ในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ รวมถึงการใช้บริการ Cloud Computing สถาบันการเงินต้องมีการดำเนินการเพื่อให้มั่นใจว่าระบบงานและข้อมูลมีความถูกต้องเชื่อถือได้ ดังนี้

(5.1) สถาบันการเงินต้อง**มีการดำเนินการเพื่อให้**มั่นใจว่า ผู้ให้บริการภายนอกมีแนวทางหรือมาตรฐานในการรักษาความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล **ซึ่งครอบคลุมตั้งแต่การพัฒนาหรือการเปลี่ยนแปลงแก้ไขระบบงาน การควบคุมทั้งในส่วนของการบันทึกข้อมูลเข้าสู่ระบบ (input validation) การประมวลผล (processing control) และการนำข้อมูลออกจากระบบ (output control)** รวมทั้ง มีการดำเนินการให้งานเทคโนโลยีสารสนเทศที่ให้บริการสามารถทำงานได้อย่างมีประสิทธิภาพและถูกต้องเชื่อถือได้ โดยควรมีความสอดคล้องกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ให้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการให้บริการ

ทั้งนี้ สถาบันการเงินอาจกำหนดให้ผู้ให้บริการภายนอกมีการประยุกต์ใช้แนวทางและการควบคุมด้านงานเทคโนโลยีสารสนเทศที่ดี เป็นมาตรฐานสากล และได้รับการยอมรับโดยทั่วไป ตามความเหมาะสม

(5.2) สถาบันการเงินต้องจัดให้มีกระบวนการ ขั้นตอน หรือ ระบบในการติดตาม ประเมินผล และตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่า ผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานด้านความถูกต้องเชื่อถือได้ของระบบงานและข้อมูลที่ได้ตกลงไว้กับสถาบันการเงิน

(6) ความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (availability)

ในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ รวมถึงการใช้บริการ Cloud Computing สถาบันการเงินต้องมีการดำเนินการเพื่อให้มั่นใจถึงความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ ดังนี้

(6.1) สถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกมีแนวทางหรือมาตรฐานในการทำให้งานเทคโนโลยีสารสนเทศที่ให้บริการแก่สถาบันการเงินพร้อมในการใช้งานอย่างต่อเนื่องทั้งในภาวะปกติและไม่ปกติ โดยควรมีความสอดคล้องกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ให้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการให้บริการ ทั้งนี้ สถาบันการเงินอาจกำหนดให้ผู้ให้บริการภายนอกมีการประยุกต์ใช้แนวทางการควบคุมด้านงานเทคโนโลยีสารสนเทศที่ดี เป็นมาตรฐานสากล และได้รับการยอมรับโดยทั่วไป ตามความเหมาะสม

(6.2) สถาบันการเงินต้องจัดให้มีกระบวนการ ขั้นตอน หรือ ระบบในการติดตาม ประเมินผล และตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่า ผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานด้านความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ให้บริการที่ได้ตกลงไว้กับสถาบันการเงิน

(7) การคุ้มครองผู้ใช้บริการของสถาบันการเงิน (consumer protection)

ในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ รวมถึงการใช้บริการ Cloud Computing สถาบันการเงินต้องมีการดำเนินการเกี่ยวกับการคุ้มครองผู้ใช้บริการของสถาบันการเงิน ดังนี้

(7.1) สถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกจะไม่นำข้อมูลของผู้ใช้บริการของสถาบันการเงินหรือข้อมูลของสถาบันการเงินไปเปิดเผยให้กับบุคคลอื่นใด โดยไม่ได้รับความยินยอมจากสถาบันการเงิน

(7.2) สถาบันการเงินต้องจัดให้มีกระบวนการ ขั้นตอน หรือ ระบบในการติดตาม ประเมินผล และตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่า ผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานด้านการคุ้มครองผู้ใช้บริการของสถาบันการเงินที่ได้ตกลงไว้กับสถาบันการเงิน

(7.3) สถาบันการเงินต้องจัดให้มีระบบการดูแลและจัดการเรื่องร้องเรียนให้แก่ผู้ใช้บริการของสถาบันการเงินอย่างเพียงพอและเหมาะสม และมีการรายงานการจัดการเรื่องร้องเรียนดังกล่าวให้คณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบ

ในระยะเวลาที่เหมาะสม **ทั้งนี้ ในกรณีที่ผู้ใช้บริการของสถาบันการเงินได้รับความเสียหายจากการใช้บริการจากผู้ให้บริการภายนอก สถาบันการเงินต้องมีแนวทางในการชดเชยความเสียหายให้แก่ผู้ใช้บริการของสถาบันการเงินอย่างเหมาะสม**

5.5.2 หลักเกณฑ์การควบคุมเฉพาะสำหรับงานเทคโนโลยีสารสนเทศที่มีความสำคัญอย่างยิ่ง (specific control)

สถาบันการเงินที่มีการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน เช่น การใช้บริการระบบประมวลผลกลาง (core banking) ศูนย์คอมพิวเตอร์ (data center) และระบบเครือข่ายสื่อสาร (network) **รวมถึงมีการใช้บริการ Cloud Computing ในงานที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน** นอกจากจะต้องปฏิบัติตามหลักเกณฑ์การควบคุมทั่วไปตามข้อ 5.5.1 แล้ว สถาบันการเงินยังต้องจัดให้มีการกำกับดูแลเพิ่มเติมที่สอดคล้องกับแนวทางการควบคุมด้านงานเทคโนโลยีสารสนเทศที่ดี เป็นมาตรฐานสากล และได้รับการยอมรับโดยทั่วไป โดยให้พิจารณาตามความเหมาะสมกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ รวมทั้ง ต้องมีระบบการกำกับดูแลที่เหมาะสมภายใต้การกำกับดูแลของคณะกรรมการของสถาบันการเงิน (board oversight) ดังนี้

(1) การกำกับดูแลเพิ่มเติม (specific risk control)

(1.1) สถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกมีกระบวนการ ขั้นตอน การประเมิน และการควบคุมความเสี่ยง อย่างน้อยตามกรอบหลักการด้านเทคโนโลยีสารสนเทศที่สำคัญ 3 ประการ คือ การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (security) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (availability) ที่เหมาะสมกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ให้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการให้บริการ โดยผู้ให้บริการภายนอกควรได้รับการรับรองตามมาตรฐานสากลที่เกี่ยวข้อง เช่น มาตรฐานของ International Organization for Standardization (ISO) และ Telecommunications Industry Association (TIA) เป็นต้น

(1.2) สถาบันการเงินต้องจัดให้มีกระบวนการ ขั้นตอน หรือ ระบบในการติดตาม ประเมินผล และตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่า ผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานสากลที่เกี่ยวข้องที่ได้ตกลงไว้กับสถาบันการเงิน และต้องจัดให้มีการทดสอบเพื่อให้มั่นใจว่า การใช้บริการจากบุคคลภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน จะไม่ก่อให้เกิดความเสี่ยงตามกรอบหลักการด้านเทคโนโลยีสารสนเทศที่สำคัญ 3 ประการ คือ การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (security) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (availability) จนนำมาสู่ช่องโหว่ที่ร้ายแรงต่อการทุจริต และ/หรือภัยคุกคามด้านเทคโนโลยีสารสนเทศทั้งจากภายในและภายนอก ซึ่งอาจส่งผลกระทบต่อธุรกิจอย่างร้ายแรง หรือก่อให้เกิดผลกระทบในวงกว้างต่อการให้บริการทางการเงินที่สำคัญของสถาบันการเงิน เช่น ต้องจัดให้มีการทดสอบแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ และมีการทดสอบระบบการรักษาความปลอดภัยเชิงลึก (penetration test) สำหรับการใช้บริการระบบ internet banking

(1.3) กรณีการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ ซึ่งรวมถึงการใช้บริการ Cloud Computing ในงานประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน สถาบันการเงินต้องกำหนดให้ผู้ให้บริการภายนอกระบุสถานที่ในการจัดเก็บข้อมูล ประมวลผลข้อมูล หรือดำเนินการใด ๆ เกี่ยวกับข้อมูลของสถาบันการเงิน (data location) เพื่อให้สถาบันการเงินสามารถบริหารความเสี่ยงของข้อมูลที่อาจเกิดขึ้นจากการใช้บริการได้อย่างเหมาะสม รวมทั้งสถาบันการเงินต้องจัดให้มีแผนฉุกเฉินรองรับกรณีที่สถาบันการเงินไม่สามารถใช้บริการ Cloud Computing และมีการทดสอบแผนฉุกเฉินก่อนใช้บริการเพื่อให้มั่นใจว่า สถาบันการเงินสามารถให้บริการทางการเงินได้อย่างต่อเนื่องตามนโยบายและแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity plan)

