บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด

นโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ
(IT Outsourcing Policy)
บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด

---

1. หลักการและเหตุผล

บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด (บริษัท) เป็นรัฐวิสาหกิจสังกัดกระทรวงการคลัง มีการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ ซึ่งระบบเทคโนโลยีสารสนเทศมีความสำคัญในการสนับสนุนการให้บริการระบบงานทางด้านการเงินของบริษัท และระบบงานบางอย่างจะต้องมีการว่าจ้างการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ โดยยังคงต้องรับผิดชอบต่อการให้บริการอย่างต่อเนื่องแก่ผู้ใช้งานของบริษัท ต้องคงความน่าเชื่อถือของการให้บริการเช่นเดียวกับที่บริษัท เป็นผู้ดำเนินการด้านเทคโนโลยีสารสนเทศด้วยตนเอง และต้องคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นต่อบริษัท ในรูปแบบที่เปลี่ยนแปลงไปจากการดำเนินงานปกติที่ดำเนินโดยบริษัท ดังนั้น บริษัทจึงจัดทำนโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing Policy) เพื่อเป็นแนวทางในการควบคุมผู้ให้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก

ทั้งนี้ หลักการและเหตุผลในการออกนโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing Policy) ให้เป็นไปตามประกาศของธนาคารแห่งประเทศไทย เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน

2. วัตถุประสงค์

2.1 เพื่อให้บริษัทมีนโยบาย หลักเกณฑ์ และกระบวนการในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ที่เหมาะสม มีประสิทธิภาพ น่าเชื่อถือ และเป็นมาตรฐาน

2.2 เพื่อกำหนดแนวทางในการว่าจ้างบุคคลธรรมดาหรือนิติบุคคลผู้ให้บริการภายนอกเข้ามาให้บริการงานด้านเทคโนโลยีสารสนเทศ โดยให้สอดคล้องกับหลักเกณฑ์ที่เกี่ยวข้องกับประกาศ เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ของบริษัท

2.3 เพื่อเสริมสร้างความมั่นใจให้กับบริษัทในด้านความสามารถในการให้บริการลูกค้า รวมทั้งการรักษาความลับของข้อมูลและระบบเทคโนโลยีสารสนเทศ

เลขที่ 33/4 อาคารเดอะไนน์ ทาวเวอร์ส แกรนด์ พระรามเก้า ชั้น 18 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์ 02-055-5999

2.4 เพื่อเสริมสร้างความมั่นใจให้กับผู้บริหารของบริษัท ด้านความสามารถในการให้บริการและแนวทางในการควบคุมการดำเนินโครงการของผู้ให้บริการด้านงานเทคโนโลยีสารสนเทศ ได้ครบถ้วนตามความต้องการและตามระยะเวลาที่บริษัทกำหนด

2.5 เพื่อส่งเสริมให้เกิดประสิทธิภาพในการดำเนินงานและการบริหารต้นทุน และเพิ่มศักยภาพในการพัฒนาการให้บริการทางการเงินให้ทันต่อเทคโนโลยีที่มีการเปลี่ยนแปลงอย่างรวดเร็ว

3. ขอบเขตของนโยบายและการบังคับใช้

3.1 งานเทคโนโลยีสารสนเทศที่ใช้บริการจากบุคคลภายนอกนั้นเป็นงานเทคโนโลยีสารสนเทศที่โดยปกติแล้วบริษัทต้องดำเนินการเอง แต่ไม่สามารถดำเนินการได้ในขณะนั้น

3.2 การใช้บริการ Cloud Computing ซึ่งมีความเกี่ยวข้องกับการจัดสรรทรัพยากรด้านงานเทคโนโลยีสารสนเทศเพื่อการจัดเก็บข้อมูล การประมวลผลหรือการดำเนินการใด ๆ เกี่ยวกับข้อมูลของบริษัทตามลักษณะการใช้บริการ

ทั้งนี้ กำหนดให้ทุกหน่วยงานซึ่งเป็นผู้ขอใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศต้องปฏิบัติตามนโยบายฉบับนี้ รวมทั้งนโยบาย ข้อบังคับ และระเบียบอื่น ๆ ที่เกี่ยวข้องของบริษัทและหน่วยงานที่กำกับดูแลอย่างเคร่งครัด

4. คำนิยาม

“บริษัท” หมายความว่า บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด

“ผู้จัดการบริษัท” หมายความว่า ผู้จัดการบริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด และในกรณีที่ผู้จัดการบริษัทเป็นกรรมการบริษัทด้วย ให้เรียกว่า “กรรมการผู้จัดการบริษัท”

“พนักงานระดับบริหาร” หมายความว่า พนักงานที่ดำรงตำแหน่งรองผู้จัดการบริษัท ผู้ช่วยผู้จัดการบริษัท และผู้จัดการฝ่าย ตามลำดับชั้น

“พนักงาน” หมายความว่า ผู้ซึ่งบริษัทได้จ้างไว้ให้ปฏิบัติงานในลักษณะประจำ และรับเงินเดือนตามระดับตำแหน่งที่กำหนด ทั้งนี้ ไม่รวมถึงผู้จัดการบริษัท

