ธนาคารแห่งประเทศไทย

4 สิงหาคม 2557

เรียน ผู้จัดการ

สถาบันการเงินทุกแห่ง

ที่ ฝนส.(01) ว. 17 /2557 เรื่อง การนำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน

ตามที่ธนาคารแห่งประเทศไทย (ธปท.) ได้อนุญาตให้สถาบันการเงินสามารถใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจ เพื่อช่วยส่งเสริมให้เกิดประสิทธิภาพด้านการดำเนินงานการบริหารต้นทุน และเพิ่มศักยภาพในการพัฒนาการให้บริการทางการเงินให้ทันต่อเทคโนโลยีที่มีการเปลี่ยนแปลงอย่างรวดเร็ว นั้น

เนื่องจากสถาบันการเงินมีความจำเป็นต้องใช้ระบบเทคโนโลยีสารสนเทศที่มีความซับซ้อนและทันสมัยมากขึ้น เพื่อสร้างศักยภาพในการให้บริการและเพื่อรองรับการแข่งขันเมื่อมีการเปิด AEC ในปี 2558 ในขณะที่สถาบันการเงินยังมีข้อจำกัดด้านทรัพยากรที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศ ดังนั้น ธปท. จึงได้ปรับปรุงแนวทางการกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศให้มีความยืดหยุ่นและสอดคล้องกับแนวปฏิบัติของสถาบันการเงินมากขึ้น และให้สามารถรองรับการใช้บริการเทคโนโลยีที่มีการพัฒนาใหม่ โดยปรับปรุงคำจำกัดความของงานเทคโนโลยีสารสนเทศให้เป็นมาตรฐานสากล และแบ่งประเภทการใช้บริการออกเป็น 2 ประเภท คือ การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน (Critical IT Outsourcing) และการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น (Other IT Outsourcing) และกำหนดหลักเกณฑ์การกำกับดูแลให้สอดคล้องกับประเภทการใช้บริการนั้น นอกจากนี้ ได้ปรับปรุงแนวทางในการแจ้งการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ โดยกำหนดให้สถาบันการเงินแจ้งการใช้บริการให้ ธปท. ทราบล่วงหน้าอย่างน้อย 30 วัน ก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการเฉพาะกรณีการใช้บริการด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงินจากผู้ให้บริการภายนอกที่ไม่เป็นบริษัทในกลุ่มธุรกิจเดียวกันเท่านั้น ส่วนการรายงานข้อมูลมายัง ธปท. นั้น ให้สถาบันการเงินส่งรายงานการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศทุกประเภทเป็นประจำทุกปี และให้รายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดขึ้นจากการใช้บริการจากผู้ให้บริการภายนอกที่มีผลกระทบต่อการให้บริการการเงินพื้นฐานของสถาบันการเงิน โดยเร็วและไม่ควรเกิน 24 ชั่วโมง โดยมีรายละเอียดของหลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศตามที่ปรากฏในประกาศธนาคารแห่งประเทศไทย ที่ สนส. 6/2557 ซึ่งได้ลงประกาศแล้วในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป เล่ม 131 ตอนพิเศษ 142 ง ลงวันที่ 29 กรกฎาคม 2557 และมีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ทั้งนี้ ในการอนุญาตให้สถาบันการเงินใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศดังกล่าว ธปท. ขอสงวนสิทธิในการกำหนดหลักเกณฑ์อื่นเพิ่มเติม สั่งการ และ/หรือ กำหนดเงื่อนไข

ฝนสว00-คส52001 -25570804

คส520	วันที่ 4 ส.ค. 2557

หรือสั่งเพิกถอนการใช้บริการ ทั้งก่อนและหลังจากที่สถาบันการเงินใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ รวมถึงพิจารณาผ่อนผันเป็นรายกรณี ตามความจำเป็น

อนึ่ง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศที่ผู้ให้บริการภายนอกมีการใช้เทคโนโลยี Cloud computing ในการให้บริการ (เช่น การให้บริการด้านจดหมายอิเล็กทรอนิกส์ การให้บริการด้านโปรแกรม หรือการให้บริการด้านการจัดเก็บข้อมูล เป็นต้น) เข้าข่ายเป็นการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทหนึ่ง ดังนั้น สถาบันการเงินจึงต้องถือปฏิบัติตามหลักเกณฑ์การกำกับดูแลที่กำหนดในประกาศฉบับนี้ อย่างไรก็ดี เนื่องจากเทคโนโลยี Cloud computing เป็นเทคโนโลยีที่เกี่ยวข้องกับการจัดสรรทรัพยากรด้านงานเทคโนโลยีสารสนเทศ อีกทั้ง การใช้เทคโนโลยี Cloud computing อาจนำไปสู่การจัดเก็บหรือประมวลผลข้อมูลสำคัญของสถาบันการเงิน ซึ่งถือเป็น Critical IT Outsourcing หรืออาจนำไปสู่การกระจุกตัวอยู่ที่ผู้ให้บริการเพียงบางราย ดังนั้น ในระยะแรกนี้ หากสถาบันการเงินประสงค์จะใช้บริการจากผู้ให้บริการภายนอกที่มีการใช้เทคโนโลยี Cloud computing ให้สถาบันการเงินหารือ ธปท. เป็นรายกรณีก่อนเริ่มใช้บริการนั้น

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นายสมบูรณ์ จิตเป็นธม)
ผู้อำนวยการอาวุโส ฝ่ายนโยบายการกำกับสถาบันการเงิน
ผู้ว่าการแทน

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

ฝ่ายนโยบายการกำกับสถาบันการเงิน
โทรศัพท์ 0 2283 6938, 0 2283 5839, 0 2283 6835
โทรสาร 0 2283 5938

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

ธนาคารแห่งประเทศไทย

ประกาศธนาคารแห่งประเทศไทย
ที่ สนส. 6 /2557
เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน

---

1. เหตุผลในการออกประกาศ

เดิมธนาคารแห่งประเทศไทยอนุญาตให้สถาบันการเงินสามารถใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ทั้งในประเทศและต่างประเทศได้ในทุกระบบงาน เพื่อส่งเสริมให้เกิดประสิทธิภาพในด้านการดำเนินงานและการบริหารต้นทุน และเพิ่มศักยภาพในการพัฒนาการให้บริการทางการเงินให้ทันต่อเทคโนโลยีที่มีการเปลี่ยนแปลงอย่างรวดเร็ว โดยได้กำหนดหลักเกณฑ์เพื่อให้สถาบันการเงินสามารถใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพและเป็นที่น่าเชื่อถือ บนพื้นฐานของการรักษาประโยชน์ของประชาชนผู้ใช้บริการ ดังนั้น แม้ว่าสถาบันการเงินจะใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ แต่สถาบันการเงินยังคงต้องมีความรับผิดชอบต่อการให้บริการอย่างต่อเนื่องแก่ผู้ใช้บริการของสถาบันการเงิน ต้องคงความน่าเชื่อถือของการให้บริการเช่นเดียวกับที่สถาบันการเงินพึงจะมีเสมือนกับที่สถาบันการเงินเป็นผู้ดำเนินการด้านเทคโนโลยีสารสนเทศด้วยตนเอง และต้องคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นต่อสถาบันการเงินในรูปแบบที่เปลี่ยนแปลงไปจากการดำเนินงานปกติที่ดำเนินการโดยสถาบันการเงินเอง เช่น ความเสี่ยงด้านปฏิบัติการ (operational risk) จากการดำเนินงานของผู้ให้บริการภายนอก ความเสี่ยงด้านกลยุทธ์ (strategic risk) ในการวางแผนการดำเนินธุรกิจ ความเสี่ยงด้านชื่อเสียง (reputational risk) และความเสี่ยงด้านกฎหมาย (legal risk) โดยเฉพาะเรื่องการรักษาความลับของข้อมูลของผู้ใช้บริการของสถาบันการเงิน **นอกจากนี้ ธนาคารแห่งประเทศไทยยังได้กำหนดให้สถาบันการเงินต้องประเมินความเสี่ยงที่เกี่ยวข้องจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศทั้งในประเทศและต่างประเทศ และแจ้งรายละเอียดการใช้บริการมายังธนาคารแห่งประเทศไทยเพื่อทราบก่อนเริ่มหรือก่อนเปลี่ยนแปลงการใช้บริการ**