(2) ระบบการกำกับดูแลที่เหมาะสม (oversight)

(2.1) สถาบันการเงินต้องนำเสนอรายละเอียดของการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน พร้อมผลการประเมินความเสี่ยงโดยละเอียดให้กับคณะกรรมการของสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมาย เพื่อพิจารณาให้ความเห็นชอบในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงินทั้งก่อนเริ่มใช้บริการ เมื่อมีการเปลี่ยนแปลงการใช้บริการอย่างมีนัยสำคัญตามที่สถาบันการเงินกำหนด หรือมีการต่ออายุสัญญา

(2.2) สถาบันการเงินต้องมีการรายงานให้คณะกรรมการของสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสมเกี่ยวกับ ผลการประเมินประสิทธิภาพ การติดตาม และการตรวจสอบการดำเนินการของผู้ให้บริการภายนอก โดยอาจพิจารณาตามกรอบหลักการด้านเทคโนโลยีสารสนเทศที่สำคัญ 3 ประการ คือ การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (security) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (availability) รวมถึงปัญหาหรือเหตุการณ์ผิดปกติและเรื่องร้องเรียนที่เกิดขึ้นจากการใช้บริการ

5.6 แนวปฏิบัติสำหรับการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

ธนาคารแห่งประเทศไทยกำหนดแนวปฏิบัติสำหรับการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ ตามประเภท**และลักษณะ**ของการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ **(เอกสารแนบ 1)** ดังนี้

5.6.1 การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน (Critical IT Outsourcing)

(1) กรณีการใช้บริการในลักษณะที่ไม่ใช่ Cloud Computing

(1.1) ในกรณีที่เป็นการใช้บริการจากผู้ให้บริการภายนอกที่เป็นบริษัทในกลุ่มธุรกิจเดียวกัน ให้สถาบันการเงินสามารถดำเนินการได้โดยไม่ต้องแจ้ง**หรือขออนุญาต**มายังธนาคารแห่งประเทศไทยก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

(1.2) ในกรณีที่เป็นการใช้บริการจากผู้ให้บริการภายนอกที่ไม่เป็นบริษัทในกลุ่มธุรกิจเดียวกัน ให้สถาบันการเงินแจ้งให้ธนาคารแห่งประเทศไทยทราบล่วงหน้าอย่างน้อย 30 วันก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

(2) กรณีการใช้บริการในลักษณะที่เป็น Cloud Computing

(2.1) การใช้บริการ Cloud Computing ในลักษณะที่มีผู้ใช้บริการเพียงรายเดียว หรือมีผู้ใช้บริการจำกัดเฉพาะบริษัทในกลุ่มธุรกิจเดียวกัน (Private Cloud)

(2.1.1) ในกรณีที่เป็นการใช้บริการ Private Cloud จากผู้ให้บริการภายนอกที่เป็นบริษัทในกลุ่มธุรกิจเดียวกัน ให้สถาบันการเงินสามารถดำเนินการได้โดยไม่ต้องแจ้งหรือขออนุญาตมายังธนาคารแห่งประเทศไทยก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

(2.1.2) ในกรณีที่เป็นการใช้บริการ Private Cloud จากผู้ให้บริการภายนอกที่ไม่เป็นบริษัทในกลุ่มธุรกิจเดียวกัน ให้สถาบันการเงินแจ้งให้ธนาคารแห่งประเทศไทยทราบล่วงหน้าอย่างน้อย 30 วันก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

(2.2) การใช้บริการ Cloud Computing ในลักษณะที่มีผู้ใช้บริการร่วมกันหลายราย (Public Cloud) ซึ่งรวมถึงการใช้บริการในลักษณะจำกัดกลุ่มสมาชิกที่มีผู้ใช้บริการที่ไม่เป็นบริษัทในกลุ่มธุรกิจเดียวกันร่วมด้วย หรือการใช้บริการที่ผสมระหว่าง Private Cloud และ Public Cloud ไม่ว่าจากผู้ให้บริการภายนอกที่เป็นบริษัทในกลุ่มธุรกิจเดียวกันหรือผู้ให้บริการภายนอกที่ไม่เป็นบริษัทในกลุ่มธุรกิจเดียวกัน ให้สถาบันการเงินขออนุญาตมายังธนาคารแห่งประเทศไทยล่วงหน้าอย่างน้อย 30 วันก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

ทั้งนี้ หากสถาบันการเงินมีข้อสงสัยเกี่ยวกับการพิจารณาลักษณะการใช้บริการ Cloud Computing ให้สถาบันการเงินหารือมาที่ ฝ่ายตรวจสอบเทคโนโลยีสารสนเทศ สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน ธนาคารแห่งประเทศไทย ก่อนดำเนินการ

ในการแจ้งหรือการขออนุญาตตามข้อ 5.6.1 ให้สถาบันการเงินส่งหนังสือแจ้งหรือขออนุญาตมายัง ฝ่ายกำกับธุรกิจสถาบันการเงิน สายนโยบายสถาบันการเงิน ธนาคารแห่งประเทศไทย โดยให้ระบุถึงเหตุผล รายละเอียดการใช้บริการ และผลการประเมินความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศดังกล่าว ที่ได้รับความเห็นชอบจากคณะกรรมการของสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมายแล้ว **ทั้งนี้ ในกรณีการขออนุญาต ธนาคารแห่งประเทศไทยจะพิจารณาให้แล้วเสร็จภายใน 30 วันนับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน**

5.6.2 การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น (Other IT Outsourcing)

ในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น (Other IT Outsourcing) **ไม่ว่าจะเป็นกรณีการใช้บริการในลักษณะที่ไม่ใช่ Cloud Computing หรือกรณีการใช้บริการในลักษณะที่เป็น Cloud Computing** ให้สถาบันการเงินสามารถดำเนินการได้โดยไม่ต้องแจ้ง**หรือขออนุญาตมายัง**ธนาคารแห่งประเทศไทยก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

5.7 การรายงานและการตรวจสอบ

การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศของสถาบันการเงิน **ซึ่งรวมถึงการใช้บริการ Cloud Computing** อาจก่อให้เกิดผลกระทบต่อทั้งผู้ใช้บริการของสถาบันการเงิน สถาบันการเงิน ระบบการเงิน และธุรกิจอื่น ดังนั้น สถาบันการเงินต้องมีการกำกับดูแลผู้ให้บริการภายนอกอย่างใกล้ชิดและต้องดำเนินการให้ธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายนอก หรือหน่วยงานกำกับดูแลอื่นได้รับทราบข้อมูลที่เกี่ยวข้องกับการใช้บริการและสามารถตรวจสอบผู้ให้บริการภายนอกดังกล่าวได้ ดังนี้

5.7.1 การรายงานต่อธนาคารแห่งประเทศไทย

(1) สถาบันการเงินต้องจัดทำรายงานการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศทุกประเภท**ตามแบบรายงานที่กำหนดในเอกสารแนบ 2** ให้มีความถูกต้องและเป็นปัจจุบัน และส่งมายัง **ฝ่ายกำกับธุรกิจสถาบันการเงิน สายนโยบายสถาบันการเงิน** ธนาคารแห่งประเทศไทย เป็นประจำทุกปี ภายใน 30 วันนับจากวันที่ 31 ธันวาคม และเมื่อธนาคารแห่งประเทศไทยร้องขอ

(2) ในกรณีที่เกิดปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการใช้บริการจากผู้ให้บริการภายนอกอันเป็นเหตุให้สถาบันการเงินไม่สามารถให้บริการการเงินพื้นฐานแก่ผู้ใช้บริการของสถาบันการเงินได้ในวงกว้าง **ให้สถาบันการเงินปฏิบัติตามประกาศธนาคารแห่งประเทศไทยว่าด้วยเหตุการณ์ที่มีนัยสำคัญที่ต้องรายงานต่อธนาคารแห่งประเทศไทย**