“หน่วยงานเทคโนโลยีสารสนเทศ” หมายความว่า ฝ่ายงาน สำนัก ส่วนงาน หรือหน่วยงานเรียกชื่ออื่นใด ตามประกาศโครงสร้างองค์กรของบริษัทที่เกี่ยวข้องกับงานทางด้านเทคโนโลยีสารสนเทศ

“ข้อมูล” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริงข้อมูลหรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะจัดทำไว้ในรูปแบบของเอกสาร แฟ้มรายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใด ที่ทำให้สิ่งที่บันทึกไว้ปรากฏเป็นทรัพย์สินชนิดหนึ่งที่มีมูลค่า และมีความสำคัญสำหรับบริษัท

"การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing)" หมายความว่า การใช้บริการจากผู้ให้บริการภายนอก (Service Provider) ในการดำเนินการด้านงานเทคโนโลยีสารสนเทศให้แก่บริษัท ซึ่งโดยปกติแล้วบริษัทต้องดำเนินการเอง

"ระบบเทคโนโลยีสารสนเทศ" หมายความว่า ข้อมูลของบริษัทที่พร้อมสำหรับการใช้งาน หรือได้รับการรวบรวมไว้สำหรับใช้งาน ได้แก่ แบบฟอร์มและเอกสารสายงานสารสนเทศ ฐานข้อมูลโปรแกรมประยุกต์ต่าง ๆ เป็นต้น

"งานเทคโนโลยีสารสนเทศ" หมายความว่า งานด้านเทคโนโลยีสารสนเทศ (Information Technology - IT) ที่ครอบคลุมถึงระบบงาน (Application) ข้อมูล (Information) โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (Infrastructure) บุคลากรและกระบวนการที่จัดการด้านเทคโนโลยีสารสนเทศ (People and Process)

"ผู้ให้บริการภายนอก" (Service Provider) หมายความว่า บุคคลภายนอกทั้งในและต่างประเทศซึ่งเข้าทำสัญญาหรือทำข้อตกลงในการให้บริการงานให้กับบริษัท อันมีลักษณะที่โดยปกติแล้วบริษัทต้องดำเนินการเอง

"หน่วยงาน" หมายความว่า ฝ่ายงาน สำนัก ส่วนงาน หรือหน่วยงานเรียกชื่ออื่นใด ตามประกาศโครงสร้างองค์กรของบริษัท

"การใช้บริการ Cloud Computing" หมายความว่า การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศในงานด้านโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศหรือระบบงานด้านเทคโนโลยีสารสนเทศ ที่มีการนำเทคโนโลยี Cloud Computing มาใช้ในการให้บริการผ่านเครือข่ายอินเตอร์เน็ต เพื่อประโยชน์ในการจัดเก็บข้อมูล การประมวลผล หรือการดำเนินการใด ๆ เกี่ยวกับข้อมูลหรือระบบงานให้แก่บริษัท ซึ่งการใช้บริการดังกล่าวสามารถปรับเปลี่ยนได้ตามความต้องการของผู้ใช้บริการ

5. เนื้อหา

5.1 หลักการสำคัญการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

หลักการสำคัญของการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศที่ต้องคำนึงถึง คือ

5.1.1 บริษัทต้องรับผิดชอบต่อการให้บริการอย่างต่อเนื่องแก่ผู้ใช้บริการของบริษัท ต้องคงความน่าเชื่อถือของการให้บริการเช่นเดียวกับที่บริษัทพึงจะมีเสมือนกับที่บริษัทเป็นผู้ดำเนินการด้านเทคโนโลยีสารสนเทศด้วยตนเอง และต้องคำนึงถึงความเสี่ยงที่อาจเกิดต่อบริษัทในรูปแบบที่เปลี่ยนแปลงไปจากการดำเนินงานปกติที่กระทำโดยบริษัทเอง

ในกรณีที่ผู้ให้บริการภายนอกมีการให้ผู้ให้บริการภายนอกรายอื่นรับช่วงต่อ (Sub Contract) เพื่อจัดการงานด้านเทคโนโลยีสารสนเทศที่ให้บริการแก่บริษัท ต้องมั่นใจว่าผู้ให้บริการ

ภายนอกจะรับผิดชอบต่อการให้บริการด้านงานเทคโนโลยีสารสนเทศแก่บริษัทเสมือนกับที่ผู้ให้บริการภายนอกเป็นผู้ให้บริการด้วยตนเอง

5.1.2 บริษัทกำหนดให้มีแนวทางบริหารความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศที่สอดคล้องกับความเสี่ยงที่อาจเกิดขึ้น ภายใต้กรอบหลักการด้านเทคโนโลยีสารสนเทศที่สำคัญ 3 ประการ คือ การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (Security) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (Integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (Availability)

5.1.3 บริษัทต้องมีการกำกับดูแลความเสี่ยง โดยหน่วยงานที่มีความประสงค์ใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศต้องมีการประเมินตนเอง (Self Assessment) ควบคุมและจัดการความเสี่ยงอย่างมีประสิทธิภาพ ภายใต้การกำกับดูแลของคณะอนุกรรมการที่ได้รับมอบหมายหรือพนักงานระดับบริหารที่ได้รับมอบหมาย