เนื่องจากการดำเนินธุรกิจและการแข่งขันของสถาบันการเงินในปัจจุบันและแนวโน้มในอนาคตมีความต้องการใช้ระบบเทคโนโลยีสารสนเทศที่มีความซับซ้อนและทันสมัยมากขึ้นเพื่อการให้บริการมีประสิทธิภาพ ในขณะที่ทรัพยากรด้านเทคโนโลยีสารสนเทศของสถาบันการเงินอาจมีข้อจำกัด สถาบันการเงินจึงมีแนวโน้มที่จะมีการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศเพิ่มขึ้น ในขณะที่หลักเกณฑ์ปัจจุบันมีข้อกำหนดที่ยังไม่คล่องตัวและอาจไม่สอดคล้องกับแนวทางในการบริหารจัดการความเสี่ยงของสถาบันการเงินและการพัฒนาด้านเทคโนโลยีสารสนเทศ

ดังนั้น ธนาคารแห่งประเทศไทยจึงเห็นควรปรับปรุงหลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศให้มีความยืดหยุ่นและสอดคล้องกับแนวปฏิบัติของสถาบันการเงิน โดยกำหนดหลักเกณฑ์ในลักษณะที่เป็นหลักการ (principle based) มากขึ้น

ฝนสป00-คส52001 -2557071 4

คส520	วันที่ 14 ก.ค. 2557

แต่ยังคงให้ความสำคัญกับการรักษาผลประโยชน์ของประชาชนผู้ใช้บริการเช่นเดิม คือ สถาบันการเงินยังคงต้องมีความรับผิดชอบต่อการให้บริการอย่างต่อเนื่องแก่ผู้ใช้บริการของสถาบันการเงิน และต้องคงความน่าเชื่อถือของการให้บริการเช่นเดียวกับที่สถาบันการเงินพึงจะมีเสมือนกับที่สถาบันการเงินเป็นผู้ดำเนินการด้านเทคโนโลยีสารสนเทศด้วยตนเอง และมุ่งเน้นให้สถาบันการเงินให้ความสำคัญกับการบริหารความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศภายใต้กรอบหลักการด้านเทคโนโลยีสารสนเทศที่สำคัญ 3 ประการ คือ การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (security) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (availability) และให้สถาบันการเงินมีการบริหารความเสี่ยงที่อาจเกิดขึ้นอย่างเหมาะสม โดยสถาบันการเงินต้องมีการประเมินตนเอง (self assessment) ควบคุม และจัดการความเสี่ยงที่มีประสิทธิภาพ มีการกำกับดูแลโดยคณะกรรมการของสถาบันการเงิน (board oversight) และมีการพิจารณาถึงความสอดคล้องกับกลยุทธ์การดำเนินธุรกิจและความสำคัญต่อการลงทุนในระบบเทคโนโลยีสารสนเทศเพื่อส่งเสริมศักยภาพในการแข่งขัน (competitiveness) โดยเฉพาะสถาบันการเงินไทย นอกจากนี้ การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศของสถาบันการเงินอาจก่อให้เกิดผลกระทบต่อทั้งผู้ใช้บริการของสถาบันการเงิน สถาบันการเงิน และระบบการเงิน ดังนั้น นอกจากสถาบันการเงินต้องมีการกำกับดูแลผู้ให้บริการภายนอกอย่างใกล้ชิดแล้ว ยังต้องดำเนินการให้ธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายนอก หรือหน่วยงานกำกับดูแลอื่นได้รับทราบข้อมูลที่เกี่ยวข้องกับการใช้บริการและสามารถตรวจสอบผู้ให้บริการดังกล่าวได้

การปรับปรุงประกาศในครั้งนี้ ธนาคารแห่งประเทศไทยได้ปรับปรุงคำจำกัดความของงานเทคโนโลยีสารสนเทศให้เป็นมาตรฐานสากลมากขึ้น และแบ่งประเภทการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศของสถาบันการเงินออกเป็น 2 ประเภท คือ การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน (Critical IT Outsourcing) และการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น (Other IT Outsourcing) พร้อมทั้ง กำหนดหลักเกณฑ์การกำกับดูแลให้สอดคล้องกับประเภทการใช้บริการนั้น นอกจากนี้ ธนาคารแห่งประเทศไทยได้กำหนดให้สถาบันการเงินแจ้งการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศให้ธนาคารแห่งประเทศไทยทราบล่วงหน้าอย่างน้อย 30 วัน ก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ เฉพาะกรณีการใช้บริการด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงินจากผู้ให้บริการภายนอกที่ไม่เป็นบริษัทในกลุ่มธุรกิจเดียวกันเท่านั้น และได้กำหนดให้สถาบันการเงินส่งรายงานดังนี้มายังธนาคารแห่งประเทศไทย (1) รายงานการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศโดยให้ส่งเป็นประจำทุกปี และ (2) รายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดขึ้นจากการใช้บริการจากผู้ให้บริการภายนอกที่มีผลกระทบต่อการให้บริการการเงินพื้นฐานของสถาบันการเงิน โดยให้ส่งโดยเร็วและไม่ควรเกิน 24 ชั่วโมง

2. อำนาจตามกฎหมาย

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

3. ประกาศที่ยกเลิก

ให้ยกเลิกประกาศธนาคารแห่งประเทศไทย ที่ สนส. 29/2551 เรื่อง การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) ลงวันที่ 3 สิงหาคม 2551

4. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ใช้บังคับกับสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

5. เนื้อหา

5.1 คำจำกัดความ

ในประกาศฉบับนี้

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

"ผู้ให้บริการภายนอก" (service provider) หมายความว่า บุคคลภายนอกทั้งในและต่างประเทศ รวมถึง บริษัทในกลุ่มธุรกิจเดียวกัน ซึ่งเข้าทำสัญญาหรือทำข้อตกลงในการให้บริการงานให้กับสถาบันการเงิน อันมีลักษณะที่โดยปกติแล้วสถาบันการเงินต้องดำเนินการเอง

"บริษัทในกลุ่มธุรกิจเดียวกัน"

(1) กรณีธนาคารพาณิชย์ที่จดทะเบียนในประเทศ หมายความว่า บริษัทในกลุ่มธุรกิจทางการเงินตามประกาศธนาคารแห่งประเทศไทย ว่าด้วยหลักเกณฑ์การกำกับแบบรวมกลุ่ม

(2) กรณีธนาคารพาณิชย์ที่จดทะเบียนจัดตั้งขึ้นในประเทศไทย แต่เป็นบริษัทลูกของสถาบันการเงินในต่างประเทศ หมายความว่า บริษัทในกลุ่มธุรกิจทางการเงินตามประกาศธนาคารแห่งประเทศไทย ว่าด้วยหลักเกณฑ์การกำกับแบบรวมกลุ่ม รวมถึง บริษัทที่มีความเกี่ยวข้องกับธนาคารพาณิชย์ที่จดทะเบียนจัดตั้งขึ้นในประเทศไทย แต่เป็นบริษัทลูกของสถาบันการเงินในต่างประเทศนั้น

(3) กรณีสาขาของธนาคารพาณิชย์ต่างประเทศ หมายความว่า สำนักงานใหญ่ สาขาที่อยู่ในประเทศอื่น สำนักงานภูมิภาคในต่างประเทศของสาขาของธนาคารพาณิชย์ต่างประเทศ รวมถึง บริษัทที่มีความเกี่ยวข้องกับธนาคารพาณิชย์ต่างประเทศนั้น

"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)

"คณะกรรมการของสถาบันการเงิน" หมายความว่า คณะกรรมการของสถาบันการเงินที่จดทะเบียนในประเทศไทย หรือคณะผู้บริหารที่มีอำนาจหน้าที่รับผิดชอบที่เกี่ยวข้องของสาขาของธนาคารพาณิชย์ต่างประเทศ