5.7.2 การตรวจสอบผู้ให้บริการภายนอกของสถาบันการเงิน

(1) สถาบันการเงินต้องจัดให้มีการตรวจสอบผู้ให้บริการภายนอก โดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก **โดยอาจกำหนดความถี่ในการตรวจสอบผู้ให้บริการภายนอกตามความเหมาะสม ซึ่งอาจพิจารณาจากความสำคัญของงานเทคโนโลยีสารสนเทศที่ใช้บริการ** และจัดทำรายงานผลการตรวจสอบผู้ให้บริการภายนอกดังกล่าวและเก็บไว้ที่สถาบันการเงิน พร้อมไว้สำหรับการตรวจสอบและเมื่อร้องขอโดยธนาคารแห่งประเทศไทย

ในกรณีที่สถาบันการเงินไม่สามารถจัดให้มีการตรวจสอบผู้ให้บริการภายนอกได้ เช่น กรณีที่ผู้ให้บริการภายนอกอยู่ในต่างประเทศและมีศูนย์ข้อมูลหลายแห่งที่เกี่ยวข้องกับการใช้บริการของสถาบันการเงิน สถาบันการเงินอาจใช้ผลการตรวจสอบของผู้ให้บริการภายนอกที่ได้รับการรับรองจากผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากลในการตรวจสอบด้านเทคโนโลยีสารสนเทศ และรับทราบโดยคณะกรรมการของสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมายแล้วได้ ทั้งนี้ ธนาคารแห่งประเทศไทยอาจพิจารณาสั่งการให้สถาบันการเงินจัดหาผู้ตรวจสอบภายนอกเข้าตรวจสอบผู้ให้บริการภายนอกดังกล่าวตามขอบเขตที่กำหนด และรายงานผลการตรวจสอบดังกล่าวให้ธนาคารแห่งประเทศไทยทราบโดยตรงด้วยก็ได้

(2) ในกรณีที่สถาบันการเงินใช้บริการจากผู้ให้บริการภายนอกที่เป็นบริษัทในกลุ่มธุรกิจเดียวกันที่อยู่ในต่างประเทศ สถาบันการเงินสามารถใช้ผลการตรวจสอบของบริษัทแม่ที่ได้รับการรับรองจากผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกที่มีความเป็นอิสระ และรับทราบโดยคณะกรรมการของสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมายแล้วได้

5.7.3 การตรวจสอบโดยธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายนอก หรือหน่วยงานกำกับดูแลอื่น

สถาบันการเงินต้องดำเนินการให้ธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายนอก หรือหน่วยงานกำกับดูแลอื่น สามารถเข้าตรวจสอบและเรียกดูข้อมูลจากผู้ให้บริการภายนอก **ซึ่งรวมถึงเข้าตรวจสอบและเรียกดูข้อมูลจากผู้ให้บริการภายนอกที่รับช่วงต่อ (sub-contract) ด้วย**

5.8 อำนาจในการพิจารณา สั่งการ เพิกถอน หรือผ่อนผัน

5.8.1 ธนาคารแห่งประเทศไทยอาจพิจารณากำหนดหลักเกณฑ์อื่นเพิ่มเติมได้ตามความเสี่ยงสำคัญที่อาจเกิดขึ้น โดยจะพิจารณาความเหมาะสมร่วมกับสถาบันการเงินเป็นรายกรณี

5.8.2 ธนาคารแห่งประเทศไทยอาจพิจารณาสั่งการ และ/หรือ กำหนดเงื่อนไขให้สถาบันการเงินถือปฏิบัติตามความเหมาะสมเป็นรายกรณี หรือสั่งเพิกถอนการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ ทั้งก่อนและหลังจากที่สถาบันการเงินใช้บริการจากผู้ให้บริการภายนอก หากพบว่า การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศดังกล่าวไม่สอดคล้องกับหลักเกณฑ์หรือเงื่อนไขที่ธนาคารแห่งประเทศไทยกำหนด

5.8.3 ธนาคารแห่งประเทศไทยอาจพิจารณาผ่อนผันเป็นรายกรณี ในกรณีที่สถาบันการเงินไม่สามารถปฏิบัติตามหลักเกณฑ์หรือเงื่อนไขที่กำหนด โดยให้สถาบันการเงินแสดงเหตุผลและความจำเป็นมาที่ **ฝ่ายกำกับธุรกิจสถาบันการเงิน สายนโยบายสถาบันการเงิน** ธนาคารแห่งประเทศไทย

5.9 บทเฉพาะกาล

5.9.1 สถาบันการเงินที่ได้แจ้งการใช้บริการจากผู้ให้บริการภายนอกที่ไม่เป็นบริษัทในกลุ่มธุรกิจเดียวกันด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงินมายังธนาคารแห่งประเทศไทยแล้วก่อนประกาศฉบับนี้มีผลใช้บังคับ ให้ดำเนินการต่อไปได้โดยไม่ต้องแจ้ง**การใช้บริการดังกล่าวมายัง**ธนาคารแห่งประเทศไทยอีก จนกว่าจะมีการเปลี่ยนแปลงการใช้บริการหรือต่ออายุหรือจัดทำสัญญาหรือข้อตกลงการใช้บริการใหม่

5.9.2 สถาบันการเงินต้องถือปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้และเงื่อนไขที่ธนาคารแห่งประเทศไทยกำหนดเพิ่มเติมในกรณีที่สถาบันการเงินได้แจ้งการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศมายังธนาคารแห่งประเทศไทยแล้ว เท่าที่ไม่ขัดกับหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ ทั้งนี้

(1) สำหรับสัญญาหรือข้อตกลงการให้บริการเดิมที่ยังมีผลบังคับใช้อยู่ในวันที่ประกาศฉบับนี้มีผลบังคับใช้ ให้สถาบันการเงินดำเนินการปรับปรุงให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ภายในเวลา 1 ปี นับจากวันที่ประกาศฉบับนี้มีผลบังคับใช้

(2) สำหรับกรณีที่มีการต่ออายุสัญญาหรือข้อตกลงการใช้บริการ ซึ่งรวมถึงกรณีการต่ออายุอัตโนมัติ หรือมีการเปลี่ยนแปลงหรือแก้ไขสัญญาหรือข้อตกลงการใช้บริการ หรือมีการทำสัญญาหรือข้อตกลงการใช้บริการใหม่ ให้สถาบันการเงินปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้นับจากวันที่ประกาศฉบับนี้มีผลบังคับใช้

หากสถาบันการเงินใดไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้หรือเงื่อนไขที่ธนาคารแห่งประเทศไทยกำหนดเพิ่มเติมได้ภายในระยะเวลาที่กำหนด ให้สถาบันการเงินหารือ พร้อมทั้งแสดงเหตุผลและความจำเป็นมาที่ **ฝ่ายกำกับธุรกิจสถาบันการเงิน สายนโยบายสถาบันการเงิน** ธนาคารแห่งประเทศไทย เพื่อพิจารณาเป็นรายกรณี

5.9.3 ในระหว่างที่ประกาศธนาคารแห่งประเทศไทยว่าด้วยเหตุการณ์ที่มีนัยสำคัญที่ต้องรายงานต่อธนาคารแห่งประเทศไทย ตามที่กำหนดในข้อ 5.7.1 (2) ยังไม่มีผลบังคับใช้ ให้สถาบันการเงินรายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดขึ้น พร้อมระบุแนวทางการแก้ไขปัญหาหรือเหตุการณ์ผิดปกติดังกล่าวมายัง ฝ่ายตรวจสอบเทคโนโลยีสารสนเทศ สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน ธนาคารแห่งประเทศไทย เพื่อทราบโดยทันทีและไม่เกิน 24 ชั่วโมงนับแต่เกิดหรือรับรู้ปัญหาหรือเหตุการณ์ผิดปกติ

6. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ 28 ธันวาคม 2559

(นายวิรไท สันติประภพ)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

ฝ่ายนโยบายการกำกับสถาบันการเงิน
โทรศัพท์ 0 2283 6938, 0 2283 5839
โทรสาร 0 2283 5938

เอกสารแนบ 1

สรุปการแจ้งและการขออนุญาตธนาคารแห่งประเทศไทย
ในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing)