5.2 ประเภทการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

5.2.1 การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อบริษัท (Critical IT Outsourcing)

การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อบริษัท หมายความว่า การใช้บริการในงานเทคโนโลยีสารสนเทศที่อาจก่อให้เกิด

(1) ความเสี่ยงและผลกระทบต่อบริษัทในวงกว้าง (Bank Wide Impact) เช่น การหยุดชะงักของการให้บริการแก่ผู้ใช้บริการของบริษัท และประชาชนทั่วไปในวงกว้าง หรือ

(2) ความเสี่ยงและผลกระทบต่อระบบงานบริษัท หรือธุรกิจอื่นในวงกว้าง (Banking System Wide Impact) เช่น การหยุดชะงักของระบบงานที่เชื่อมต่อกับระบบชำระเงิน เป็นต้น

ทั้งนี้ ตัวอย่างการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อบริษัท เช่น การใช้บริการระบบประมวลผลกลาง (Core Banking System) ศูนย์คอมพิวเตอร์ (Data Center) และระบบเครือข่ายสื่อสาร (Network System) เป็นต้น

5.2.2 การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น (Other IT Outsourcing)

การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น หมายความว่า การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศที่ไม่เข้าข่ายเป็นการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อบริษัท ตามข้อ 5.2.1

5.3 แนวทางการกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

บริษัทได้กำหนดแนวทางการกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศตามประเภทของการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศตามข้อ 5.2 ดังนี้

5.3.1 กรณีใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อบริษัท (Critical IT Outsourcing) ต้องปฏิบัติตามทั้งหลักเกณฑ์การควบคุมทั่วไป (General Control) และหลักเกณฑ์การควบคุมเฉพาะสำหรับงานเทคโนโลยีสารสนเทศที่มีความสำคัญอย่างยิ่ง (Specific Control) โดยให้พิจารณาตามความเหมาะสมกับขนาดองค์กร ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการและความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ

5.3.2 กรณีใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทอื่น (Other IT Outsourcing) ต้องปฏิบัติตามหลักเกณฑ์การควบคุมทั่วไป (General Control) โดยให้พิจารณาตามความเหมาะสมกับขนาดองค์กร ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการและความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ

5.4 หลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศต้องปฏิบัติตามกฎหมาย ข้อบังคับของทางการ หรือมาตรฐานสากลที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศที่ใช้บริการ รวมถึงหลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศและระเบียบข้อบังคับของบริษัท ดังนี้

5.4.1 หลักเกณฑ์การควบคุมทั่วไป (General Control)

การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศทั้งสองประเภทตามข้อ 5.2 ต้องให้ความสำคัญในเรื่องการปฏิบัติตามนโยบาย การบริหารความเสี่ยง การบริหารจัดการผู้ให้บริการภายนอก (Service Provider Management) การรักษาความปลอดภัยและความลับของระบบงาน และข้อมูล (Security) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (Integrity) ความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (Availability) และการคุ้มครองผู้ใช้บริการของบริษัท (Consumer protection) โดยให้พิจารณาตามความเหมาะสมกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ ดังนี้

(1) นโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศและการใช้บริการ Cloud Computing

(1.1) ต้องกำหนดกลยุทธ์ที่ชัดเจนสำหรับการตัดสินใจใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ เช่น เหตุผลความจำเป็นทางธุรกิจ รวมถึงประโยชน์และต้นทุน ทั้งนี้ บริษัทต้องมั่นใจว่าการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศนั้น ไม่ขัดต่อ

กฎหมายและข้อบังคับของทางการของประเทศไทยและประเทศของผู้ให้บริการภายนอก ในกรณีที่ผู้ให้บริการภายนอกประกอบธุรกิจในต่างประเทศ รวมถึงระเบียบ ข้อบังคับของบริษัท เพื่อไม่ก่อให้เกิดช่องโหว่ที่นำไปสู่การเกิดการทุจริตที่ร้ายแรงหรือก่อให้เกิดภัยคุกคามด้านเทคโนโลยีสารสนเทศ ทั้งจากภายในและภายนอกจนอาจส่งผลกระทบต่อธุรกิจอย่างร้ายแรง และไม่ส่งผลกระทบต่อเสถียรภาพของระบบสถาบันการเงิน และระบบการเงินของประเทศไทยอย่างร้ายแรง

(1.2) ต้องคำนึงถึงความสอดคล้องกับกลยุทธ์ทางธุรกิจและความสามารถในการแข่งขัน ทั้งนี้ ควรครอบคลุมเรื่องการแบ่งประเภทของการใช้บริการ การบริหารความเสี่ยงที่เกิดจากการใช้บริการ การบริหารจัดการผู้ให้บริการภายนอก การรักษาความปลอดภัยและความลับของระบบงาน และข้อมูลการรักษาความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล การรักษาความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ การคุ้มครองผู้ใช้บริการของบริษัท การกำกับดูแลเพิ่มเติมกรณีการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อบริษัท (Critical IT Outsourcing) และการรายงานและการตรวจสอบ เป็นต้น