5.2 การอนุญาตให้สถาบันการเงินใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

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

ทั้งนี้ หลักการสำคัญของการอนุญาตให้สถาบันการเงินใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ คือ

(1) สถาบันการเงินต้องรับผิดชอบต่อการให้บริการอย่างต่อเนื่องแก่ผู้ใช้บริการของสถาบันการเงิน ต้องคงความน่าเชื่อถือของการให้บริการเช่นเดียวกับที่สถาบันการเงินพึงจะมีเสมือนกับที่สถาบันการเงินเป็นผู้ดำเนินการด้านเทคโนโลยีสารสนเทศด้วยตนเอง และต้องคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นต่อสถาบันการเงินในรูปแบบที่เปลี่ยนแปลงไปจากการดำเนินงานปกติที่กระทำโดยสถาบันการเงินเอง

ในกรณีที่ผู้ให้บริการภายนอกมีการให้ผู้ให้บริการภายนอกรายอื่นรับช่วงจัดการงานด้านเทคโนโลยีสารสนเทศที่ให้บริการแก่สถาบันการเงินต่อ (sub-contract) สถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกจะรับผิดชอบต่อการให้บริการด้านงานเทคโนโลยีสารสนเทศแก่สถาบันการเงินเสมือนกับที่ผู้ให้บริการภายนอกเป็นผู้ให้บริการด้วยตนเอง

(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 หรือ

(3) ความเสียหายหรือเหตุการณ์อื่น เช่น การทุจริตทั้งทางตรงและทางอ้อมในวงกว้างหรือร้ายแรง ภัยคุกคามด้านเทคโนโลยีสารสนเทศทั้งจากภายในและภายนอก และเหตุการณ์อื่นตามที่ธนาคารแห่งประเทศไทยอาจกำหนดเพิ่มเติม

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

5.3.2 การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น (Other IT Outsourcing)

การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น หมายถึง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศที่ไม่เข้าข่ายเป็นการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงินตามข้อ 5.3.1

ทั้งนี้ หากสถาบันการเงินมีข้อสงสัยเกี่ยวกับการพิจารณาประเภทการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ ให้สถาบันการเงินหารือมาที่ ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ สายกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทย ก่อนดำเนินการ

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 รวมถึง หลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ 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

(1.1) สถาบันการเงินต้องกำหนดกลยุทธ์ที่ชัดเจนสำหรับการตัดสินใจใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ เช่น เหตุผลความจำเป็นทางธุรกิจ รวมถึงประโยชน์และต้นทุน ทั้งนี้ สถาบันการเงินต้องมั่นใจว่า การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศนั้น ไม่ขัดต่อกฎหมายและข้อบังคับของทางการของประเทศไทยและประเทศของผู้ให้บริการภายนอก ในกรณีที่ผู้ให้บริการภายนอกประกอบธุรกิจในต่างประเทศ ไม่ก่อให้เกิดช่องโหว่ที่นำไปสู่การเกิดการทุจริตที่ร้ายแรงหรือก่อให้เกิดภัยคุกคามด้านเทคโนโลยีสารสนเทศทั้งจากภายในและภายนอก จนอาจส่งผลกระทบต่อธุรกิจอย่างร้ายแรง และไม่ส่งผลกระทบต่อเสถียรภาพของระบบสถาบันการเงิน และระบบการเงินของประเทศไทยอย่างร้ายแรง

(1.2) สถาบันการเงินต้องกำหนดนโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศอย่างชัดเจนและเป็นลายลักษณ์อักษร โดยต้องสอดคล้องกับนโยบายในการใช้บริการจากบุคคลภายนอก (outsourcing policy) และต้องคำนึงถึงความสอดคล้อง

กับกลยุทธ์ทางธุรกิจและความสามารถในการแข่งขัน ซึ่งนโยบายดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการของสถาบันการเงิน **ทั้งนี้ นโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศควรครอบคลุมเรื่อง การแบ่งประเภทของการใช้บริการ การบริหารความเสี่ยงที่เกิดจากการใช้บริการ การบริหารจัดการผู้ให้บริการภายนอก การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล การรักษาความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล การรักษาความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ การคุ้มครองผู้ใช้บริการของสถาบันการเงิน การกำกับดูแลเพิ่มเติมกรณีการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน (Critical IT Outsourcing) และการรายงานและการตรวจสอบ เป็นต้น**

(1.3) สถาบันการเงินต้องมีการทบทวนนโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับกลยุทธ์ของสถาบันการเงินที่อาจเปลี่ยนแปลงไป

(2) การบริหารความเสี่ยง

(2.1) สถาบันการเงินต้องกำหนดนโยบายการบริหารความเสี่ยง**จากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ**อย่างชัดเจน**และเป็นลายลักษณ์อักษร** โดยต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงโดยรวมของสถาบันการเงิน รวมถึง **ขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ** และต้องได้รับความเห็นชอบจากคณะกรรมการของสถาบันการเงิน**หรือคณะกรรมการที่ได้รับมอบหมาย** รวมทั้งต้องมีการกำหนดแนวทาง วิธีการ และผู้รับผิดชอบในการบริหารความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศอย่างชัดเจนและเป็นลายลักษณ์อักษร ต้องประเมินผลการปฏิบัติตามแนวทางและวิธีการที่กำหนดอย่างสม่ำเสมอ **และต้องมีการรายงานผลการปฏิบัติดังกล่าวให้คณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสม**

(2.2) สถาบันการเงิน**ต้องมีความรู้ความเข้าใจในงานเทคโนโลยีสารสนเทศที่ใช้บริการจากผู้ให้บริการภายนอกตามสมควร** ต้องสามารถประเมินระดับความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ **และต้องจัดให้มีระบบการประเมิน ควบคุมและบริหารจัดการความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศให้ครอบคลุมความเสี่ยงที่สำคัญที่อาจเกิดขึ้น (เช่น ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านกฎหมาย และความเสี่ยงด้านเทคโนโลยีสารสนเทศ) โดยควรสอดคล้องกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ**

(2.3) **สถาบันการเงินต้องจัดให้มีแนวทางในการติดตามประสิทธิภาพในการให้บริการของผู้ให้บริการภายนอกอย่างต่อเนื่อง แนวทางในการรับทราบการเปลี่ยนแปลงที่เกิดขึ้นกับผู้ให้บริการภายนอก รวมถึง แนวทางในการรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นจากการให้บริการของผู้ให้บริการภายนอก (day-to-day incident) อย่างสม่ำเสมอ ทั้งนี้ สถาบันการเงินต้องมีส่วนร่วมในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติ หากสถาบันการเงินประเมินว่า เหตุการณ์ผิดปกติที่เกิดขึ้นนั้นอาจกระทบต่อการดำเนินธุรกิจของสถาบันการเงินอย่างมีนัยสำคัญ นอกจากนี้ สถาบันการเงินต้องมีการทบทวนและประเมินประสิทธิภาพในการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ และมีการรายงานผล**

การประเมินดังกล่าวให้คณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสม

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

(3) การบริหารจัดการผู้ให้บริการภายนอก (service provider management)

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

(3.2) สถาบันการเงินต้องมีการจัดทำสัญญาการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร **หรือมีการจัดทำข้อตกลงการให้บริการ (service level agreement) เป็นลายลักษณ์อักษรกรณีที่ผู้ให้บริการภายนอกเป็นบริษัทในกลุ่มธุรกิจเดียวกัน** และต้องระบุบทบาท หน้าที่ ความรับผิดชอบ เงื่อนไขการให้บริการของผู้ให้บริการภายนอก **และความรับผิดต่อความเสียหายอย่างใด ๆ ในกรณีที่ผู้ให้บริการภายนอกไม่ปฏิบัติตามเงื่อนไขในการให้บริการ ไว้ในสัญญาหรือข้อตกลงให้บริการให้ชัดเจน ส่วนเนื้อหาของสัญญาและข้อตกลงการให้บริการ**ควรครอบคลุมประเด็นสำคัญ เช่น ขอบเขตงานเทคโนโลยีสารสนเทศที่ใช้บริการและเงื่อนไขในการให้บริการของผู้ให้บริการภายนอก มาตรฐานของการปฏิบัติงานขั้นต่ำที่ต้องการจากผู้ให้บริการภายนอก **(เช่น มาตรฐานด้านการรักษาความปลอดภัยและความลับของข้อมูล ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ)** ระบบการควบคุมภายในของผู้ให้บริการภายนอก การจัดทำแผนฉุกเฉินสำหรับการให้บริการของผู้ให้บริการภายนอกที่ควรสอดคล้องกับแผนฉุกเฉินของสถาบันการเงิน การรายงานผลการปฏิบัติงานของผู้ให้บริการภายนอก**ซึ่งครอบคลุมถึงการรายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการให้บริการ** ความรับผิดชอบของสถาบันการเงินและผู้ให้บริการภายนอก ภาระผูกพันในกรณีที่เกิดปัญหา