---

1. **การใช้บริการงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน (Critical IT Outsourcing)**

(1) กรณีการใช้บริการในลักษณะที่ไม่ใช่ Cloud Computing

(1.1) ในกรณีที่เป็นการใช้บริการจากผู้ให้บริการภายนอกที่เป็นบริษัทในกลุ่มธุรกิจเดียวกัน ให้สถาบันการเงินสามารถดำเนินการได้โดยไม่ต้องแจ้งหรือขออนุญาตมายังธนาคารแห่งประเทศไทยก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

(1.2) ในกรณีที่เป็นการใช้บริการจากผู้ให้บริการภายนอกที่ไม่เป็นบริษัทในกลุ่มธุรกิจเดียวกัน ให้สถาบันการเงิน<u>แจ้ง</u>ให้ธนาคารแห่งประเทศไทยทราบล่วงหน้าอย่างน้อย 30 วันก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

(2) กรณีการใช้บริการในลักษณะที่เป็น Cloud Computing (อ้างอิงตามข้อ 5.6.1 (2) ของประกาศ)

(2.1) ในกรณีที่เป็นการใช้บริการ Private Cloud จากผู้ให้บริการภายนอกที่เป็นบริษัทในกลุ่มธุรกิจเดียวกัน ให้สถาบันการเงินสามารถดำเนินการได้โดยไม่ต้องแจ้งหรือขออนุญาตมายังธนาคารแห่งประเทศไทยก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

(2.2) ในกรณีที่เป็นการใช้บริการ Private Cloud จากผู้ให้บริการภายนอกที่ไม่เป็นบริษัทในกลุ่มธุรกิจเดียวกัน ให้สถาบันการเงิน<u>แจ้ง</u>ให้ธนาคารแห่งประเทศไทยทราบล่วงหน้าอย่างน้อย 30 วันก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

(2.3) ในกรณีที่เป็นการใช้บริการ Public Cloud ไม่ว่าจากผู้ให้บริการภายนอกที่เป็นบริษัทในกลุ่มธุรกิจเดียวกันหรือผู้ให้บริการภายนอกที่ไม่เป็นบริษัทในกลุ่มธุรกิจเดียวกัน ให้สถาบันการเงิน<u>ขออนุญาต</u>มายังธนาคารแห่งประเทศไทยล่วงหน้าอย่างน้อย 30 วันก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

<table>
<tr><th rowspan="3">ผู้ให้บริการภายนอก</th><th colspan="3">งาน Critical IT Outsourcing</th></tr>
<tr><th rowspan="2">การใช้บริการ
ในลักษณะที่ไม่ใช่
Cloud Computing</th><th colspan="2">การใช้บริการในลักษณะที่เป็น
Cloud Computing</th></tr>
<tr><th>Private</th><th>Public</th></tr>
<tr><td>1. บริษัท<u>ใน</u>กลุ่มธุรกิจเดียวกัน</td><td colspan="2">ไม่ต้องแจ้ง / ไม่ต้องขออนุญาต</td><td rowspan="2">ต้องขออนุญาตล่วงหน้าอย่างน้อย 30 วันก่อนเริ่ม / เปลี่ยนแปลงการใช้บริการ</td></tr>
<tr><td>2. บริษัท<u>นอก</u>กลุ่มธุรกิจเดียวกัน</td><td colspan="2">ต้องแจ้งล่วงหน้าอย่างน้อย 30 วันก่อนเริ่ม / เปลี่ยนแปลงการใช้บริการ</td></tr>
</table>

2. การใช้บริการงานเทคโนโลยีสารสนเทศประเภทอื่น (Other IT Outsourcing)

ในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น (Other IT Outsourcing) ไม่ว่าจะเป็นกรณีการใช้บริการในลักษณะที่ไม่ใช่ Cloud Computing หรือกรณีการใช้บริการในลักษณะที่เป็น Cloud Computing ให้สถาบันการเงินสามารถดำเนินการได้โดยไม่ต้องแจ้งหรือขออนุญาตมายังธนาคารแห่งประเทศไทยก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

ชื่อสถาบันการเงิน .....

แบบรายงานการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน (Critical IT Outsourcing)

ณ 31 ธันวาคม 25XX

ชื่องาน (ระบุชื่องานตามเอกสารแนบ 2.3)	ลักษณะและขอบเขตในการใช้บริการ[1/]	ลักษณะของการใช้บริการ Cloud Computing[2/] (ถ้ามี)	ชื่อผู้ให้บริการภายนอก[3/]	รายละเอียดเกี่ยวกับผู้ให้บริการภายนอก								วันเริ่มใช้และสิ้นสุดสัญญาหรือข้อตกลงการให้บริการ[6/]	ค่าบริการ[7/] (ถ้ามี)	เลขที่คำขอในระบบ e-Application (ถ้ามี)	เลขที่หนังสือรับทราบ/อนุญาต วัน/เดือน/ปี ที่ได้รับทราบ/อนุญาต (ถ้ามี)	ปัญหาและอุปสรรคจากการใช้บริการ/รายละเอียดเพิ่มเติม (ถ้ามี)
				ประเภทของผู้ให้บริการภายนอก				สถานที่ตั้ง (จดทะเบียน)	ที่ตั้งศูนย์คอมพิวเตอร์[4/]		การรับรองที่เกี่ยวข้องกับงาน IT (certificate)[5/]					
				บริษัทในกลุ่มธุรกิจเดียวกัน		บริษัทนอกกลุ่มธุรกิจ										
				ในประเทศ	ต่างประเทศ	ในประเทศ	ต่างประเทศ		ศูนย์หลัก	ศูนย์สำรอง						
1. โครงสร้าง IT Infrastructure																
1.1 ศูนย์ประมวลผลหลัก																
1.2																
2. Service Channel																
2.1 ระบบงานสาขา																
2.2																
3. ระบบงานรองรับการประมวลผลธุรกรรมของสถาบันการเงิน (Processing System)																
3.1 กลุ่มงานสินเชื่อ																
3.1.1 ระบบสินเชื่อรายใหญ่ (Commercial Loan)																
3.1.2																
4. ระบบงานสนับสนุนการปฏิบัติงาน (Middle & Back Office)																
4.1 ระบบงานด้านบัญชีการเงิน																
4.2																
ตัวอย่าง *3.1.2 ระบบสินเชื่อรายย่อย (Consumer Loan)*	*การประมวลผลข้อมูลการให้บริการสินเชื่อรายย่อย*	-	*ABC (Thailand)*	-	-	✓	-	*ไทย*	*กรุงเทพ*	*ระยอง*	*ISO 27001*	*5 มี.ค. 25XX - 31 ธ.ค. 25XX*	*1,000,000 บาท / ปี*	*A25XXXXXXXXXX*	*ฝกก.(02) XX/25XX 15 ม.ค. 25XX*	*การส่งรายงานล่าช้ากว่าที่กำหนด*

หมายเหตุ:

[1/] ให้ระบุลักษณะและขอบเขตในการใช้บริการพอสังเขป และรายงานเฉพาะการใช้บริการ Critical IT Outsourcing ที่ยังมีผล ณ วันที่รายงานข้อมูล

[2/] ให้ระบุลักษณะของการใช้บริการ Cloud Computing ว่าเป็น Private Cloud หรือ Public Cloud (ถ้ามี)

[3/] ให้ระบุชื่อเฉพาะผู้ให้บริการหลัก ไม่รวมผู้ให้บริการภายนอกที่เข้าทำสัญญาเพื่อรับช่วงงานต่อ (sub-contract)

[4/] ให้ระบุที่ตั้งของศูนย์คอมพิวเตอร์เฉพาะที่เกี่ยวข้องกับงาน IT ที่สถาบันการเงินใช้บริการ เช่น data location

[5/] ให้ระบุเอกสารการรับรองมาตรฐานสากลเฉพาะที่เกี่ยวข้องกับงาน IT ที่สถาบันการเงินใช้บริการ

[6/] ในกรณีที่ไม่มีการระบุวันหมดอายุหรือกำหนดเป็นเงื่อนไข ให้ระบุเฉพาะวันเริ่มต้นสัญญา/ข้อตกลง พร้อมทั้งให้ระบุในช่อง "ปัญหาและอุปสรรคจากการใช้บริการ/รายละเอียดเพิ่มเติม" เช่น สัญญา/ข้อตกลงเป็นแบบไม่กำหนดวันหมดอายุ (open-ended)

[7/] ให้กรอกข้อมูลการคิดค่าบริการตามสัญญาการใช้บริการ เช่น ค่าบริการแบบเหมาจ่ายรายปี/เดือน อัตราค่าบริการต่อธุรกรรม (ถ้ามี)

ชื่อสถาบันการเงิน .....

แบบรายงานการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น (Other IT Outsourcing)

ณ 31 ธันวาคม 25XX

ชื่องาน (ระบุชื่องานตามเอกสารแนบ 2.3)	ลักษณะและขอบเขตในการใช้บริการ[1/]	ลักษณะของการใช้บริการ Cloud Computing[2/] (ถ้ามี)	ชื่อผู้ให้บริการภายนอก[3/]	รายละเอียดเกี่ยวกับผู้ให้บริการภายนอก								วันเริ่มใช้และสิ้นสุดสัญญาหรือข้อตกลงการให้บริการ[6/]	ค่าบริการ[7/] (ถ้ามี)	เลขที่คำขอในระบบ e-Application (ถ้ามี)	เลขที่หนังสือรับทราบ/อนุญาต วัน/เดือน/ปี ที่ได้รับทราบ/อนุญาต (ถ้ามี)	ปัญหาและอุปสรรคจากการใช้บริการ/รายละเอียดเพิ่มเติม (ถ้ามี)
				ประเภทของผู้ให้บริการภายนอก				สถานที่ตั้ง (จดทะเบียน)	ที่ตั้งศูนย์คอมพิวเตอร์[4/]		การรับรองที่เกี่ยวข้องกับงาน IT (certificate)[5/]					
				บริษัทในกลุ่มธุรกิจเดียวกัน		บริษัทนอกกลุ่มธุรกิจ										
				ในประเทศ	ต่างประเทศ	ในประเทศ	ต่างประเทศ		ศูนย์หลัก	ศูนย์สำรอง						
1. โครงสร้าง IT Infrastructure																
1.1 ศูนย์ประมวลผลหลัก																
1.2																
2. Service Channel																
2.1 ระบบงานสาขา																
2.2																
3. ระบบงานรองรับการประมวลผลธุรกรรมของสถาบันการเงิน (Processing System)																
3.1 กลุ่มงานสินเชื่อ																
3.1.1 ระบบสินเชื่อรายใหญ่ (Commercial Loan)																
3.1.2																
4. ระบบงานสนับสนุนการปฏิบัติงาน (Middle & Back Office)																
4.1 ระบบงานด้านบัญชีการเงิน																
4.2																
ตัวอย่าง																
3.4 ระบบสนับสนุนงานขาย	*การประมวลผลข้อมูลเพื่อนำเสนอผลิตภัณฑ์ทางการเงิน*	*Public Cloud*	*XYZ*	-	-	-	√	*สิงคโปร์*	*สิงคโปร์*	*ฮ่องกง*	*ISO 27018*	*1 พ.ค. 25XX - 31 ธ.ค. 25XX*	*200,000 บาท / ปี*	-	-	-

หมายเหตุ:

[1/] ให้ระบุลักษณะและขอบเขตในการใช้บริการพอสังเขป และรายงานเฉพาะการใช้บริการ Other IT Outsourcing ที่ยังมีผล ณ วันที่รายงานข้อมูล

[2/] ให้ระบุลักษณะของการใช้บริการ Cloud Computing ว่าเป็น Private Cloud หรือ Public Cloud (ถ้ามี)

[3/] ให้ระบุชื่อเฉพาะผู้ให้บริการหลัก ไม่รวมผู้ให้บริการภายนอกที่เข้าทำสัญญาเพื่อรับช่วงงานต่อ (sub-contract)

[4/] ให้ระบุที่ตั้งของศูนย์คอมพิวเตอร์เฉพาะที่เกี่ยวข้องกับงาน IT ที่สถาบันการเงินใช้บริการ

[5/] ให้ระบุเอกสารการรับรองมาตรฐานสากลเฉพาะที่เกี่ยวข้องกับงาน IT ที่สถาบันการเงินใช้บริการ

[6/] ในกรณีที่ไม่มีการระบุวันหมดอายุหรือกำหนดเป็นเงื่อนไข ให้ระบุเฉพาะวันเริ่มต้นสัญญา/ข้อตกลง พร้อมทั้งให้ระบุในช่อง "ปัญหาและอุปสรรคจากการใช้บริการ/รายละเอียดเพิ่มเติม" เช่น สัญญา/ข้อตกลงเป็นแบบไม่กำหนดวันหมดอายุ (open-ended)

[7/] ให้กรอกข้อมูลการคิดค่าบริการตามสัญญาการใช้บริการ เช่น ค่าบริการแบบเหมาจ่ายรายปี/เดือน อัตราค่าบริการต่อธุรกรรม (ถ้ามี)

ตัวอย่างชื่องาน IT Outsourcing

1. โครงสร้าง IT Infrastructure
1.1 ศูนย์ประมวลผลหลัก
1.2 ศูนย์ประมวลผลสำรอง
1.3 ระบบเครือข่ายสื่อสาร
1.4 ระบบ Core Banking
1.5 ระบบฐานข้อมูลลูกค้า (CIF)
1.6 ระบบที่เชื่อมต่อกับตัวกลางการโอน/ชำระเงินระหว่างสถาบันการเงิน เช่น ระบบโอนเงินระหว่างประเทศ ระบบ BAHTNET, ORFT, SWIFT, ICAS, Payment Gateway
1.7 ระบบรักษาความปลอดภัยเทคโนโลยีสารสนเทศ
1.8 สื่อบันทึกข้อมูล
1.9 อื่น ๆ (โปรดระบุ)
2. Service Channel
2.1 ระบบงานสาขา
2.2 ระบบ ATM
2.3 ระบบ CDM
2.4 ระบบ Call Center (IVR)
2.5 ระบบ Internet Banking
2.6 ระบบ Mobile Banking
2.7 ระบบ e-Money
2.8 อื่น ๆ (โปรดระบุ)
3. ระบบงานรองรับการประมวลผลธุรกรรมของสถาบันการเงิน (Processing System)
3.1 กลุ่มงานสินเชื่อ
3.1.1 ระบบสินเชื่อรายใหญ่ (Commercial Loan)
3.1.2 ระบบสินเชื่อรายย่อย (Consumer Loan)
3.1.3 ระบบ Hire Purchase
3.1.4 ระบบ Housing Loan
3.1.5 ระบบ Credit Card
3.1.6 ระบบ Credit Rating/Scoring
3.1.7 ระบบ Collateral/Appraisal
3.1.8 ระบบ Loan Approval
3.1.9 ระบบ Collection and Debt Management
3.1.10 อื่น ๆ (โปรดระบุ)
3.2 กลุ่มงานเงินฝาก (เปิดบัญชี/ฝาก/ถอน/โอน/ชำระเงิน)
3.2.1 ..... (โปรดระบุ)
3.3 กลุ่มงานบริหารเงินและธุรกรรมด้านตลาดเงิน
3.3.1 ระบบ Treasury Management
3.3.2 ระบบ Trade Finance
3.3.3 ระบบ FX
3.3.4 ระบบ Cash Management
3.3.5 อื่น ๆ (โปรดระบุ)
3.4 งานอื่น ๆ เช่น ระบบสนับสนุนงานขาย (Customer Relationship Management)
3.4.1 ..... (โปรดระบุ)
4. ระบบงานสนับสนุนการปฏิบัติงาน (Middle & Back Office)
4.1 ระบบงานด้านบัญชีการเงิน
4.2 ระบบบริหารความเสี่ยง
4.3 ระบบ AML/CFT
4.4 ระบบสำนักงานและจัดการเอกสารภายใน (Document Management, Office, Email)
4.5 ระบบงานจัดการ วิเคราะห์ข้อมูล และจัดทำรายงาน เช่น Enterprise Data Warehouse, MIS, DMS-BOT
4.6 ระบบ Fraud Monitoring System
4.7 อื่น ๆ (โปรดระบุ)