(1.3) ต้องให้มีการทบทวนนโยบายจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือหากมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้สอดคล้องกับกลยุทธ์ของบริษัทที่อาจเปลี่ยนแปลงไป

(2) การบริหารความเสี่ยงในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ และการใช้บริการ Cloud Computing

(2.1) กำหนดให้มีแนวทางการบริหารความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศอย่างชัดเจนและเป็นลายลักษณ์อักษรโดยต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงของบริษัท รวมถึงขนาดปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ และนโยบายการบริหารความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศดังกล่าว ต้องได้รับความเห็นชอบหรือได้รับการอนุมัติจากผู้มีอำนาจตามระเบียบของบริษัท ทั้งนี้ ต้องมีการกำหนดแนวทาง วิธีการ และผู้รับผิดชอบในการบริหารความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการจากผู้ให้บริการภายนอก ด้านงานเทคโนโลยีสารสนเทศอย่างชัดเจนและเป็นลายลักษณ์อักษร ต้องประเมินผลการปฏิบัติตาม แนวทางและวิธีการที่กำหนดอย่างสม่ำเสมอ และต้องมีการรายงานผลการปฏิบัติดังกล่าวให้คณะอนุกรรมการที่ได้รับมอบหมายหรือพนักงานระดับบริหารที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสม

(2.2) ต้องมีความรู้ความเข้าใจในงานเทคโนโลยีสารสนเทศที่ใช้บริการจากผู้ให้บริการภายนอกตามสมควร ต้องสามารถประเมินระดับความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ และต้องจัดให้มีระบบการประเมิน ควบคุม และบริหารจัดการความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศให้ครอบคลุมความเสี่ยงที่สำคัญที่อาจเกิดขึ้น (เช่น ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านกฎหมาย และ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นต้น) โดยควรสอดคล้องกับขนาดปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ

ทั้งนี้ ในการประเมินความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ รวมถึงการใช้บริการ Cloud Computing ควรครอบคลุมถึงความเสี่ยงที่เกี่ยวข้องกับการรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) การพึ่งพิงการใช้บริการจากผู้ให้บริการภายนอกจนอาจทำให้การเปลี่ยนแปลงหรือยกเลิกการใช้บริการทำได้ยาก (Vendor Lock-In) และมีผลกระทบต่อระบบงานของบริษัท นอกจากนี้ ในกรณีที่มีการใช้บริการจากผู้ให้บริการภายนอกในต่างประเทศ โดยเฉพาะการจัดเก็บข้อมูล การประมวลผลหรือการดำเนินการใด ๆ เกี่ยวกับข้อมูลต้องมีการประเมินความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการในต่างประเทศนั้น เช่น ความเสี่ยงจากการไม่สามารถเข้าถึงข้อมูลอันเนื่องมาจากการขัดข้องหรือการปิดกั้นเครือข่ายสื่อสาร หรือระบบสื่อสารระหว่างประเทศ (Information Access Risk) และความเสี่ยงด้านกฎหมายที่เกี่ยวข้องกับการปฏิบัติตามหลักเกณฑ์ของต่างประเทศ (Cross - Border Compliance) เป็นต้น

(2.3) ต้องจัดให้มีแนวทางในการติดตามประสิทธิภาพในการให้บริการของผู้ให้บริการภายนอกอย่างต่อเนื่อง แนวทางในการรับทราบการเปลี่ยนแปลงที่เกิดขึ้นกับผู้ให้บริการภายนอก รวมถึงแนวทางในการรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นจากการให้บริการของผู้ให้บริการภายนอก (Day - to - Day Incident) อย่างสม่ำเสมอ ทั้งนี้ บริษัทต้องมีส่วนร่วมในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติ หากบริษัทประเมินว่าเหตุการณ์ผิดปกติที่เกิดขึ้นนั้นอาจกระทบต่อการดำเนินธุรกิจของบริษัทอย่างมีนัยสำคัญ นอกจากนี้บริษัทต้องมีการทบทวนและประเมินประสิทธิภาพในการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ และมีการรายงานผลการประเมินดังกล่าวให้คณะอนุกรรมการที่ได้รับมอบหมายหรือพนักงานระดับบริหารที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสม

(2.4) ต้องจัดให้มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) ที่ครอบคลุมถึงการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ โดยควรสอดคล้องกับขนาดปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการและความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ รวมถึงผลกระทบของการใช้บริการที่มีต่อการดำเนินธุรกิจของบริษัท และต้องจัดให้มีแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (Disaster Recovery Plan) เพื่อรองรับกรณีการเกิดปัญหาหรือเหตุการณ์ผิดปกติจากการใช้บริการจากผู้ให้บริการภายนอกและเพื่อลดผลกระทบที่อาจเกิดขึ้น โดยบริษัทต้องมั่นใจว่าจะมีข้อมูลพร้อมใช้ภายในประเทศสำหรับการดำเนินธุรกิจและการให้บริการแก่ลูกค้าอย่างต่อเนื่อง และต้องมีการทบทวนและทดสอบการปฏิบัติตามแผนรองรับการดำเนินธุรกิจและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอเพื่อให้สามารถปฏิบัติงานได้จริง รวมทั้งต้องจัดให้มีกระบวนการในการบริหารจัดการปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการใช้บริการ และมีการรายงานปัญหาหรือเหตุการณ์ผิดปกติและการจัดการปัญหา