ในการให้บริการ เงื่อนไขหรือแนวทางในการเปลี่ยนแปลงหรือยกเลิกสัญญา รวมถึงสิทธิของสถาบันการเงิน ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก หรือธนาคารแห่งประเทศไทย ในการเรียกดูข้อมูลที่เกี่ยวข้องและการตรวจสอบการดำเนินงานและการควบคุมภายในของผู้ให้บริการภายนอก**ทั้งในกรณีที่ผู้ให้บริการภายนอกประกอบธุรกิจในประเทศและต่างประเทศ** นอกจากนี้ สถาบันการเงินต้องมีการเก็บ**สัญญาหรือข้อตกลงการให้บริการ**ไว้ที่สถาบันการเงินเพื่อให้พร้อมสำหรับการตรวจสอบของธนาคารแห่งประเทศไทย และเมื่อธนาคารแห่งประเทศไทยร้องขอ

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

(4) การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (security)

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

(4.2) สถาบันการเงินต้องจัดให้มีกระบวนการ ขั้นตอน หรือ ระบบในการติดตาม ประเมินผล และตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่า ผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานด้านการรักษาความปลอดภัยและความลับของระบบงานและข้อมูลที่ได้ตกลงไว้กับสถาบันการเงิน

(4.3) สถาบันการเงินต้องจัดให้มีกระบวนการ ขั้นตอน หรือ ระบบในการดำเนินการนำข้อมูลของผู้ใช้บริการของสถาบันการเงินและข้อมูลของสถาบันการเงินทั้งหมดกลับมาจากผู้ให้บริการภายนอก และสถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกมีกระบวนการ ขั้นตอน หรือ ระบบในการดำเนินการทำลายข้อมูลของผู้ใช้บริการของสถาบันการเงินและข้อมูลของสถาบันการเงินทั้งหมดเมื่อมีการสิ้นสุดหรือยกเลิกการใช้บริการจากผู้ให้บริการภายนอก

(5) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (integrity)

(5.1) สถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกมีแนวทางหรือมาตรฐานในการรักษาความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล ซึ่งครอบคลุมทั้งระบบประมวลผลข้อมูลที่อยู่ระหว่างการรับส่ง และระบบการจัดเก็บข้อมูล รวมทั้ง มีการดำเนินการให้งานเทคโนโลยีสารสนเทศที่ให้บริการสามารถทำงานได้อย่างมีประสิทธิภาพและถูกต้องเชื่อถือได้ โดยควรมีความสอดคล้องกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ให้บริการ และความเสี่ยงที่เกี่ยวเนื่อง

กับการให้บริการ ทั้งนี้ สถาบันการเงินอาจกำหนดให้ผู้ให้บริการภายนอกมีการประยุกต์ใช้แนวทางการควบคุมด้านงานเทคโนโลยีสารสนเทศที่ดี เป็นมาตรฐานสากล และได้รับการยอมรับโดยทั่วไป ตามความเหมาะสม

(5.2) สถาบันการเงินต้องจัดให้มีกระบวนการ ขั้นตอน หรือ ระบบในการติดตาม ประเมินผล และตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่า ผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานด้านความถูกต้องเชื่อถือได้ของระบบงานและข้อมูลที่ได้ตกลงไว้กับสถาบันการเงิน

(6) ความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (availability)

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

(6.2) สถาบันการเงินต้องจัดให้มีกระบวนการ ขั้นตอน หรือ ระบบในการติดตาม ประเมินผล และตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่า ผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานด้านความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ให้บริการที่ได้ตกลงไว้กับสถาบันการเงิน

(7) การคุ้มครองผู้ใช้บริการของสถาบันการเงิน (consumer protection)

(7.1) สถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกมีแนวทางหรือมาตรฐานในการดูแลและป้องกันข้อมูลสำคัญของผู้ใช้บริการของสถาบันการเงิน โดยควรสอดคล้องกับกฎหมาย ข้อบังคับที่เกี่ยวข้องของทางการ และมาตรฐานสากลที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศนั้น

(7.2) สถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกจะไม่นำข้อมูลของผู้ใช้บริการของสถาบันการเงินหรือข้อมูลของสถาบันการเงินไปเปิดเผยให้กับบุคคลอื่นใด โดยไม่ได้รับความยินยอมจากสถาบันการเงิน เว้นแต่กรณีที่เป็นไปตามกฎหมายหรือข้อบังคับของทางการที่เกี่ยวข้อง

(7.3) สถาบันการเงินต้องจัดให้มีกระบวนการ ขั้นตอน หรือ ระบบในการติดตาม ประเมินผล และตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่า ผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานด้านการคุ้มครองผู้ใช้บริการของสถาบันการเงินที่ได้ตกลงไว้กับสถาบันการเงิน

(7.4) สถาบันการเงินต้องจัดให้มีระบบการดูแลและจัดการเรื่องร้องเรียนให้แก่ผู้ใช้บริการของสถาบันการเงินอย่างเพียงพอและเหมาะสม และมีการรายงานการจัดการเรื่องร้องเรียนดังกล่าวให้คณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสม

5.5.2 หลักเกณฑ์การควบคุมเฉพาะสำหรับงานเทคโนโลยีสารสนเทศที่มีความสำคัญอย่างยิ่ง (specific control)

สถาบันการเงินที่มีการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน เช่น การใช้บริการระบบประมวลผลกลาง (core banking) ศูนย์คอมพิวเตอร์ (data center) และระบบเครือข่ายสื่อสาร (network) 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 ผู้ให้บริการภายนอกมีกระบวนการขั้นตอน การประเมิน และการควบคุมความเสี่ยง อย่างน้อยตามกรอบหลักการด้านเทคโนโลยีสารสนเทศที่สำคัญ 3 ประการ คือ การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (security) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (availability) ที่สอดคล้องตามหลักมาตรฐานสากลที่เกี่ยวข้อง ซึ่งอาจพิจารณาประยุกต์ให้เหมาะสมกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ให้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการให้บริการ เช่น

(1.1.1) กรณีการรักษาความปลอดภัยของระบบประมวลผลกลาง (core banking) ผู้ให้บริการภายนอกอาจพิจารณานำมาตรฐานของ International Organization for Standardization (ISO ซึ่งปัจจุบัน คือ ISO-27001) มาใช้เป็นแนวทางในการควบคุมความเสี่ยงอย่างเหมาะสม

(1.1.2) กรณีการประเมินและควบคุมความเสี่ยงของศูนย์คอมพิวเตอร์ (data center) ผู้ให้บริการภายนอกอาจพิจารณาประยุกต์ใช้มาตรฐานของ Telecommunications Industry Association (TIA ซึ่งปัจจุบัน คือ TIA-942) ตามระดับ (level) ที่เหมาะสม

(1.1.3) กรณีการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับ internet banking ผู้ให้บริการภายนอกอาจพิจารณานำมาตรฐาน ISO ที่เกี่ยวข้องหรือมาตรฐานสากลอื่นที่ดีมาใช้เป็นแนวทางในการรักษาความปลอดภัยอย่างเหมาะสม