***หมายเหตุ** : โปรดใช้เลขข้อและชื่องานตามที่ธนาคารแห่งประเทศไทยกำหนด*

คำถาม – คำตอบแนบท้ายประกาศ
เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing)
ในการประกอบธุรกิจของสถาบันการเงิน
ลงวันที่ 28 ธันวาคม 2559

ข้อ	ประเด็นคำถาม	แนวคำตอบ
ขอบเขตการบังคับใช้		
1.	สาขาต่างประเทศของธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทย (สาขาต่างประเทศฯ) ที่มีการใช้บริการจากผู้ให้บริการภายนอก ต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ด้วยหรือไม่	สาขาต่างประเทศฯ ต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ด้วย เนื่องจากสาขาต่างประเทศฯ ถือเป็นนิติบุคคลเดียวกันกับธนาคารพาณิชย์ที่เป็นสำนักงานใหญ่ในประเทศไทย
2.	บริษัทลูกของธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทยจะต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ด้วยหรือไม่	บริษัทลูกของธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทยที่อยู่ในกลุ่ม Solo Consolidation ต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ด้วย
คำจำกัดความ		
3.	การใช้บริการจากบุคคลภายนอกในเรื่องต่อไปนี้เข้าข่ายเป็นการใช้บริการ IT Outsourcing หรือไม่ และจะมีแนวทางในการพิจารณาว่าเข้าข่ายเป็นการใช้บริการ IT Outsourcing อย่างไร • การจัดซื้อและติดตั้งโปรแกรม (software) สำเร็จรูป เช่น Microsoft Windows หรือ Microsoft Office • การจัดซื้อและติดตั้งอุปกรณ์คอมพิวเตอร์ (hardware) • การจ้างที่ปรึกษาด้านเทคโนโลยีสารสนเทศ หรือการจ้างทีมงานเพื่อพัฒนา software หรือ application • การบำรุงรักษาต่อเนื่องตามโปรแกรมการดูแลของผู้ให้บริการภายนอกสำหรับ hardware และ software • การส่งข้อมูลไปยังบริษัทแม่ เพื่อปฏิบัติตามข้อกำหนดของหลักเกณฑ์ในต่างประเทศ เช่น FATCA • การใช้บริการ IT Outsourcing เพื่อเป็นแผนฉุกเฉินของสถาบันการเงิน • **การใช้บริการข้อมูลการเงิน ข้อมูลตลาด ข้อมูลธุรกิจ เช่น Credit Bureau, BOL, Bloomberg เป็นต้น** • **การตรวจสอบเพื่อรับรองมาตรฐานหรือเอกสารการรับรองที่เกี่ยวข้องกับ IT (certificate)**	การพิจารณาว่า การใช้บริการงาน IT ใดเข้าข่ายเป็น IT Outsourcing ให้พิจารณาว่า งาน IT ที่ใช้บริการจากบุคคลภายนอกนั้น เป็นงาน IT ที่โดยปกติแล้วสถาบันการเงินต้องดำเนินการเอง ซึ่งรวมถึง การพัฒนา software หรือ application และการเตรียมการด้าน IT ตามแผนฉุกเฉินของสถาบันการเงิน <u>แต่ไม่รวมถึง</u> • การจัดซื้อ ติดตั้ง และบำรุงรักษาโปรแกรมสำเร็จรูป (software) ในการทำงานพื้นฐาน เช่น - โปรแกรมการทำงานเอกสาร (ได้แก่ MS Office หรือ SPSS เป็นต้น) - โปรแกรมป้องกันไวรัส (ได้แก่ Norton antivirus หรือ McAfee antivirus เป็นต้น) • การจัดซื้อ ติดตั้ง และบำรุงรักษา อุปกรณ์คอมพิวเตอร์ (hardware) ได้แก่ เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่อง printer เป็นต้น • การใช้บริการที่เชื่อมต่อไปยังระบบกลาง เช่น ระบบการชำระเงิน (ได้แก่ VISA, MASTER, NITMX หรือ PCC เป็นต้น) • การใช้บริการที่เชื่อมต่อไปยังระบบของทางการ (ได้แก่ NCB หรือ DMS เป็นต้น) • การส่งข้อมูลไปยังบริษัทแม่เพื่อปฏิบัติตามหลักเกณฑ์ในต่างประเทศ • **การใช้บริการข้อมูลการเงิน ข้อมูลตลาด ข้อมูลธุรกิจ เช่น Credit Bureau, BOL, Bloomberg, Moody's, Standard & Poors และ Fitch Rating เป็นต้น** • **การตรวจสอบเพื่อรับรองมาตรฐานหรือเอกสาร**

ข้อ	ประเด็นคำถาม	แนวคำตอบ
		การรับรองที่เกี่ยวข้องกับ IT (certificate) เช่น ISO-27001 • **การจ้างบุคคลากรภายนอกมาแก้ไขปัญหาระบบงานที่เกิดขึ้นแบบฉุกเฉินอย่างทันท่วงที ซึ่งสถาบันการเงินไม่สามารถแก้ไขปัญหาดังกล่าวได้**
4.	ในกรณีที่สถาบันการเงินมีการเช่าพื้นที่เพื่อใช้เป็นศูนย์คอมพิวเตอร์ (data center) โดยผู้ให้เช่าทำหน้าที่ในการบริหารจัดการระบบสาธารณูปโภคต่าง ๆ ภายในศูนย์คอมพิวเตอร์ (facility) ด้วย เช่น ระบบไฟฟ้า ระบบทำความเย็นและควบคุมความชื้น ระบบป้องกันและระงับอัคคีภัย เพื่อให้อยู่ในสภาพที่พร้อมใช้งานอย่างต่อเนื่อง เข้าข่ายเป็นการใช้บริการ IT Outsourcing หรือไม่	การเช่าพื้นที่เพื่อใช้เป็นศูนย์คอมพิวเตอร์ โดยผู้ให้เช่าทำหน้าที่บริหารจัดการระบบสาธารณูปโภคด้วย เข้าข่ายเป็นการใช้บริการ IT Outsourcing เนื่องจากการบริหารจัดการระบบสาธารณูปโภคซึ่งเป็นโครงสร้างพื้นฐานที่มีความสำคัญภายในศูนย์คอมพิวเตอร์ถือเป็นปัจจัยหลักที่มีผลต่อการดำเนินการอย่างต่อเนื่องของศูนย์คอมพิวเตอร์นั้น ทั้งนี้ สถาบันการเงินต้องพิจารณาว่า การใช้บริการดังกล่าวเข้าข่ายเป็น Critical IT Outsourcing หรือ Other IT Outsourcing โดยพิจารณาตามความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการใช้บริการดังกล่าวด้วย
การอนุญาตให้สถาบันการเงินใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ		
5.	สถาบันการเงินต้องทำการประเมินตนเอง (self-assessment) ตามหลักเกณฑ์การใช้บริการ IT Outsourcing เมื่อใด	สถาบันการเงินต้องประเมินตนเองตั้งแต่ก่อนเริ่มใช้บริการ IT Outsourcing เพื่อให้ทราบถึงความเสี่ยงจากการใช้บริการและกำหนดแนวทางในการควบคุมและจัดการความเสี่ยงนั้น และเพื่อนำผลการประเมินดังกล่าวมาประเมินประสิทธิภาพในการให้บริการของผู้ให้บริการภายนอกด้วย ทั้งนี้ การประเมินความเสี่ยงควรสอดคล้องกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงาน IT ที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ
การแบ่งประเภทการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ		
6.	แนวทางในการพิจารณาการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน (Critical IT Outsourcing) ควรเป็นอย่างไร	สถาบันการเงินต้องพิจารณาว่า หากงาน IT ที่ใช้บริการมีความเสี่ยงและผลกระทบในวงกว้างทั้งต่อสถาบันการเงิน ระบบสถาบันการเงิน หรือธุรกิจอื่น ก็ถือว่า เข้าข่ายเป็นการใช้บริการ Critical IT Outsourcing
7.	ระบบเครือข่ายสื่อสาร (network) ตามตัวอย่าง Critical IT Outsourcing ในข้อ 5.3.1 หมายถึงอะไร	การใช้บริการระบบเครือข่ายสื่อสาร (network) ที่เข้าข่ายเป็นการใช้บริการ Critical IT Outsourcing หมายถึง การใช้บริการระบบเครือข่ายสื่อสารที่มีการเชื่อมโยงอุปกรณ์ ระบบงาน และข้อมูลสำคัญ เข้าไว้ด้วยกัน และหากระบบเครือข่ายสื่อสารนั้นเกิดความผิดพลาด ก็อาจก่อให้เกิดความเสี่ยงและผลกระทบในวงกว้างทั้งต่อสถาบันการเงิน ระบบสถาบันการเงิน หรือธุรกิจอื่น แต่ไม่รวมถึง การใช้บริการระบบเครือข่ายสื่อสารที่สถาบันการเงินไม่สามารถดำเนินการได้เอง เช่น การใช้บริการระบบเครือข่าย Internet หรือการเช่าสายสื่อสาร fiber optic