หรือเหตุการณ์ผิดปกติดังกล่าว ให้คณะอนุกรรมการที่ได้รับมอบหมายหรือพนักงานระดับบริหารที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสม

(3) การบริหารจัดการผู้ให้บริการภายนอก (Service Provider Management) ในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศและการใช้บริการ Cloud Computing

(3.1) ต้องกำหนดกระบวนการและหลักเกณฑ์ในการคัดเลือกผู้ให้บริการภายนอกที่ชัดเจน และมีการตรวจสอบความพร้อมและพิจารณาความเหมาะสมของผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกจะสามารถให้บริการได้อย่างต่อเนื่อง และสามารถตอบสนองความต้องการของบริษัทได้ โดยควรคำนึงถึงปัจจัยที่สำคัญ เช่น ความรู้ด้านเทคโนโลยีสารสนเทศ ประสบการณ์ระบบการบริหารงานภายใน ศักยภาพ และความสามารถในการให้บริการทั้งในภาวะปกติและไม่ปกติ โดยเฉพาะอย่างยิ่งกรณีที่ผู้ให้บริการภายนอกนั้นมีการให้บริการแก่ผู้ใช้บริการหลายราย (Concentration Risk) เป็นต้น

ทั้งนี้ ในการคัดเลือกผู้ให้บริการ Cloud Computing ควรคำนึงถึงความพร้อมและมาตรฐานในการให้บริการของผู้ให้บริการดังกล่าว โดยผู้ให้บริการ Cloud Computing ควรได้รับการรับรองมาตรฐานสากลที่เกี่ยวข้อง เช่น มาตรฐานสากลในเรื่องการรักษาความปลอดภัยของระบบงานและข้อมูล เป็นต้น

(3.2) ต้องให้มีการจัดทำสัญญาการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร หรือมีการจัดทำข้อตกลงการให้บริการ (Service Level Agreement) เป็นลายลักษณ์อักษร และต้องระบุบทบาท หน้าที่ ความรับผิดชอบ เงื่อนไขการให้บริการของผู้ให้บริการภายนอก และความรับผิดต่อความเสียหายใด ๆ ในกรณีที่ผู้ให้บริการภายนอกไม่ปฏิบัติตามเงื่อนไขในการให้บริการไว้ในสัญญาหรือข้อตกลงให้บริการให้ชัดเจน ส่วนเนื้อหาของสัญญาและข้อตกลงการให้บริการควรครอบคลุมประเด็นสำคัญ เช่น

(3.2.1) ขอบเขตงานเทคโนโลยีสารสนเทศที่ใช้บริการและเงื่อนไขในการให้บริการของผู้ให้บริการภายนอก

(3.2.2) มาตรฐานของการปฏิบัติงานขั้นต่ำที่ต้องการจากผู้ให้บริการภายนอก (เช่น มาตรฐานด้านการรักษาความปลอดภัยและความลับของข้อมูล การห้ามนำข้อมูลไปใช้นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงการให้บริการ ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ เป็นต้น)

(3.2.3) ระบบการควบคุมภายในของผู้ให้บริการภายนอก

(3.2.4) การจัดทำแผนฉุกเฉินสำหรับการให้บริการภายนอกที่ควรสอดคล้องกับแผนฉุกเฉินของบริษัท

(3.2.5) การรายงานผลการปฏิบัติงานของผู้ให้บริการภายนอกซึ่งครอบคลุมถึงการรายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการให้บริการ

(3.2.6) ความรับผิดชอบของบริษัทและผู้ให้บริการภายนอก ภาระผูกพันในกรณีที่เกิดปัญหาในการให้บริการ เงื่อนไขหรือแนวทางในการเปลี่ยนแปลงหรือยกเลิกสัญญา เช่น การทำลายข้อมูลของผู้ให้บริการของบริษัทและข้อมูลของบริษัททั้งหมดเมื่อสิ้นสุดหรือยกเลิกการใช้บริการจากผู้ให้บริการภายนอก เป็นต้น

(3.2.7) สิทธิของบริษัท ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก หรือธนาคารแห่งประเทศไทย ในการเรียกดูข้อมูลที่เกี่ยวข้องและการตรวจสอบการดำเนินงานและการควบคุมภายในของผู้ให้บริการภายนอก ทั้งในกรณีที่ผู้ให้บริการภายนอกประกอบธุรกิจในประเทศและต่างประเทศ

นอกจากนี้ บริษัทต้องมีการเก็บสัญญาหรือข้อตกลงการให้บริการ และควรพิจารณาความเหมาะสมในการจัดซื้อจัดจ้างก่อนสัญญาจะหมดอายุลง เพื่อให้พร้อมสำหรับการตรวจสอบและเมื่อมีการร้องขอ