(1.2) สถาบันการเงินต้องจัดให้มีกระบวนการ ขั้นตอน หรือ ระบบในการติดตาม ประเมินผล และตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่า ผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานสากลที่เกี่ยวข้องที่ได้ตกลงไว้กับสถาบันการเงิน และต้องจัดให้มีการทดสอบเพื่อให้มั่นใจว่า การใช้บริการจากบุคคลภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน จะไม่ก่อให้เกิดความเสี่ยงตามกรอบหลักการด้านเทคโนโลยีสารสนเทศที่สำคัญ 3 ประการ คือ การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (security)

ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (availability) จนนำมาสู่ช่องโหว่ที่ร้ายแรงต่อการทุจริต และ/หรือ ภัยคุกคามด้านเทคโนโลยีสารสนเทศทั้งจากภายในและภายนอก ซึ่งอาจส่งผลกระทบต่อธุรกิจอย่างร้ายแรง หรือก่อให้เกิดผลกระทบในวงกว้างต่อการให้บริการทางการเงินที่สำคัญของสถาบันการเงิน เช่น ต้องจัดให้มีการทดสอบแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ และมีการทดสอบระบบการรักษาความปลอดภัยเชิงลึก (penetration test) สำหรับการใช้บริการระบบ internet banking

(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) รวมถึง ปัญหาหรือเหตุการณ์ผิดปกติและเรื่องร้องเรียนที่เกิดขึ้นจากการใช้บริการ

5.6 แนวปฏิบัติสำหรับการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

ธนาคารแห่งประเทศไทยกำหนดแนวปฏิบัติสำหรับการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ ตามประเภทของการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ ดังนี้

5.6.1 การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน (Critical IT Outsourcing)

(1) ในกรณีที่เป็นการใช้บริการจากผู้ให้บริการภายนอกที่เป็นบริษัทในกลุ่มธุรกิจเดียวกัน ให้สถาบันการเงินสามารถดำเนินการได้โดยไม่ต้องแจ้งให้ธนาคารแห่งประเทศไทยทราบก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

(2) ในกรณีที่เป็นการใช้บริการจากผู้ให้บริการภายนอกที่ไม่เป็นบริษัทในกลุ่มธุรกิจเดียวกัน ให้สถาบันการเงินแจ้งให้ ฝ่ายกำกับสถาบันการเงิน สายกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทย ทราบล่วงหน้าอย่างน้อย 30 วัน ก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ โดยให้ระบุถึงเหตุผล รายละเอียดการใช้บริการ และผลการประเมินความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศดังกล่าว ที่ได้รับความเห็นชอบจากคณะกรรมการของสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมายแล้ว

5.6.2 การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น (Other IT Outsourcing) ให้สถาบันการเงินสามารถดำเนินการได้โดยไม่ต้องแจ้งให้ธนาคารแห่งประเทศไทยทราบก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

5.7 การรายงานและการตรวจสอบ

การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศของสถาบันการเงินอาจก่อให้เกิดผลกระทบต่อทั้งผู้ใช้บริการของสถาบันการเงิน สถาบันการเงิน ระบบการเงิน และธุรกิจอื่น ดังนั้น สถาบันการเงินต้องมีการกำกับดูแลผู้ให้บริการภายนอกอย่างใกล้ชิดและต้องดำเนินการให้ธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายนอก หรือหน่วยงานกำกับดูแลอื่น ได้รับทราบข้อมูลที่เกี่ยวข้องกับการใช้บริการและสามารถตรวจสอบผู้ให้บริการภายนอกดังกล่าวได้ ดังนี้

5.7.1 การรายงานต่อธนาคารแห่งประเทศไทย

(1) สถาบันการเงินต้องจัดทำรายงานการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศทุกประเภท ให้มีความถูกต้องและเป็นปัจจุบัน และส่งมายัง ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ สายกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทย เป็นประจำทุกปี ภายใน 30 วัน นับจากวันที่ 31 ธันวาคม และเมื่อธนาคารแห่งประเทศไทยร้องขอ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(1.1) ชื่องานเทคโนโลยีสารสนเทศและขอบเขตในการใช้บริการจากผู้ให้บริการภายนอก

(1.2) ชื่อผู้ให้บริการภายนอก

(1.3) วันที่เริ่มใช้บริการและวันที่สิ้นสุดสัญญาหรือข้อตกลงการให้บริการ

(1.4) ปัญหาและอุปสรรคจากการใช้บริการจากผู้ให้บริการภายนอก

(1.5) เอกสารการรับรองที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศที่ให้บริการ (certificate) ของผู้ให้บริการภายนอก ที่ตั้งของศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรองที่รองรับงานเทคโนโลยีสารสนเทศที่ผู้ให้บริการภายนอกให้บริการแก่สถาบันการเงิน ทั้งนี้ เฉพาะกรณีที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศที่สถาบันการเงินใช้บริการ

(2) สถาบันการเงินต้องจัดทำรายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดขึ้นจากการใช้บริการจากผู้ให้บริการภายนอกที่มีผลกระทบต่อการให้บริการของสถาบันการเงิน อันเป็นเหตุให้สถาบันการเงินไม่สามารถให้บริการการเงินพื้นฐานแก่ผู้ใช้บริการของสถาบันการเงินได้ในวงกว้าง พร้อมระบุแนวทางการแก้ไขปัญหาหรือเหตุการณ์ผิดปกติดังกล่าว และส่งมายัง ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ สายกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทย เพื่อทราบเมื่อมีการเกิดปัญหาหรือเหตุการณ์ผิดปกติขึ้นโดยเร็ว ทั้งนี้ ไม่ควรเกิน 24 ชั่วโมง

5.7.2 การตรวจสอบผู้ให้บริการภายนอกของสถาบันการเงิน

สถาบันการเงินต้องจัดให้มีการตรวจสอบผู้ให้บริการภายนอกอย่างสม่ำเสมอโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก และจัดทำรายงานผลการตรวจสอบผู้ให้บริการภายนอกดังกล่าวและเก็บไว้ที่สถาบันการเงิน พร้อมไว้สำหรับการตรวจสอบและเมื่อร้องขอโดยธนาคารแห่งประเทศไทย

ในกรณีที่สถาบันการเงินใช้บริการจากผู้ให้บริการภายนอกที่เป็นบริษัทในกลุ่มธุรกิจเดียวกันที่อยู่ในต่างประเทศ สถาบันการเงินสามารถใช้ผลการตรวจสอบของบริษัทแม่ที่ได้รับการรับรองจากผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกที่มีความเป็นอิสระ และรับทราบโดยคณะกรรมการของสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมายแล้วได้

5.7.3 การตรวจสอบโดยธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายนอก หรือหน่วยงานกำกับดูแลอื่น

สถาบันการเงินต้องดำเนินการให้ธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายนอก หรือหน่วยงานกำกับดูแลอื่น สามารถเรียกดูข้อมูลที่เกี่ยวข้องกับการให้บริการของผู้ให้บริการภายนอกและเข้าตรวจสอบผู้ให้บริการภายนอกดังกล่าวได้

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 โดยให้สถาบันการเงินที่มีความจำเป็นดังกล่าว หารือ พร้อมทั้งแสดงเหตุผลและความจำเป็นมาที่ ฝ่ายกำกับสถาบันการเงิน สายกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทย

5.9 บทเฉพาะกาล

5.9.1 สถาบันการเงินที่ได้แจ้งการใช้บริการจากผู้ให้บริการภายนอกที่ไม่เป็นบริษัทในกลุ่มธุรกิจเดียวกันด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงินต่อธนาคารแห่งประเทศไทยแล้วก่อนประกาศฉบับนี้มีผลใช้บังคับ ให้ดำเนินการต่อไปได้โดยไม่ต้องแจ้งธนาคารแห่งประเทศไทยอีก จนกว่าจะมีการเปลี่ยนแปลงการใช้บริการ หรือต่ออายุหรือจัดทำสัญญาหรือข้อตกลงการใช้บริการใหม่

5.9.2 สถาบันการเงินต้องถือปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้และเงื่อนไขที่ธนาคารแห่งประเทศไทยกำหนดเพิ่มเติมในกรณีที่สถาบันการเงินได้แจ้งการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศมายังธนาคารแห่งประเทศไทยแล้ว เท่าที่ไม่ขัดกับหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ ทั้งนี้

(1) สำหรับสัญญาหรือข้อตกลงการให้บริการเดิมที่ยังมีผลบังคับใช้อยู่ในวันที่ประกาศฉบับนี้มีผลบังคับใช้ ให้สถาบันการเงินดำเนินการปรับปรุงให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ภายในเวลา 1 ปี นับจากวันที่ประกาศฉบับนี้มีผลบังคับใช้

(2) สำหรับกรณีที่มีการต่ออายุสัญญาหรือข้อตกลงการใช้บริการ ซึ่งรวมถึงกรณีการต่ออายุอัตโนมัติ หรือมีการเปลี่ยนแปลงหรือแก้ไขสัญญาหรือข้อตกลงการใช้บริการ หรือมีการทำสัญญาหรือข้อตกลงการใช้บริการใหม่ ให้สถาบันการเงินปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ นับจากวันที่ประกาศฉบับนี้มีผลบังคับใช้

หากสถาบันการเงินใดไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้หรือเงื่อนไขที่ธนาคารแห่งประเทศไทยกำหนดเพิ่มเติมได้ภายในระยะเวลาที่กำหนด ให้สถาบันการเงินหารือ พร้อมทั้งแสดงเหตุผลและความจำเป็นมาที่ ฝ่ายกำกับสถาบันการเงิน สายกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทย เพื่อพิจารณาเป็นรายกรณี

6. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ 14 กรกฎาคม 2557

ประสาร ไตรรัตน์วรกุล

(นายประสาร ไตรรัตน์วรกุล)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

ฝ่ายนโยบายการกำกับสถาบันการเงิน
โทรศัพท์ 0 2283 6938, 0 2283 5839, 0 2283 6835
โทรสาร 0 2283 5938

คำถาม – คำตอบแนบท้ายประกาศ
เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing)
ในการประกอบธุรกิจของสถาบันการเงิน
ลงวันที่ 27 พฤศจิกายน 2557

ข้อ	ประเด็นคำถาม	แนวคำตอบ
ขอบเขตการบังคับใช้		
1.	สาขาต่างประเทศของธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทย (สาขาต่างประเทศฯ) ที่มีการใช้บริการจากผู้ให้บริการภายนอก ต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ด้วยหรือไม่	สาขาต่างประเทศฯ ต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ด้วย เนื่องจากสาขาต่างประเทศฯ ถือเป็นนิติบุคคลเดียวกันกับธนาคารพาณิชย์ที่เป็นสำนักงานใหญ่ในประเทศไทย
2.	บริษัทลูกของธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทยจะต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ด้วยหรือไม่	บริษัทลูกของธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทยที่อยู่ในกลุ่ม Solo Consolidation ต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ด้วย
คำจำกัดความ		
3.	การใช้บริการบุคคลภายนอกในเรื่องต่อไปนี้เข้าข่ายเป็นการใช้บริการ IT Outsourcing หรือไม่ และจะมีแนวทางในการพิจารณาว่าเข้าข่ายเป็นการใช้บริการ IT Outsourcing อย่างไร • การจัดซื้อและติดตั้งโปรแกรม (software) สำเร็จรูป เช่น Microsoft Windows หรือ Microsoft Office • การจัดซื้อและติดตั้งอุปกรณ์คอมพิวเตอร์ (hardware) • การจ้างที่ปรึกษาด้านเทคโนโลยีสารสนเทศหรือการจ้างทีมงานเพื่อพัฒนา software หรือ application • การบำรุงรักษาต่อเนื่องตามโปรแกรมการดูแลของผู้ให้บริการภายนอกสำหรับ hardware และ software • การส่งข้อมูลไปยังบริษัทแม่ เพื่อปฏิบัติตามข้อกำหนดของหลักเกณฑ์ในต่างประเทศ เช่น FATCA • การใช้บริการ IT Outsourcing เพื่อเป็นแผนฉุกเฉินของสถาบันการเงิน	การพิจารณาว่า การใช้บริการงาน IT ใดเข้าข่ายเป็น IT Outsourcing ให้พิจารณาว่า งาน IT ที่ใช้บริการจากบุคคลภายนอกนั้น เป็นงาน IT ที่โดยปกติแล้วสถาบันการเงินต้องดำเนินการเอง ซึ่งรวมถึง การพัฒนา software หรือ application และการเตรียมการด้าน IT ตามแผนฉุกเฉินของสถาบันการเงิน แต่ไม่รวมถึงการจัดซื้อ ติดตั้ง และบำรุงรักษาโปรแกรมสำเร็จรูปในการทำงานพื้นฐาน เช่น โปรแกรมการทำงานเอกสาร (ได้แก่ MS Office หรือ SPSS เป็นต้น) โปรแกรมป้องกันไวรัส (ได้แก่ Norton antivirus หรือ McAfee antivirus เป็นต้น) และอุปกรณ์คอมพิวเตอร์ (ได้แก่ เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่อง printer เป็นต้น) การใช้บริการที่เชื่อมต่อไปยังระบบกลาง เช่น ระบบการชำระเงิน (ได้แก่ VISA, MASTER, NITMX หรือ PCC เป็นต้น) การใช้บริการที่เชื่อมมายังระบบของทางการ (ได้แก่ NCB หรือ DMS เป็นต้น) และการส่งข้อมูลไปยังบริษัทแม่เพื่อปฏิบัติตามหลักเกณฑ์ในต่างประเทศ
4	ในกรณีที่สถาบันการเงินมีการเช่าพื้นที่เพื่อใช้เป็นศูนย์คอมพิวเตอร์ (data center) โดยผู้ให้เช่าทำหน้าที่ในการบริหารจัดการระบบสาธารณูปโภคต่าง ๆ ภายในศูนย์คอมพิวเตอร์ (facility) ด้วย เช่น ระบบไฟฟ้า ระบบทำความเย็นและควบคุมความชื้น ระบบป้องกันและระงับอัคคีภัย	การเช่าพื้นที่เพื่อใช้เป็นศูนย์คอมพิวเตอร์ โดยผู้ให้เช่าทำหน้าที่บริหารจัดการระบบสาธารณูปโภคด้วย เข้าข่ายเป็นการใช้บริการ IT Outsourcing เนื่องจากการบริหารจัดการระบบสาธารณูปโภคซึ่งเป็นโครงสร้างพื้นฐานที่มีความสำคัญภายในศูนย์คอมพิวเตอร์ถือเป็นปัจจัยหลักที่มีผลต่อการดำเนินการอย่างต่อเนื่องของศูนย์คอมพิวเตอร์นั้น

ข้อ	ประเด็นคำถาม	แนวคำตอบ
	เพื่อให้อยู่ในสภาพที่พร้อมใช้งานอย่างต่อเนื่อง เข้าข่ายเป็นการใช้บริการ IT Outsourcing หรือไม่	ทั้งนี้ สถาบันการเงินต้องพิจารณาว่า การใช้บริการดังกล่าวเข้าข่ายเป็น Critical IT Outsourcing หรือ Other IT Outsourcing โดยพิจารณาตามความเสี่ยง ผลกระทบ และความเสียหายที่อาจเกิดขึ้นจากการใช้บริการดังกล่าว
การอนุญาตให้สถาบันการเงินใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ		
5.	สถาบันการเงินต้องทำการประเมินตนเอง (self assessment) ตามหลักเกณฑ์การใช้บริการ IT Outsourcing เมื่อใด	สถาบันการเงินต้องประเมินตนเองตั้งแต่ก่อนเริ่มใช้บริการ IT Outsourcing เพื่อให้ทราบถึงความเสี่ยงจากการใช้บริการ และสามารถกำหนดแนวทางในการควบคุมและจัดการความเสี่ยงนั้นได้ และใช้ผลการประเมินดังกล่าวมาประเมินประสิทธิภาพในการให้บริการของผู้ให้บริการภายนอกได้ ทั้งนี้ การประเมินความเสี่ยงควรสอดคล้องกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงาน IT ที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ
การแบ่งประเภทการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ		
6.	แนวทางในการพิจารณาการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อสถาบันการเงิน (Critical IT Outsourcing) ควรเป็นอย่างไร	สถาบันการเงินต้องพิจารณาว่า หากงาน IT ที่ใช้บริการมีความเสี่ยงและผลกระทบในวงกว้างทั้งต่อสถาบันการเงิน ระบบสถาบันการเงิน หรือธุรกิจอื่น หรืออาจก่อให้เกิดความเสียหายหรือเหตุการณ์อื่น ๆ 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 อาจก่อให้เกิดความเสี่ยงและผลกระทบในวงกว้างทั้งต่อสถาบันการเงิน ระบบสถาบันการเงิน หรือธุรกิจอื่น หรืออาจก่อให้เกิดความเสียหายหรือเหตุการณ์ฉุกเฉินอื่น ๆ แต่ไม่รวมถึงการใช้บริการระบบเครือข่ายสื่อสารที่สถาบันการเงินไม่สามารถดำเนินการได้เอง เช่น การใช้บริการระบบเครือข่าย Internet หรือการเช่าสายสื่อสาร fiber optic
หลักเกณฑ์การควบคุมทั่วไป: นโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ		
8.	คณะกรรมการสถาบันการเงินมีหน้าที่อนุมัตินโยบายการใช้บริการ IT Outsourcing แล้วยังต้องอนุมัติการใช้บริการ Critical IT Outsourcing กับบริษัทนอกกลุ่มธุรกิจเดียวกัน ก่อนการใช้บริการด้วยอีกหรือไม่	คณะกรรมการสถาบันการเงินมีหน้าที่ให้ความเห็นชอบนโยบายการใช้บริการ IT Outsourcing ซึ่งเป็นนโยบายในภาพรวมของการใช้บริการ และการใช้บริการ Critical IT Outsourcing ด้วย แต่สามารถมอบหมายการใช้บริการ Critical IT Outsourcing ให้คณะกรรมการชุดอื่นให้ความเห็นชอบแทนได้

ข้อ	ประเด็นคำถาม	แนวคำตอบ
9.	ในกรณีสาขาของธนาคารพาณิชย์ต่างประเทศขอเสนอให้สำนักงานใหญ่หรือสำนักงานภูมิภาคของสาขาของธนาคารพาณิชย์ต่างประเทศเป็นผู้อนุมัตินโยบายการใช้บริการ IT Outsourcing เพื่อเพิ่มความคล่องตัวในการดำเนินงาน ได้หรือไม่	สาขาของธนาคารพาณิชย์ต่างประเทศสามารถให้สำนักงานใหญ่หรือสำนักงานภูมิภาคเป็นผู้อนุมัตินโยบายการใช้บริการ IT Outsourcing ได้ แต่คณะผู้บริหารที่มีหน้าที่รับผิดชอบที่เกี่ยวข้องที่อยู่ในประเทศไทย ต้องให้ความเห็นชอบต่อนโยบายดังกล่าวด้วย
10.	การกำหนดให้นโยบายการใช้บริการ IT Outsourcing ต้องสอดคล้องกับกลยุทธ์ทางธุรกิจ หมายถึง ต้องให้สถาบันการเงินกำหนดนโยบายเป็นรายปีว่าในปีนั้นจะมีการใช้บริการ IT Outsourcing อะไรบ้างใช่หรือไม่ และในกรณีที่มีการทบทวนนโยบายการใช้บริการประจำปีแล้ว แต่ไม่มีการแก้ไขปรับปรุง จำเป็นต้องรายงานผลการทบทวนให้คณะกรรมการของสถาบันการเงินทราบหรือไม่	สถาบันการเงินควรกำหนดนโยบายการใช้บริการ IT Outsourcing ให้สอดคล้องกับกลยุทธ์และการแข่งขันทางธุรกิจที่มีการเปลี่ยนแปลง โดยควรทบทวนนโยบายการใช้บริการ IT Outsourcing ดังกล่าวอย่างน้อยปีละครั้ง และต้องรายงานผลการทบทวนให้คณะกรรมการของสถาบันการเงินทราบแม้จะไม่มีการแก้ไข
หลักเกณฑ์การควบคุมเฉพาะสำหรับงานเทคโนโลยีสารสนเทศที่มีความสำคัญอย่างยิ่ง		
11.	การกำกับดูแลเพิ่มเติม (specific risk control) ตามหลักเกณฑ์ข้อ 5.5.2 (1) ที่ว่า สถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกมีกระบวนการ ขั้นตอน การประเมิน และการควบคุมความเสี่ยงอย่างน้อยตามกรอบหลักการด้าน IT ที่สอดคล้องกับมาตรฐานสากลนั้น หมายถึง ผู้ให้บริการภายนอกต้องมีเอกสารการรับรองความเป็นมาตรฐานสากลด้านงาน IT ด้วยใช่หรือไม่ และควรมีมาตรฐานในระดับใด และหากสาขาของธนาคารพาณิชย์ต่างประเทศ ใช้บริการระบบประมวลผลกลาง (core banking) จากบริษัทแม่ สาขาของธนาคารพาณิชย์ต่างประเทศ ต้องตรวจสอบว่า 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 โดยพิจารณาจากขนาด ปริมาณธุรกรรม ความซับซ้อนของงาน IT ที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ ทั้งนี้ ในกรณีที่บริษัทแม่ไม่มี certificate สาขาของธนาคารพาณิชย์ต่างประเทศสามารถใช้ผลการตรวจสอบที่ได้รับการรับรองจากผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกของบริษัทแม่ได้
12.	กระบวนการ ขั้นตอน หรือระบบในการติดตาม ประเมินผล และตรวจสอบผู้ให้บริการภายนอก เช่น การทดสอบระบบการรักษาความปลอดภัยเชิงลึก (penetration test) สำหรับการใช้บริการระบบ Internet banking ตามที่กำหนดในข้อ 5.2 (1.2) นั้น ควรมีความถี่เท่าใด	สถาบันการเงินควรจัดให้ผู้ให้บริการภายนอกมีการทดสอบระบบการรักษาความปลอดภัยเชิงลึก (penetration test) อย่างน้อยปีละครั้ง และ/หรือ ทุกครั้งที่มีการเปลี่ยนแปลงค่าความปลอดภัยหรือมีการเปลี่ยนแปลงความเสี่ยงด้าน IT ที่มีนัยสำคัญที่อาจเปิดช่องโหว่ให้เกิดภัยคุกคามจากภายในและภายนอกได้

ข้อ	ประเด็นคำถาม	แนวคำตอบ
แนวปฏิบัติสำหรับการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ		
13.	ในกรณีที่ผู้ให้บริการภายนอกมีการจ้างผู้ให้บริการภายนอกรายอื่นรับช่วงจัดการงาน IT ที่รับให้บริการต่อ (sub-contract) โดยงานดังกล่าวนั้นเป็นงาน Critical IT Outsourcing สถาบันการเงินจะต้องปฏิบัติอย่างไร	ในกรณีที่ผู้ให้บริการภายนอกมีการ sub-contract งาน IT ที่รับให้บริการบางส่วนหรือทั้งหมดต่อให้กับผู้ให้บริการภายนอกรายอื่น สถาบันการเงินไม่ต้องแจ้งการ subcontract ดังกล่าวมายังธนาคารแห่งประเทศไทย แต่สถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกจะรับผิดชอบต่อการให้บริการด้านงาน IT แก่สถาบันการเงินเสมือนกับที่ผู้ให้บริการภายนอกเป็นผู้ให้บริการด้วยตนเอง และการ subcontract นั้นจะต้องไม่มีเจตนาหลีกเลี่ยงการปฏิบัติตามหลักเกณฑ์ IT Outsourcing
การรายงานต่อธนาคารแห่งประเทศไทย		
14.	ตามที่ธนาคารแห่งประเทศไทยกำหนดให้ต้องมีการจัดทำรายงานการใช้บริการ IT Outsourcing ซึ่งมีเนื้อหาครอบคลุมวันที่เริ่มใช้บริการและวันที่สิ้นสุดสัญญาหรือข้อตกลงการให้บริการนั้น เนื่องจากสาขาของธนาคารพาณิชย์ต่างประเทศเป็นผู้รับนโยบายการใช้บริการ IT Outsourcing จากบริษัทแม่ในต่างประเทศ ซึ่งสัญญาที่เกี่ยวข้องกับการใช้บริการ IT Outsourcing ส่วนใหญ่จะดำเนินการและจัดทำโดยบริษัทแม่ โดยไม่ได้กำหนดวันสิ้นสุดสัญญาไว้ และสัญญาบางฉบับอาจถูกจัดทำไว้เป็นเวลานาน สาขาของธนาคารพาณิชย์ต่างประเทศควรดำเนินการอย่างไรหากไม่สามารถจัดหาข้อมูลวันที่เริ่มใช้บริการและวันที่สิ้นสุดสัญญาได้	ตามหลักการบริหารความเสี่ยงที่ดี สถาบันการเงินควรเก็บสัญญาหรือข้อตกลงการให้บริการที่ยังมีผลบังคับใช้อยู่ไว้เพื่อเป็นเอกสารหลักฐานประกอบการดำเนินการต่าง ๆ ที่เกี่ยวข้อง ซึ่งในสัญญาหรือข้อตกลงการให้บริการโดยทั่วไปควรระบุวันเริ่มต้นและวันสิ้นสุดการให้บริการไว้ แต่หากสัญญาหรือข้อตกลงการให้บริการมีการกำหนดวันสิ้นสุดสัญญาเป็นเงื่อนไข เช่น สิ้นสุดเมื่อได้รับการบอกเลิกสัญญา ก็ให้สถาบันการเงินรายงานเงื่อนไขของการสิ้นสุดสัญญานั้นในส่วนของวันที่สิ้นสุดสัญญา ทั้งนี้ หากสัญญาหรือข้อตกลงการให้บริการถูกดำเนินการหรือจัดทำโดยบริษัทแม่ สาขาของธนาคารพาณิชย์ต่างประเทศควรขอข้อมูลดังกล่าวจากบริษัทแม่
15.	ในการรายงานการใช้บริการ IT Outsourcing ต่อธนาคารแห่งประเทศไทยเป็นประจำทุกปีตามข้อ 5.7.1 (1) นั้น สถาบันการเงินสามารถจัดกลุ่มการรายงานโดยแยกตามประเภทการใช้บริการและรวมระบบงานที่ใช้บริการลักษณะเดียวกันไว้ในหมวดหมู่เดียวกัน เพื่อการรายงาน ได้หรือไม่	สถาบันการเงินสามารถพิจารณาจัดกลุ่มหรือกำหนดรูปแบบการรายงานตามความเหมาะสม แต่ต้องครอบคลุมการใช้บริการ IT Outsourcing ในทุกระบบงานและมีเนื้อหาอย่างน้อยตามที่กำหนดไว้ในประกาศ
16.	ในการกำหนดให้สถาบันการเงินต้องจัดทำรายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดขึ้นจากการใช้บริการ IT Outsourcing ที่มีผลกระทบต่อการให้บริการของสถาบันการเงิน ตามข้อ 5.7.1 (2) นั้น ปัญหาหรือเหตุการณ์ผิดปกติดังกล่าว หมายถึงปัญหาหรือเหตุการณ์ผิดปกติที่เกิดขึ้นจากการใช้บริการ Critical IT Outsourcing เท่านั้น ใช่หรือไม่	สถาบันการเงินต้องจัดทำและรายงานปัญหาหรือเหตุการณ์ผิดปกติขึ้นโดยเร็ว ซึ่งไม่ควรเกิน 24 ชั่วโมง ทั้งกรณีการใช้บริการ Critical IT Outsourcing และ Other IT Outsourcing หากปัญหาหรือเหตุการณ์ผิดปกตินั้น มีผลกระทบต่อการให้บริการการเงินพื้นฐานในวงกว้าง เช่น ธุรกรรมการฝากเงิน การถอนเงิน และการโอนเงิน ตัวอย่างปัญหาหรือเหตุการณ์ผิดปกติดังกล่าว เช่น • ระบบไฟฟ้าภายในศูนย์คอมพิวเตอร์ (data center) มีปัญหาทำให้เครื่องประมวลผลสำคัญหยุดชะงัก • ระบบประมวลผลกลาง (core banking) มีปัญหา

ข้อ	ประเด็นคำถาม	แนวคำตอบ
		ทำให้ไม่สามารถประมวลผลรายการสำคัญได้ • ระบบเครือข่าย (network) มีปัญหา ทำให้ไม่สามารถเชื่อมโยงระบบต่าง ๆ เช่น ระบบช่องทางสาขา หรือระบบ ATM เพื่อให้บริการแก่ประชาชนได้ ทั้งนี้ สถาบันการเงินสามารถกำหนดรูปแบบรายงานได้ตามความเหมาะสม โดยอย่างน้อยควรระบุถึงลักษณะของปัญหาหรือเหตุการณ์ผิดปกติ และแนวทางการแก้ไขปัญหาหรือเหตุการณ์ผิดปกติดังกล่าว
การตรวจสอบผู้ให้บริการภายนอกของสถาบันการเงิน		
17.	ในการกำหนดให้สถาบันการเงินต้องจัดให้มีการตรวจสอบผู้ให้บริการภายนอกอย่างสม่ำเสมอตามข้อ 5.7.2 นั้น ความถี่ในการตรวจสอบควรเป็นเท่าใด และการตรวจสอบผู้ให้บริการภายนอกทุกการใช้บริการ IT Outsourcing อาจเป็นภาระมากเกินไป สถาบันการเงินสามารถตรวจสอบผู้ให้บริการภายนอกเฉพาะ Critical IT Outsourcing โดยใช้แบบสอบถามหรือให้ผู้ตรวจสอบที่เป็นอิสระตรวจสอบแทน ได้หรือไม่	สถาบันการเงินสามารถกำหนดความถี่ในการตรวจสอบผู้ให้บริการภายนอกจากได้ตามความเหมาะสม โดยพิจารณาตามความสำคัญของงาน IT ที่ใช้บริการ เช่น อาจกำหนดความถี่ในการตรวจสอบ Critical IT Outsourcing มากกว่าความถี่ในการตรวจสอบ Other IT Outsourcing ทั้งนี้ ธปท. ไม่ได้จำกัดรูปแบบและวิธีการในการตรวจสอบ แต่ต้องทำให้สถาบันการเงินได้รับทราบข้อมูลที่แสดงถึงความสามารถของผู้ให้บริการภายนอกในการปฏิบัติตามนโยบายและเงื่อนไขที่กำหนดได้ โดยเฉพาะในด้านการรักษาความปลอดภัยและความลับของข้อมูล (security) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (availability)
ประเด็นอื่น ๆ		
18.	ประกาศการใช้บริการ IT Outsourcing เกี่ยวข้องกับแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT best practice) อย่างไร	ประกาศฉบับนี้เป็นการกำหนดหลักเกณฑ์ให้สถาบันการเงินที่มีการใช้บริการ IT Outsourcing ถือปฏิบัติ ในขณะที่ IT best practice เป็นแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงด้าน Operational / IT risk management ซึ่งสถาบันการเงินสามารถนำ IT best practice มาประยุกต์ใช้ให้เหมาะสมกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงาน IT ที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการได้
19.	สถาบันการเงินสามารถกำหนดระดับความเสี่ยงและหลักเกณฑ์การประเมินความเสี่ยงในการใช้บริการ IT Outsourcing ตามกรอบการบริหารความเสี่ยงของสถาบันการเงินเองได้ ใช่หรือไม่	สถาบันการเงินสามารถพิจารณาปฏิบัติตามหลักเกณฑ์การควบคุมความเสี่ยงต่าง ๆ ให้สอดคล้องกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงาน IT ที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการได้

ฝ่ายนโยบายการกำกับสถาบันการเงิน
โทร. 0-2283-6938, 0-2283-5839, 0-2283-6835