ข้อ	ประเด็นคำถาม	แนวคำตอบ
หลักเกณฑ์การควบคุมทั่วไป : นโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ		
8.	คณะกรรมการของสถาบันการเงินมีหน้าที่ให้ความเห็นชอบนโยบายการใช้บริการ IT Outsourcing แล้ว ยังต้องให้ความเห็นชอบการใช้บริการ Critical IT Outsourcing กับบริษัทนอกกลุ่มธุรกิจเดียวกัน ก่อนการใช้บริการด้วยหรือไม่	คณะกรรมการของสถาบันการเงินมีหน้าที่ให้ความเห็นชอบนโยบายการใช้บริการ IT Outsourcing ซึ่งเป็นนโยบายในภาพรวมของการใช้บริการ และการใช้บริการ Critical IT Outsourcing ด้วย แต่สามารถมอบหมายให้คณะกรรมการชุดอื่นให้ความเห็นชอบการใช้บริการ Critical IT Outsourcing แทนได้
9.	ในกรณีสาขาของธนาคารพาณิชย์ต่างประเทศขอเสนอให้สำนักงานใหญ่หรือสำนักงานภูมิภาคของสาขาของธนาคารพาณิชย์ต่างประเทศเป็นผู้อนุมัตินโยบายการใช้บริการ IT Outsourcing เพื่อเพิ่มความคล่องตัวในการดำเนินงาน ได้หรือไม่	สาขาของธนาคารพาณิชย์ต่างประเทศสามารถให้คณะกรรมการที่ได้รับมอบหมายของสำนักงานใหญ่หรือสำนักงานภูมิภาคเป็นผู้อนุมัตินโยบายการใช้บริการ IT Outsourcing ได้ แต่คณะผู้บริหารที่มีหน้าที่รับผิดชอบที่เกี่ยวข้องที่อยู่ในประเทศไทย ต้องให้ความเห็นชอบต่อนโยบายดังกล่าวด้วย
10.	การกำหนดให้นโยบายการใช้บริการ IT Outsourcing ต้องสอดคล้องกับกลยุทธ์ทางธุรกิจ หมายถึงต้องให้สถาบันการเงินกำหนดนโยบายเป็นรายปีว่าในปีนั้นจะมีการใช้บริการ IT Outsourcing อะไรบ้างใช่หรือไม่ และในกรณีที่มีการทบทวนนโยบายการใช้บริการประจำปีแล้ว แต่ไม่มีการแก้ไขปรับปรุง จำเป็นต้องรายงานผลการทบทวนให้คณะกรรมการของสถาบันการเงินทราบหรือไม่	สถาบันการเงินควรกำหนดนโยบายการใช้บริการ IT Outsourcing ให้สอดคล้องกับกลยุทธ์และการแข่งขันทางธุรกิจที่มีการเปลี่ยนแปลง โดยควรทบทวนนโยบายการใช้บริการ IT Outsourcing ดังกล่าวอย่างน้อยปีละครั้ง **ทั้งนี้ หากทบทวนแล้วไม่มีการเปลี่ยนแปลงนโยบายดังกล่าว** สถาบันการเงินต้องรายงานผลการทบทวนให้คณะกรรมการของสถาบันการเงินทราบด้วย
หลักเกณฑ์การควบคุมเฉพาะสำหรับงานเทคโนโลยีสารสนเทศที่มีความสำคัญอย่างยิ่ง		
11.	การกำกับดูแลเพิ่มเติม (specific risk control) ตามหลักเกณฑ์ข้อ 5.5.2 (1) ที่ว่า สถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกมีกระบวนการขั้นตอน การประเมิน และการควบคุมความเสี่ยงอย่างน้อยตามกรอบหลักการด้าน IT ที่สอดคล้องกับมาตรฐานสากลนั้น หมายถึง ผู้ให้บริการภายนอกต้องมีเอกสารการรับรองความเป็นมาตรฐานสากลด้านงาน IT ด้วยใช่หรือไม่ และควรมีมาตรฐานในระดับใด และหากสาขาของธนาคารพาณิชย์ต่างประเทศ ใช้บริการระบบประมวลผลกลาง (core banking) จากบริษัทแม่ สาขาของธนาคารพาณิชย์ต่างประเทศต้องตรวจสอบว่า บริษัทแม่ได้รับการรับรองตามมาตรฐานของ International Organization for Standardization (ISO) ด้วยหรือไม่ และหากบริษัทแม่ไม่มี certificate จะต้องดำเนินการอย่างไร	การกำกับดูแลเพิ่มเติมเป็นหลักเกณฑ์ที่กำหนดให้สถาบันการเงินที่ใช้บริการ Critical IT Outsourcing จากผู้ให้บริการภายนอกรวมถึงบริษัทแม่ ต้องมีกระบวนการในการติดตาม ประเมินผล และตรวจสอบผู้ให้บริการภายนอกเพื่อให้มั่นใจว่า ผู้ให้บริการภายนอกสามารถปฏิบัติตามมาตรฐานสากลด้านงาน IT ได้ ซึ่งอาจทำได้โดยการขอเอกสารหรือหนังสือรับรองที่แสดงถึงการที่ผู้ให้บริการภายนอกสามารถปฏิบัติตามมาตรฐานสากลได้ ทั้งนี้ มาตรฐาน ISO ที่ระบุในประกาศเป็นเพียงตัวอย่างของมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบงานและข้อมูลเท่านั้น จึงอาจใช้มาตรฐานสากลอื่นแทนได้ แต่สถาบันการเงินควรพิจารณาระดับของมาตรฐานสากลที่ผู้ให้บริการภายนอกควรปฏิบัติได้ โดยพิจารณาจากขนาดปริมาณธุรกรรม ความซับซ้อนของงาน IT ที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ ทั้งนี้ ในกรณีที่**ใช้บริการจากบริษัทแม่และ**บริษัทแม่ไม่มี certificate สาขาของธนาคารพาณิชย์ต่างประเทศสามารถใช้ผลการตรวจสอบของบริษัทแม่ที่ได้รับการรับรองจากผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก**ที่มี**