ทั้งนี้ ในกรณีที่ผู้ให้บริการภายนอกประกอบธุรกิจในต่างประเทศและหน่วยงานกำกับดูแลในประเทศนั้นมีข้อจำกัดเกี่ยวกับการเข้าตรวจสอบการดำเนินงานของผู้ให้บริการภายนอกดังกล่าว หรือมีข้อกฎหมาย หรือหลักเกณฑ์การกำกับดูแลที่แตกต่างจากที่บริษัทกำหนด ซึ่งทำให้ต้องปฏิบัติตามกฎหมาย ข้อกำหนด หรือหลักเกณฑ์การกำกับดูแลของหน่วยงานกำกับดูแลในประเทศนั้นด้วย บริษัทขอสงวนสิทธิ์ในการพิจารณากำหนดหลักเกณฑ์การกำกับดูแล และ/หรือเงื่อนไขอื่นตามธนาคารแห่งประเทศไทยกำหนดเป็นรายกรณีตามความเหมาะสม

(4) การรักษาความปลอดภัยและความลับของระบบและข้อมูล (Security) ในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ และการใช้บริการ Cloud Computing

(4.1) ต้องมั่นใจว่าผู้ให้บริการภายนอกมีแนวทางหรือมาตรฐานในการรักษาความปลอดภัยและความลับของระบบงานและข้อมูล ทั้งข้อมูลของผู้ใช้บริการของบริษัทและข้อมูลของบริษัท โดยควรมีความสอดคล้องกับขนาดปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ให้บริการและความเสี่ยงที่เกี่ยวเนื่องกับการให้บริการ ทั้งนี้ บริษัทอาจกำหนดให้ผู้ให้บริการภายนอกมีการประยุกต์ใช้แนวทางการควบคุมด้านงานเทคโนโลยีสารสนเทศที่ดี เป็นมาตรฐานสากล และได้รับการยอมรับโดยทั่วไปตามความเหมาะสม

ในกรณีที่มีการใช้บริการ Cloud Computing ต้องมั่นใจว่าผู้ให้บริการ Cloud Computing มีแนวทางการรักษาความปลอดภัยข้อมูลสำคัญของผู้ใช้บริการของบริษัทและข้อมูลของบริษัทตามวิธีการและมาตรฐานสากล เช่น การเข้ารหัสข้อมูล (Data Encryption) การควบคุมกุญแจที่ใช้เข้าถึงและเข้ารหัสข้อมูลบนระบบ Cloud Computing (Key Management) เป็นต้น

(4.2) ต้องจัดให้มีกระบวนการ ขั้นตอน หรือระบบในการติดตาม ประเมินผลและตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานด้านการรักษาความปลอดภัยและความลับของระบบงานและข้อมูลที่ได้ตกลงไว้กับบริษัท

(4.3) ต้องจัดให้มีกระบวนการ ขั้นตอน หรือระบบในการดำเนินการนำข้อมูลของผู้ใช้บริการของบริษัทและข้อมูลของบริษัททั้งหมดกลับมาจากผู้ให้บริการภายนอก และบริษัทต้องมั่นใจว่าผู้ให้บริการภายนอกมีกระบวนการขั้นตอน หรือระบบในการดำเนินการทำลายข้อมูลของผู้ใช้บริการของบริษัทและข้อมูลของบริษัททั้งหมดเมื่อมีการสิ้นสุดหรือยกเลิกการใช้บริการจากผู้ให้บริการภายนอก

(4.4) ต้องมั่นใจว่าผู้ให้บริการภายนอกมีแนวทางหรือมาตรฐานในการดูแลและป้องกันข้อมูลสำคัญของผู้ใช้บริการของบริษัทและข้อมูลของบริษัท โดยควรสอดคล้องกับกฎหมายข้อบังคับที่เกี่ยวข้องของทางการ และมาตรฐานสากลที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศนั้น

(5) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (Integrity) ในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ และการใช้บริการ Cloud Computing

(5.1) ต้องมั่นใจว่าผู้ให้บริการภายนอกมีแนวทางหรือมาตรฐานในการรักษาความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล ซึ่งครอบคลุมตั้งแต่การพัฒนาหรือการเปลี่ยนแปลงแก้ไขระบบงานการควบคุมทั้งในส่วนของการบันทึกข้อมูลเข้าสู่ระบบ (Input Validation) การประมวลผล (Processing Control) และการนำข้อมูลออกจากระบบ (Output Control) รวมทั้งมีการดำเนินการให้งานเทคโนโลยีสารสนเทศที่ให้บริการสามารถทำงานได้อย่างมีประสิทธิภาพและถูกต้องเชื่อถือได้ โดยควรมีความสอดคล้องกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ให้บริการและความเสี่ยงที่เกี่ยวเนื่องกับการให้บริการ ทั้งนี้ บริษัทอาจกำหนดให้ผู้ให้บริการภายนอกมีการประยุกต์ใช้แนวทางการควบคุมด้านงานเทคโนโลยีสารสนเทศที่ดี เป็นมาตรฐานสากล และได้รับการยอมรับโดยทั่วไปตามความเหมาะสม

(5.2) ต้องจัดให้มีกระบวนการ ขั้นตอน หรือระบบในการติดตามประเมินผลและตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานด้านความถูกต้องเชื่อถือได้ของระบบงานและข้อมูลที่ได้ตกลงไว้กับบริษัท