ข้อ	ประเด็นคำถาม	แนวคำตอบ
		ความเป็นอิสระได้ ทั้งนี้คณะกรรมการของสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมายต้องรับทราบผลการตรวจสอบดังกล่าวด้วย
12.	กระบวนการ ขั้นตอน หรือระบบในการติดตามประเมินผล และตรวจสอบผู้ให้บริการภายนอก เช่น การทดสอบระบบการรักษาความปลอดภัยเชิงลึก (penetration test) สำหรับการใช้บริการระบบ internet banking ตามที่กำหนดในข้อ 5.5.2 (1.2) นั้น ควรมีความถี่เท่าใด	สถาบันการเงินควรจัดให้ผู้ให้บริการภายนอกมีการทดสอบระบบการรักษาความปลอดภัยเชิงลึก (penetration test) อย่างน้อยปีละครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงค่าความปลอดภัยหรือมีการเปลี่ยนแปลงความเสี่ยงด้าน IT อย่างมีนัยสำคัญที่อาจเปิดช่องโหว่ให้เกิดภัยคุกคามจากภายในและภายนอกได้
แนวปฏิบัติสำหรับการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ		
13.	ในกรณีที่ผู้ให้บริการภายนอกมีการจ้างผู้ให้บริการภายนอกรายอื่นรับช่วงจัดการงาน IT ที่รับให้บริการต่อ (sub-contract) โดยงานดังกล่าวนั้นเป็นงาน Critical IT Outsourcing สถาบันการเงินจะต้องปฏิบัติอย่างไร	ในกรณีที่ผู้ให้บริการภายนอกมีการ sub-contract งาน IT ที่รับให้บริการบางส่วนหรือทั้งหมดต่อให้กับผู้ให้บริการภายนอกรายอื่น สถาบันการเงินไม่ต้องแจ้งการ sub-contract ดังกล่าวมายังธนาคารแห่งประเทศไทย แต่สถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกจะรับผิดชอบต่อการให้บริการด้านงาน IT แก่สถาบันการเงินเสมือนกับที่ผู้ให้บริการภายนอกเป็นผู้ให้บริการด้วยตนเอง และการ sub-contract นั้นจะต้องไม่มีเจตนาหลีกเลี่ยงการปฏิบัติตามหลักเกณฑ์ IT Outsourcing
การรายงานต่อธนาคารแห่งประเทศไทย		
14.	ตามที่ธนาคารแห่งประเทศไทยกำหนดให้ต้องมีการจัดทำรายงานการใช้บริการ IT Outsourcing **ตามแบบรายงานที่กำหนดในเอกสารแนบ 2** ซึ่งมีเนื้อหาครอบคลุมวันที่เริ่มใช้บริการและวันที่สิ้นสุดสัญญาหรือข้อตกลงการให้บริการนั้น เนื่องจากสาขาของธนาคารพาณิชย์ต่างประเทศเป็นผู้รับนโยบายการใช้บริการ IT Outsourcing จากบริษัทแม่ในต่างประเทศ ซึ่งสัญญาที่เกี่ยวข้องกับการใช้บริการ IT Outsourcing ส่วนใหญ่จะดำเนินการและจัดทำโดยบริษัทแม่ โดยไม่ได้กำหนดวันสิ้นสุดสัญญาไว้ และสัญญาบางฉบับอาจถูกจัดทำไว้เป็นเวลานาน สาขาของธนาคารพาณิชย์ต่างประเทศ ควรดำเนินการอย่างไรหากไม่สามารถจัดหาข้อมูลวันที่เริ่มใช้บริการและวันที่สิ้นสุดสัญญาได้	ตามหลักการบริหารความเสี่ยงที่ดี สถาบันการเงินควรเก็บสัญญาหรือข้อตกลงการให้บริการที่ยังมีผลบังคับใช้อยู่ไว้เพื่อเป็นเอกสารหลักฐานประกอบการดำเนินการต่าง ๆ ที่เกี่ยวข้อง ซึ่งในสัญญาหรือข้อตกลงการให้บริการโดยทั่วไปควรระบุวันเริ่มต้นและวันสิ้นสุดการให้บริการไว้ แต่หากสัญญาหรือข้อตกลงการให้บริการมีการกำหนดวันสิ้นสุดสัญญาเป็นเงื่อนไข เช่น สิ้นสุดเมื่อได้รับการบอกเลิกสัญญา **ให้สถาบันการเงินรายงานวันเริ่มต้นการใช้บริการในช่อง "วันเริ่มใช้และสิ้นสุดสัญญาหรือข้อตกลงการให้บริการ" และระบุเงื่อนไขของการสิ้นสุดสัญญานั้นในช่อง "ปัญหาและอุปสรรคจากการใช้บริการ/รายละเอียดเพิ่มเติม"** ทั้งนี้ หากสัญญาหรือข้อตกลงการให้บริการถูกดำเนินการหรือจัดทำโดยบริษัทแม่ สาขาของธนาคารพาณิชย์ต่างประเทศควรขอข้อมูลดังกล่าวจากบริษัทแม่
15.	ในการกำหนดให้สถาบันการเงินต้องจัดทำรายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดขึ้นจากการใช้บริการ IT Outsourcing ที่มีผลกระทบต่อการให้บริการของสถาบันการเงิน ตามข้อ 5.7.1 (2) นั้น ปัญหาหรือเหตุการณ์ผิดปกติดังกล่าว หมายถึง	ปัญหาหรือเหตุการณ์ผิดปกติที่ส่งผลกระทบต่อการให้บริการการเงินพื้นฐานในวงกว้าง**ที่ต้องรายงานตามข้อ 5.7.1 (2)** เช่น ธุรกรรมการฝากเงิน การถอนเงิน และการโอนเงิน อาจเกิดขึ้นได้ทั้งจากการใช้บริการ Critical IT Outsourcing และ Other IT Outsourcing

ข้อ	ประเด็นคำถาม	แนวคำตอบ
	ปัญหาหรือเหตุการณ์ผิดปกติที่เกิดขึ้นจากการใช้บริการ Critical IT Outsourcing เท่านั้น ใช่หรือไม่	ตัวอย่างปัญหาหรือเหตุการณ์ผิดปกติดังกล่าว เช่น • ระบบไฟฟ้าภายในศูนย์คอมพิวเตอร์ (data center) มีปัญหาทำให้เครื่องประมวลผลสำคัญหยุดชะงัก • ระบบประมวลผลกลาง (core banking) มีปัญหาทำให้ไม่สามารถประมวลผลรายการสำคัญได้ • ระบบเครือข่าย (network) มีปัญหา ทำให้ไม่สามารถเชื่อมโยงระบบต่าง ๆ เช่น ระบบช่องทางสาขา หรือระบบ ATM เพื่อให้บริการแก่ประชาชนได้ ทั้งนี้ **ในระหว่างที่ประกาศธนาคารแห่งประเทศไทยว่าด้วยเหตุการณ์ที่มีนัยสำคัญที่ต้องรายงานต่อธนาคารแห่งประเทศไทย ยังไม่มีผลบังคับใช้** สถาบันการเงินสามารถกำหนดรูปแบบรายงานได้ตามความเหมาะสม โดยอย่างน้อยควรระบุถึงลักษณะของปัญหาหรือเหตุการณ์ผิดปกติ และแนวทางการแก้ไขปัญหาหรือเหตุการณ์ผิดปกติดังกล่าว
การตรวจสอบผู้ให้บริการภายนอกของสถาบันการเงิน		
16.	การตรวจสอบผู้ให้บริการภายนอกทุกการใช้บริการ IT Outsourcing อาจเป็นภาระมากเกินไป สถาบันการเงินสามารถตรวจสอบผู้ให้บริการภายนอกเฉพาะ Critical IT Outsourcing โดยใช้แบบสอบถามหรือให้ผู้ตรวจสอบที่เป็นอิสระตรวจสอบแทน ได้หรือไม่	ธนาคารแห่งประเทศไทยไม่ได้จำกัดรูปแบบและวิธีการในการตรวจสอบผู้ให้บริการภายนอก แต่ต้องทำให้สถาบันการเงินได้รับทราบข้อมูลที่แสดงถึงความสามารถของผู้ให้บริการภายนอกในการปฏิบัติตามนโยบายและเงื่อนไขที่กำหนดได้ โดยเฉพาะในด้านการรักษาความปลอดภัยและความลับของข้อมูล (security) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (availability)
ประเด็นอื่น ๆ		
17.	ประกาศการใช้บริการ IT Outsourcing เกี่ยวข้องกับแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT best practice สำหรับธุรกรรมฝาก ถอน และโอนเงิน และธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์ การให้บริการการเงินและการชำระเงินทางอิเล็กทรอนิกส์) อย่างไร	ประกาศฉบับนี้เป็นการกำหนดหลักเกณฑ์ให้สถาบันการเงินที่มีการใช้บริการ IT Outsourcing ถือปฏิบัติ ในขณะที่ IT best practice เป็นแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงด้าน Operational / IT risk management ซึ่งสถาบันการเงินสามารถนำ IT best practice มาประยุกต์ใช้ให้เหมาะสมกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงาน IT ที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการได้
18.	สถาบันการเงินสามารถกำหนดระดับความเสี่ยงและหลักเกณฑ์การประเมินความเสี่ยงในการใช้บริการ IT Outsourcing ตามกรอบการบริหารความเสี่ยงของสถาบันการเงินเองได้ ใช่หรือไม่	สถาบันการเงินสามารถพิจารณาปฏิบัติตามหลักเกณฑ์การควบคุมความเสี่ยงต่าง ๆ ให้สอดคล้องกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงาน IT ที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการได้

ฝ่ายนโยบายการกำกับสถาบันการเงิน
โทร. 0-2283-6938, 0-2283-5869