(6) ความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (Availability) ในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศและการใช้บริการ Cloud Computing

(6.1) ต้องมั่นใจว่าผู้ให้บริการภายนอกมีแนวทางหรือมาตรฐานในการทำให้งานเทคโนโลยีสารสนเทศที่ให้บริการแก่บริษัทพร้อมในการใช้งานอย่างต่อเนื่อง ทั้งในภาวะปกติและไม่ปกติ โดยควรมีความสอดคล้องกับขนาดปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ให้บริการและความเสี่ยงที่เกี่ยวเนื่องกับการให้บริการ ทั้งนี้ บริษัทอาจกำหนดให้ผู้ให้บริการภายนอกมีการประยุกต์ใช้แนวทางการควบคุมด้านงานเทคโนโลยีสารสนเทศที่ดีเป็นมาตรฐานสากล และได้รับการยอมรับโดยทั่วไปตามความเหมาะสม

(6.2) ต้องจัดให้มีกระบวนการ ขั้นตอน หรือระบบในการติดตาม ประเมินผลและตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานด้านความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ให้บริการที่ได้ตกลงไว้กับบริษัท

(7) การคุ้มครองผู้ใช้บริการของบริษัท (Consumer protection) ในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ และการใช้บริการ Cloud Computing

(7.1) ต้องมั่นใจว่าผู้ให้บริการภายนอกจะไม่นำข้อมูลของผู้ใช้บริการของบริษัทหรือข้อมูลของบริษัทไปเปิดเผยให้กับบุคคลอื่นใดโดยไม่ได้รับความยินยอมจากบริษัท

(7.2) ต้องจัดให้มีกระบวนการ ขั้นตอน หรือ ระบบในการติดตาม ประเมินผล และตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานด้านการคุ้มครองผู้ใช้บริการของบริษัทที่ได้ตกลงไว้กับบริษัท

(7.3) ต้องให้มีระบบการดูแลและจัดการเรื่องร้องเรียนให้แก่ผู้ใช้บริการของบริษัทอย่างเพียงพอและเหมาะสม และมีการรายงานการจัดการเรื่องร้องเรียนดังกล่าวให้คณะอนุกรรมการที่ได้รับมอบหมายหรือพนักงานระดับบริหารที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสม ทั้งนี้ ในกรณีที่ผู้ใช้บริการของบริษัทได้รับความเสียหายจากการใช้บริการจากผู้ให้บริการภายนอก ต้องมีแนวทางในการชดเชยความเสียหายให้แก่ผู้ใช้บริการของบริษัทอย่างเหมาะสม

5.4.2 หลักเกณฑ์การควบคุมเฉพาะสำหรับงานเทคโนโลยีสารสนเทศที่มีความสำคัญอย่างยิ่ง (Specific Control)

กรณีที่ใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อบริษัท เช่น การใช้บริการระบบประมวลผลกลาง (Core Banking System) ศูนย์คอมพิวเตอร์ (Data Center) และระบบเครือข่ายสื่อสาร (Network System) รวมถึงมีการใช้บริการ Cloud Computing ในงานที่มีความสำคัญอย่างยิ่งต่อบริษัท เป็นต้น นอกจากจะต้องปฏิบัติตามหลักเกณฑ์การควบคุมทั่วไปตามข้อ 5.4.1 แล้ว บริษัทต้องจัดให้มีการกำกับดูแลเพิ่มเติมที่สอดคล้องกับแนวทางการควบคุมด้านงานเทคโนโลยีสารสนเทศที่ดี เป็นมาตรฐานสากลและได้รับการยอมรับโดยทั่วไป โดยให้พิจารณาตามความเหมาะสมกับขนาดปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ รวมทั้งต้องมีระบบการกำกับดูแลที่เหมาะสมภายใต้การกำกับดูแลของคณะอนุกรรมการที่ได้รับมอบหมายหรือพนักงานระดับบริหารที่ได้รับมอบหมายตามหลักเกณฑ์การควบคุมเฉพาะสำหรับงานเทคโนโลยีสารสนเทศที่มีความสำคัญอย่างยิ่ง (Specific Control) ดังนี้

(1) การกำกับดูแลเพิ่มเติม (Specific Risk Control)

(1.1) ผู้ให้บริการภายนอกต้องมีกระบวนการ ขั้นตอน การประเมิน และการควบคุมความเสี่ยง อย่างน้อยตามกรอบหลักการด้านเทคโนโลยีสารสนเทศที่สำคัญ 3 ประการ คือ การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (Security) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (Integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (Availability) ที่สอดคล้องตามหลักมาตรฐานสากลที่เกี่ยวข้อง ซึ่งอาจพิจารณาประยุกต์ให้เหมาะสมกับขนาดปริมาณธุรกรรม ความซับซ้อนของงาน

เทคโนโลยีสารสนเทศที่ให้บริการและความเสี่ยงที่เกี่ยวเนื่องกับการให้บริการ โดยผู้ให้บริการภายนอกควรได้รับการรับรองตามมาตรฐานสากลที่เกี่ยวข้องเช่น มาตรฐานของ International Organization for Standardization (ISO) และ Telecommunications Industry Association (TIA) เป็นต้น

(1.2) ต้องจัดให้มีกระบวนการ ขั้นตอน หรือระบบในการติดตามประเมินผลและตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานสากลที่เกี่ยวข้องที่ได้ตกลงไว้กับบริษัท และต้องจัดให้มีการทดสอบเพื่อให้มั่นใจว่าการใช้บริการจากบุคคลภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อบริษัทจะไม่ก่อให้เกิดความเสี่ยงตามกรอบหลักการด้านเทคโนโลยีสารสนเทศที่สำคัญ 3 ประการ คือ การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (Security) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (Integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (Availability) จนนำมาสู่ช่องโหว่ที่ร้ายแรงต่อการทุจริต และ/หรือภัยคุกคามด้านเทคโนโลยีสารสนเทศ ทั้งจากภายในและภายนอก ซึ่งอาจส่งผลกระทบต่อธุรกิจอย่างร้ายแรง หรือก่อให้เกิดผลกระทบในวงกว้างต่อการให้บริการทางการเงินที่สำคัญของบริษัท เช่น ต้องจัดให้มีการทดสอบแผนฉุกเฉินด้านงานเทคโนโลยีสารสนเทศ และมีการทดสอบระบบการรักษาความปลอดภัยเชิงลึก (Penetration Test) สำหรับการใช้งานบริการระบบอินเตอร์เน็ต (Internet Banking) และระบบดิจิตัลผ่านอุปกรณ์เคลื่อนที่ (Mobile Banking) เป็นต้น

(1.3) กรณีการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ ซึ่งรวมถึงการใช้บริการ Cloud Computing ในงานประเภทที่มีความสำคัญอย่างยิ่งต่อบริษัทต้องกำหนดให้ผู้ให้บริการภายนอกระบุสถานที่ในการจัดเก็บข้อมูล ประมวลผลข้อมูล หรือดำเนินการใด ๆ เกี่ยวกับข้อมูลของบริษัท (Data Location) เพื่อให้บริษัทสามารถบริหารความเสี่ยงของข้อมูลที่อาจเกิดขึ้นกับการใช้บริการได้อย่างเหมาะสม รวมทั้งบริษัทต้องจัดให้มีแผนฉุกเฉินรองรับกรณีที่บริษัทไม่สามารถใช้บริการ Cloud Computing และมีการทดสอบแผนฉุกเฉินก่อนใช้บริการเพื่อให้มั่นใจว่าบริษัทสามารถให้บริการทางการเงินได้อย่างต่อเนื่องตามนโยบายและแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan)

(2) ระบบการกำกับดูแลที่เหมาะสม (Oversight)

(2.1) ต้องนำเสนอรายละเอียดของการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อบริษัทพร้อมผลการประเมินความเสี่ยงโดยละเอียดให้กับคณะอนุกรรมการที่ได้รับมอบหมายหรือพนักงานระดับบริหารที่ได้รับมอบหมาย เพื่อพิจารณาให้ความเห็นชอบในการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศประเภทที่มีความสำคัญอย่างยิ่งต่อบริษัททั้งก่อนเริ่มใช้บริการ เมื่อมีการเปลี่ยนแปลงการใช้บริการอย่างมีนัยสำคัญตามที่บริษัทกำหนดหรือมีการต่ออายุสัญญา

(2.2) ต้องมีการรายงานให้คณะอนุกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสมเกี่ยวกับผลการประเมินประสิทธิภาพการติดตามและการตรวจสอบการดำเนินการของผู้ให้บริการภายนอก โดยอาจพิจารณาตามกรอบหลักการ

ด้านเทคโนโลยีสารสนเทศที่สำคัญ 3 ประการ คือ การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (Security) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (Integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (Availability) รวมถึงปัญหาหรือเหตุการณ์ผิดปกติและเรื่องร้องเรียนที่เกิดขึ้นจากการใช้บริการ

6. การปฏิบัติงานและการควบคุมภายใน

ให้ผู้จัดการบริษัทกำหนดระเบียบ หลักเกณฑ์ หรือวิธีปฏิบัติในการดำเนินการตามนโยบายฉบับนี้ ให้หน่วยงานที่เกี่ยวข้องได้ยึดถือปฏิบัติ

7. บทเฉพาะกาล

การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศที่มีการอนุมัติก่อนหน้าประกาศนโยบายฉบับนี้ ให้ถือว่าได้ดำเนินการคัดเลือกและการว่าจ้างผู้ให้บริการตามวิธีการและอำนาจอนุมัติที่บริษัทได้กำหนดไว้โดยอนุโลม

หากมีการต่ออายุการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศที่ได้รับอนุโลมตามความในวรรคแรกนั้น หน่วยงานหรือโครงการที่จะใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศจะต้องถือปฏิบัติตามนโยบายฉบับนี้โดยเคร่งครัด

ประกาศ ณ วันที่ 12 มิถุนายน พ.ศ. 2566

(นางญาใจ พัฒนสุขวสันต์)
ประธานกรรมการ
บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด