คู่มือตรวจสอบ
การใช้บริการด้านเทคโนโลยี
จากบุคคลภายนอก
(Outsourcing Technology Services)

คำนำ

คู่มือฉบับนี้จะนำมาทดแทนคู่มือ 1996 FFIEC Information Systems Examination Handbook บท IS Servicing – Provider and Receiver

อุตสาหกรรมการให้บริการทางการเงินจากอดีตจนถึงปัจจุบันมีการเปลี่ยนแปลงค่อนข้างมากและเป็นไปอย่างรวดเร็ว ความก้าวหน้าทางเทคโนโลยีทำให้สถาบันการเงินสามารถออกและเสนอผลิตภัณฑ์และบริการผ่านช่องทางที่หลากหลายมากขึ้น การเปลี่ยนแปลงดังกล่าวส่งผลให้สถาบันการเงินมีการพึ่งพาผู้ให้บริการทางด้านเทคโนโลยีมากขึ้น ซึ่งมักจะเรียกลักษณะการพึ่งพาดังกล่าวว่า Outsourcing

คู่มือ FFIEC เรื่อง Outsourcing Technology Services Booklet กล่าวถึงแนวทางและขั้นตอนการปฏิบัติงานตรวจสอบสำหรับผู้ตรวจสอบและเจ้าหน้าที่ของสถาบันการเงิน ใช้ในการประเมินกระบวนการบริหารความเสี่ยงของสถาบันการเงินจากการใช้บริการของผู้ให้บริการภายนอก การบริหารและการติดตามการให้บริการของผู้ให้บริการดังกล่าว นอกจากแนวทางตามคู่มือนี้ สถาบันการเงินจะต้องนำกฎหมาย กฎระเบียบของทางการและผู้กำกับดูแลในเรื่องที่เกี่ยวข้องทั้งของสถาบันการเงินและผู้ให้บริการ มาประกอบการพิจารณาในการบริหารจัดการความเสี่ยงจากการใช้บริการจากผู้ให้บริการ เพื่อให้เกิดความสอดคล้องกับความเสี่ยงโดยรวมของสถาบันการเงิน

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ หวังว่าแนวทางการตรวจสอบในคู่มือฉบับนี้จะเป็นประโยชน์และช่วยพัฒนาการตรวจสอบให้มีประสิทธิภาพต่อไปในอนาคต

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ

ธันวาคม 2551

สารบัญ

<u>ส่วนที่ 1</u> บทนำ

การว่าจ้างบริการด้านเทคโนโลยีจากภายนอกช่วยให้สถาบันการเงินสามารถเสนอบริการที่ทันสมัยแก่ลูกค้าโดยไม่ต้องลงทุนเป็นเจ้าของเทคโนโลยีหรือมีบุคลากรที่มีทักษะในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศดังกล่าว ในหลายๆ สถานการณ์ การใช้บริการจากภายนอกเป็นทางเลือกที่ทำให้สถาบันการเงินประหยัดต้นทุนมากกว่าการที่สถาบันการเงินดำเนินการเอง แต่ก็ไม่ได้หมายความว่าสถาบันการเงินจะมีความเสี่ยงพื้นฐานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการดำเนินธุรกิจลดลง อันได้แก่ ความเสี่ยงจากการสูญเสียทางการเงิน ความเสียเปรียบทางการแข่งขัน การเสื่อมเสียชื่อเสียง การรั่วไหลของข้อมูล และการปฏิบัติที่ไม่เป็นไปตามกฎระเบียบของทางการ เนื่องจากงานดำเนินการโดยผู้ให้บริการภายนอก ดังนั้น ความเสี่ยงอาจจะต้องพิจารณาในอีกแง่มุมหนึ่งที่แตกต่างไปจากงานที่ดำเนินการโดยสถาบันการเงินเอง ซึ่งสถาบันการเงินจำเป็นต้องมีกระบวนการควบคุมที่เหมาะสมในการใช้ติดตามความเสี่ยงดังกล่าว

สถาบันการเงินสามารถใช้บริการจากภายนอกได้ในหลายลักษณะ ตามคำจำกัดความในหนังสือที่ สนส.29/2551 ลงวันที่ 3 สิงหาคม 2551 เรื่อง การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) รวมถึงหลักเกณฑ์ของทางการที่เกี่ยวข้องในเรื่องดังกล่าวซึ่งจะมีผลบังคับใช้ต่อไป

คู่มือฉบับนี้จะกล่าวถึงความรับผิดชอบของสถาบันการเงินในการบริหารความเสี่ยงที่เกี่ยวข้องกับการใช้บริการด้านเทคโนโลยีสารสนเทศจากภายนอก

เหตุผลของการตัดสินใจเลือกใช้บริการจากภายนอกอาจมีได้หลายอย่าง ดังนี้

- เพื่อให้เกิดประสิทธิภาพทางการเงินและการปฏิบัติงาน
- ตอบสนองเป้าหมายของผู้บริหารที่จะมุ่งเน้นการทำธุรกิจหลักมากขึ้น
- ข้อจำกัดของทรัพยากรภายในที่ใช้ในการดำเนินงานหลัก
- เพื่อได้รับทักษะความเชี่ยวชาญเฉพาะด้าน
- เพิ่มความต่อเนื่องของการให้บริการ
- เพิ่มช่องทางการเสนอผลิตภัณฑ์และบริการ
- เพิ่มความสามารถในการจัดหาและสนับสนุนเทคโนโลยีปัจจุบัน โดยไม่ต้องแก้ไขปัญหาอุปสรรคเองและหลีกเลี่ยงความล้าสมัย
- รักษาเงินทุนไว้สำหรับการลงทุนธุรกิจอื่น

การใช้บริการด้านเทคโนโลยีจากภายนอกช่วยเพิ่มคุณภาพ ลดค่าใช้จ่าย เสริมสร้างการควบคุมให้แข็งแกร่งขึ้น รวมทั้งสามารถบรรลุวัตถุประสงค์ตามที่ได้กล่าวข้างต้น ซึ่งการตัดสินใจ

ใช้บริการจากภายนอกควรรวมอยู่ในแผนกลยุทธ์และเป้าหมายขององค์กร

และก่อนที่จะตัดสินใจใช้บริการจากภายนอกนั้น ผู้บริหารของสถาบันการเงินควรได้รับความมั่นใจว่าการดำเนินการดังกล่าวจะสอดคล้องกับแผนกลยุทธ์ขององค์กร และควรมีการประเมินข้อเสนอเทียบกับหลักเกณฑ์การพิจารณาที่กำหนด ระดับของการดูแลและสอบทานกิจกรรมที่ใช้บริการจากภายนอกขึ้นอยู่กับความสำคัญของบริการ กระบวนการ หรือระบบงานที่มีต่อการดำเนินงานของสถาบันการเงิน

สถาบันการเงินควรมีกระบวนการบริหารความเสี่ยงจากการใช้บริการจากภายนอกอย่างครอบคลุมเพื่อติดตามดูแลการดำเนินงานของผู้ให้บริการ กระบวนการดังกล่าวควรประกอบด้วยการประเมินความเสี่ยง การคัดเลือกผู้ให้บริการ การสอบทานสัญญา และการติดตามการดำเนินงานของผู้ให้บริการ นอกจากนี้ สถาบันการเงินจะต้องตระหนักถึงความเสี่ยงด้านกฎหมายที่สืบเนื่องจากข้อกฎหมาย กฎระเบียบของทางการและผู้กำกับดูแลของทั้งสถาบันการเงินและผู้ให้บริการในเรื่องที่เกี่ยวข้อง และนำประเด็นดังกล่าวมาประกอบการพิจารณาในการกำหนดกระบวนการบริหารจัดการความเสี่ยงจากการใช้บริการจากภายนอกด้วย งานที่ใช้บริการจากภายนอกควรต้องมีการบริหารความเสี่ยง การรักษาความปลอดภัย การรักษาความลับ และการปฏิบัติตามนโยบายอื่นๆ **ที่เหมือนกับกรณีที่สถาบันการเงินนั้นดำเนินงานเอง** คู่มือฉบับนี้มุ่งเน้นวิธีที่หน่วยงานกำกับดูแลภาครัฐใช้ในการสอบทานกระบวนการบริหารความเสี่ยงของสถาบันการเงินที่ใช้บริการจากผู้ให้บริการภายนอก

เพื่อให้มั่นใจว่าสถาบันการเงินดำเนินงานด้วยความปลอดภัยและมั่นคง บริการที่ดำเนินการโดยผู้ให้บริการด้านเทคโนโลยีจึงอยู่ภายใต้ขอบเขตการกำกับตรวจสอบขององค์กรภาครัฐที่กำกับสถาบันการเงิน มีอำนาจในการกำกับตรวจสอบกิจกรรมและข้อมูลทั้งหมดของสถาบันการเงินไม่ว่าสถาบันการเงินจะดำเนินการและเก็บรักษาเองหรือโดยบุคคลที่สาม รวมถึงการดำเนินงานทั้งที่อยู่ภายในและภายนอกสถาบันการเงิน ดังนั้น จึงไม่มีอุปสรรคในการกำกับตรวจสอบสถาบันการเงินที่โอนงานให้บุคคลภายนอกดำเนินการแทน

หลักทั่วไปของการบริหารการใช้บริการจากภายนอกที่มีประสิทธิภาพที่จะกล่าวถึงในคู่มือฉบับนี้สามารถนำไปใช้กับการใช้บริการพัฒนาโปรแกรมระบบงานโดยผู้เชี่ยวชาญภายนอกด้วย ซึ่งได้มีกล่าวอยู่แล้วในคู่มือเรื่องการพัฒนาและการจัดหาระบบงานและโปรแกรม (Development and Acquisition Booklet)

อนึ่ง กรณีของสถาบันการเงินที่มีนโยบายในการใช้บริการจากสำนักงานใหญ่ สาขา บริษัทในกลุ่มหรือบริษัทในเครือ ให้ถือปฏิบัติตามหนังสือที่ สนส.29/2551 ลงวันที่ 3 สิงหาคม 2551 เรื่อง การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) รวมถึงหลักเกณฑ์ของทางการที่เกี่ยวข้องในเรื่องดังกล่าวซึ่งจะมีผลบังคับใช้ต่อไป

<u>ส่วนที่ 2</u> แนวทางที่พึงปฏิบัติ

2.1 ความรับผิดชอบของคณะกรรมการและผู้บริหารระดับสูง

<u>สรุปแนวทางการปฏิบัติ</u>

คณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงินควรจัดทำและอนุมัตินโยบายการกำกับดูแลกระบวนการใช้บริการจากภายนอกตามแนวความเสี่ยง ซึ่งนโยบายควรครอบคลุมความเสี่ยงที่เกิดจากการใช้บริการภายนอกและมีความเหมาะสมกับขนาดและความซับซ้อนของสถาบันการเงิน

คณะกรรมการและผู้บริหารระดับสูงมีความรับผิดชอบในการกำกับดูแลการใช้บริการจากภายนอก **ถึงแม้ว่าเทคโนโลยีมักจะเป็นประเด็นสำคัญในการพิจารณาตัดสินใจใช้บริการจากภายนอก** แต่การบริหารไม่ได้เกี่ยวข้องเพียงเรื่องเทคโนโลยีเท่านั้น การบริหารการใช้บริการจากภายนอกเป็นเรื่องที่เกี่ยวข้องกับการบริหารโดยรวมทั้งองค์กร **การดูแลการใช้บริการจากภายนอกควรมีกรอบแนวทางสำหรับผู้บริหารใช้ในการระบุ ประเมิน ติดตาม และควบคุมความเสี่ยงที่เกี่ยวข้องกับการใช้บริการจากภายนอก** คณะกรรมการและผู้บริหารระดับสูงควรพัฒนานโยบายและนำไปใช้ในการกำกับดูแลกระบวนการที่เกี่ยวข้องกับการใช้บริการจากภายนอกอย่างต่อเนื่อง และครอบคลุมทุก**ขั้นตอนของกระบวนการ ได้แก่ การกำหนดความต้องการใช้บริการ การกำหนดกลยุทธ์ การคัดเลือกผู้ให้บริการ การจัดทำสัญญา การติดตาม การเปลี่ยนแปลง และการยกเลิกการใช้บริการ**

ปัจจัยหลักที่สถาบันการเงินควรพิจารณา มีดังนี้

- การให้ความมั่นใจว่าการใช้บริการจากภายนอกสามารถสนับสนุนความต้องการทางธุรกิจและแผนกลยุทธ์โดยรวมขององค์กรทั้งระยะสั้นและระยะยาว
- การให้ความมั่นใจว่าสถาบันการเงินมีทักษะความเชี่ยวชาญอย่างเพียงพอในการกำกับควบคุมดูแลและบริหารการใช้บริการจากภายนอก
- การประเมินผู้ให้บริการตามขอบเขตและความสำคัญของบริการที่จะว่าจ้าง
- การจัดทำแผนการติดตามผู้ให้บริการในลักษณะครอบคลุมทั้งองค์กร โดยใช้ผลจากการประเมินความเสี่ยงของการใช้บริการภายนอกที่ดำเนินการตั้งแต่เริ่มต้นและที่ดำเนินการอย่างต่อเนื่อง

- **การแจ้งหน่วยงานกำกับดูแลราชการให้ทราบถึงการใช้บริการจากภายนอก** (หากเป็นข้อกำหนดของทางการ)

ความเสี่ยงของการใช้บริการจากภายนอกจะเป็นตัวกำหนดเวลาและบุคลากรที่จะใช้ในการบริหารการใช้บริการดังกล่าว ตัวอย่างเช่น การใช้บริการประมวลผลพอร์ตบัตรเครดิตขนาดเล็กต้องการระดับการติดตามดูแลที่แตกต่างไปจากการใช้บริการประมวลผลใบสมัครขอสินเชื่อทั้งหมด และ**สถาบันการเงินที่มีขนาดเล็กและซับซ้อนน้อยอาจมีความยืดหยุ่นน้อยกว่าสถาบันการเงินขนาดใหญ่ในการเจรจาต่อรองบริการที่ตรงกับความต้องการและการติดตามการดำเนินงานของผู้ให้บริการ**

2.2 การบริหารความเสี่ยง

การบริหารความเสี่ยง คือ กระบวนการระบุ ประเมิน ติดตาม และบริหารความเสี่ยง ไม่ว่าสถาบันการเงินจะดำเนินการด้านเทคโนโลยีและเก็บรักษาข้อมูลเองหรือว่าจ้างผู้ให้บริการดำเนินการแทนก็ยังมีความเสี่ยงอยู่ ซึ่งเป็นความรับผิดชอบของผู้บริหารสถาบันการเงินในการบริหารความเสี่ยงต่างๆ ที่เกิดจากการใช้บริการจากภายนอก ดังนั้น สถาบันการเงินควรจัดทำและรักษากระบวนการบริหารความเสี่ยงในการสร้างและติดตามการดำเนินงานโดยผู้ให้บริการภายนอกที่มีประสิทธิภาพ

กระบวนการบริหารความเสี่ยงที่มีประสิทธิภาพเกี่ยวข้องกับปัจจัยหลักหลายปัจจัยดังนี้

- การทำให้คณะกรรมการและผู้บริหารระดับสูงตระหนักถึงความเสี่ยงที่เกี่ยวข้องกับการใช้บริการจากภายนอกเพื่อให้เกิดการปฏิบัติอย่างต่อเนื่องในการบริหารความเสี่ยงที่มีประสิทธิผล
- การให้ความมั่นใจว่าการใช้บริการจากภายนอกดำเนินการด้วยความรอบคอบรัดกุมตามแง่มุมของความเสี่ยงด้านต่างๆ รวมทั้งสอดคล้องกับวัตถุประสงค์ของธุรกิจ
- การประเมินความต้องการอย่างเป็นระบบพร้อมกับจัดทำข้อกำหนดตามแนวความเสี่ยง
- การใช้เครื่องมือควบคุมความเสี่ยงที่มีประสิทธิผล
- การติดตามอย่างต่อเนื่องในการระบุและประเมินการเปลี่ยนแปลงของความเสี่ยงเมื่อเทียบกับที่เคยประเมินไว้ตั้งแต่แรก
- การจัดทำขั้นตอนปฏิบัติงาน บทบาทความรับผิดชอบ และการรายงานผลการปฏิบัติงาน

กระบวนการบริหารความเสี่ยงดังกล่าวครอบคลุมกิจกรรม ดังต่อไปนี้

- การประเมินความเสี่ยงและการกำหนดความต้องการ
- การประเมินอย่างถี่ถ้วนในการคัดเลือกผู้ให้บริการ
- การจัดทำสัญญาและการนำออกใช้งาน
- การติดตามการดำเนินงานของผู้ให้บริการ

สิ่งที่กล่าวมาข้างต้นมุ่งเน้นองค์ประกอบความเสี่ยงที่เกี่ยวข้องกับการใช้บริการภายนอก สำหรับคู่มือการตรวจสอบเทคโนโลยีสารสนเทศ เรื่อง Supervision of Technology Service Providers (TSP) Booklet จะกล่าวถึงความเสี่ยงจากการใช้บริการภายนอกในแง่มุมของผู้ให้บริการ

2.2.1 การประเมินความเสี่ยงและความต้องการ

<u>สรุปแนวทางการปฏิบัติ</u>

ผู้บริหารควร

- **ระบุความเสี่ยง**ของการใช้บริการจากภายนอก
- ร่วมมือกับผู้เกี่ยวข้องในการ**จัดทำความต้องการที่เป็นลายลักษณ์อักษรเพื่อใช้ในการควบคุม**การดำเนินการของผู้ให้บริการ
- **ใช้ความต้องการดังกล่าวเป็นแนวทางในการบริหารงาน**ในขั้นตอนที่เหลือของกระบวนการใช้บริการจากภายนอก

การใช้บริการด้านเทคโนโลยีสารสนเทศจากภายนอกเป็นส่วนหนึ่งของความเสี่ยงด้านปฏิบัติการ (หรือเรียกอีกอย่างว่า Transaction Risk) ความเสี่ยงด้านปฏิบัติการเกิดจากการทุจริต ความผิดพลาดในการปฏิบัติงาน หรือการไม่สามารถส่งมอบผลิตภัณฑ์และบริการ การไม่สามารถบริหารจัดการข้อมูลความเสี่ยงสามารถเกิดขึ้นได้ในแต่ละขั้นตอนของกระบวนการส่งมอบผลิตภัณฑ์และบริการของสถาบันการเงิน ความเสี่ยงด้านปฏิบัติการนอกจากจะเป็นเรื่องที่เกี่ยวข้องกับการประมวลผลรายการแล้ว ยังจะเกี่ยวข้องกับงานส่วนอื่นๆ เช่น การให้บริการลูกค้า การสนับสนุนและพัฒนาระบบงาน กระบวนการควบคุมภายใน การวางแผนฉุกเฉินและสมรรถนะของระบบงาน ความเสี่ยงด้านปฏิบัติการอาจส่งผลกระทบต่อความเสี่ยงอื่น เช่น อัตราดอกเบี้ย การปฏิบัติตามกฎหมาย สภาพคล่อง ราคา กลยุทธ์ หรือชื่อเสียง ดังนี้

- **ความเสี่ยงด้านชื่อเสียง** – ความผิดพลาด ความล่าช้า หรือการไม่มีเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการให้บริการลูกค้าสามารถส่งผลกระทบต่อชื่อเสียงของสถาบันการเงินที่

ให้บริการ ตัวอย่างเช่น การที่ผู้ให้บริการด้านเทคโนโลยีไม่สามารถบำรุงรักษาแผนกู้ธุรกิจและอุปกรณ์ต่างๆ ให้มีความพร้อมใช้งานในภาวะฉุกเฉินอาจลดศักยภาพของสถาบันการเงินในการให้บริการสำคัญแก่ลูกค้าได้

- **ความเสี่ยงด้านกลยุทธ์** – ทักษะและประสบการณ์ของผู้บริหารที่ไม่เพียงพออาจนำไปสู่การขาดความเข้าใจและขาดการควบคุมความเสี่ยงที่สำคัญ นอกจากนี้ ข้อมูลจากผู้ให้บริการที่ไม่ถูกต้องสามารถทำให้การตัดสินใจเชิงกลยุทธ์ของผู้บริหารผิดพลาดได้

- **ความเสี่ยงด้านกฎหมาย** - หากกิจกรรมที่ดำเนินการโดยผู้ให้บริการภายนอกไม่เป็นไปตามกฎระเบียบทางการอาจส่งผลกระทบถึงสถาบันการเงินซึ่งอาจมีความผิดตามกฎหมายได้ ตัวอย่างเช่น การเปิดเผยข้อมูลลูกค้าที่ไม่ถูกต้อง ไม่ทันเวลา หรือไม่ได้รับอนุญาต อาจทำให้สถาบันการเงินต้องโทษทางกฎหมาย ถึงแม้ว่าผู้ให้บริการมักจะทำข้อตกลงยินยอมที่จะปฏิบัติตาม พรบ.ธุรกิจสถาบันการเงิน พ.ศ. 2551 ก็ตาม แต่มักจะขาดการติดตามการเปลี่ยนแปลงของกฎระเบียบหรือหลักเกณฑ์ของทางการ ซึ่งก็จะส่งผลให้สถาบันการเงินมีความเสี่ยงด้านกฎหมายที่เพิ่มขึ้น

- **ความเสี่ยงด้านอัตราดอกเบี้ย สภาพคล่อง และราคา** – ความผิดพลาดที่เกิดจากการประมวลผลธุรกรรมที่เกี่ยวข้องกับรายได้จากการลงทุน หรือการชำระรายการหนี้สินสามารถนำไปสู่การตัดสินใจบริหารการลงทุนหรือสภาพคล่องที่ไม่เหมาะสม ส่งผลให้มีความเสี่ยงด้านตลาดเพิ่มขึ้น

(1) <u>การพิจารณาความเสี่ยงเชิงปริมาณ</u>

ความเสี่ยงเชิงปริมาณที่เกี่ยวข้องกับการใช้บริการจากภายนอกขึ้นอยู่กับงานที่ใช้บริการ ตัวผู้ให้บริการ และเทคโนโลยีที่ผู้ให้บริการใช้ในการให้บริการ **ผู้บริหารควรพิจารณาปัจจัยในการประเมินความเสี่ยงเชิงปริมาณ เพื่อใช้เป็นข้อมูลสนับสนุนการตัดสินใจในช่วงเริ่มต้น**ของการพิจารณาทางเลือกในการใช้บริการภายนอก **ดังต่อไปนี้**

- ความเสี่ยงที่เกี่ยวกับงานที่ใช้บริการจากภายนอก ได้แก่ ความสำคัญของข้อมูลที่ผู้ให้บริการมีสิทธิเข้าถึง การป้องกัน หรือการควบคุมโดยผู้ให้บริการ ปริมาณของรายการธุรกรรม และความมีนัยสำคัญของงานที่จะใช้บริการและผลกระทบต่อธุรกิจของสถาบันการเงิน

- ความเสี่ยงที่เกี่ยวกับผู้ให้บริการ ได้แก่ ความมั่นคงของฐานะการเงิน อัตราการลาออกของพนักงานและผู้บริหาร ความสามารถในการรักษาความต่อเนื่องในการดำเนินธุรกิจ ความสามารถในการจัดหาระบบสารสนเทศเพื่อการบริหารที่ถูกต้องเชื่อถือได้ และทันเวลา ประสบการณ์เกี่ยวกับงานที่เสนอจะให้บริการ การพึ่งพาผู้ให้บริการรับจ้างช่วงต่อ สถานที่ตั้ง โดยเฉพาะถ้าเป็นกรณีผู้ให้บริการที่อยู่ในต่างประเทศ (โปรดดูภาคผนวก: ผู้ให้บริการภายนอกที่อยู่ต่างประเทศ) ระบบสำรองและความน่าเชื่อถือของสายสื่อสาร

- ความเสี่ยงที่เกี่ยวกับเทคโนโลยีที่ผู้ให้บริการใช้ในการให้บริการ ได้แก่ ความน่าเชื่อถือของระบบและอุปกรณ์ต่างๆ การรักษาความปลอดภัย ความสามารถในการปรับปรุงให้สอดคล้องกับพัฒนาการของเทคโนโลยี

(2) <u>การกำหนดความต้องการ</u>

การกำหนดความต้องการของธุรกิจสามารถช่วยกำหนดขั้นตอนการดำเนินงาน รวมไปถึงการบริหารการใช้บริการจากภายนอกในระยะต่อไป การจัดทำความต้องการจะต้องผ่านกระบวนการระบุงานหรือกิจกรรมที่จะใช้บริการจากภายนอก การประเมินความเสี่ยงของการใช้บริการจากภายนอก และการจัดทำมาตรฐานการควบคุมต่างๆ **ซึ่งความต้องการที่กำหนดจะเป็นฐานในการทำความเข้าใจกันระหว่างสถาบันการเงินกับผู้ให้บริการเกี่ยวกับความเสี่ยง การจัดการความเสี่ยงและวิธีการบริหารควบคุมความเสี่ยง**

(2.1) แนวปฏิบัติหลัก

แนวทางที่พึงปฏิบัติในการจัดทำความต้องการ ครอบคลุมเรื่อง ดังนี้

- **การเข้ามามีส่วนร่วมของผู้เกี่ยวข้อง** – หน่วยงานต่างๆ ที่เกี่ยวข้องโดยตรงกับผู้ให้บริการ หรือผู้ใช้บริการจากผู้ให้บริการรายนั้น ควรมีส่วนร่วมในการกำหนดความต้องการสำหรับผลิตภัณฑ์และบริการดังกล่าว

- **การบูรณาการ** – ความต้องการควรสนับสนุนการดำเนินงานตามขั้นตอนต่างๆ ได้แก่ การชักชวนผู้ให้บริการยื่นข้อเสนอจัดหาบริการ การคัดเลือก การเจรจาสัญญา และการติดตามการดำเนินงาน

- **การจัดทำเอกสาร** - การจัดทำเอกสารช่วยให้มั่นใจได้ว่าบริการที่ว่าจ้างเป็นไปตามความต้องการที่สถาบันการเงินกำหนด นอกจากนี้ เอกสารที่จัดทำขึ้นยังสามารถใช้ในการสอบทานความเพียงพอและความถูกต้องเชื่อถือได้ของกระบวนการดำเนินการได้ด้วย

(2.2) องค์ประกอบ

ขั้นตอนการจัดทำความต้องการ **คือ กระบวนการจัดทำเอกสารแสดงรายละเอียดของความคาดหวังต่างๆ เกี่ยวกับการใช้บริการจากผู้ให้บริการภายนอกของสถาบันการเงิน รายละเอียดของความต้องการในแต่ละหัวข้อที่แสดงต่อไปนี้เป็นภาพกว้างๆ ซึ่งสถาบันการเงินอาจพิจารณาปรับให้เหมาะสมกับระดับความเสี่ยงในการใช้บริการแต่ละกรณี ดังนี้**

(2.2.1) ขอบเขตและลักษณะของบริการ

- คำอธิบายของบริการ
- เทคโนโลยี

- การบริการลูกค้า

(2.2.2) มาตรฐานและระดับการให้บริการ

- ความพร้อมใช้และการดำเนินงาน
- การบริหารการเปลี่ยนแปลง
- การรายงานทางการเงิน
- คุณภาพของบริการ
- การรักษาความปลอดภัย
- ความต่อเนื่องของธุรกิจ

(2.2.3) ลักษณะขั้นต่ำที่ยอมรับได้ของผู้ให้บริการ

- ประสบการณ์ในการทำธุรกิจ
- ประสบการณ์ในการบริหาร
- โครงสร้างเทคโนโลยีและระบบงาน
- การควบคุมกระบวนการปฏิบัติงาน
- ฐานะการเงิน
- ชื่อเสียง รวมถึงแหล่งอ้างอิง
- ระดับการพึ่งพาบุคคลที่สาม ผู้รับจ้างช่วงงานต่อ หรือหุ้นส่วน
- ประวัติทางกฎหมาย การปฏิบัติตามระเบียบของทางการ
- ความสามารถในการบรรลุความต้องการในอนาคต

(2.2.4) การติดตามและการรายงาน

- เกณฑ์ที่ใช้ในการวัดและการรายงาน
- สิทธิในการเข้าตรวจสอบ
- รายงานของบุคคลที่สาม
- การประสานงานเพื่อตอบโต้เหตุการณ์ที่กระทบกับความปลอดภัย

(2.2.5) ข้อกำหนดในการโอนงาน/ส่งมอบงาน (Transition Requirement)

- การโอนย้ายข้อมูลไปให้ผู้ให้บริการในช่วงเริ่มต้น
- การใช้เครื่องมือสื่อสารที่จำเป็น
- การโอนย้ายข้อมูลกลับคืนจากผู้ให้บริการ หากยกเลิกสัญญา
- การฝึกอบรมพนักงาน

(2.2.6) ระยะเวลาของสัญญา การยกเลิกสัญญา และการมอบหมายสิทธิ

- วันเริ่มต้นของสัญญา และระยะเวลาของสัญญา

- เงื่อนไขและสิทธิในการยกเลิกสัญญา
- ความเป็นเจ้าของข้อมูล
- การเรียกข้อมูลกลับคืนในรูป machine-readable format อย่างทันเวลา
- ค่าใช้จ่ายในการโอนงาน/ส่งมอบงาน
- ข้อจำกัดในการกำกับดูแลการมอบหมายสิทธิไปให้บุคคลที่สาม
- ข้อพิพาท/โต้แย้ง
- การรักษาความลับของข้อมูล

(2.2.7) การคุ้มครองความเสียหายตามสัญญา

- การชดใช้ความเสียหาย
- ขีดจำกัดของความรับผิดชอบต่อความเสียหาย
- การประกันภัย

กรณีที่มีการใช้บริการของบริษัทในเครือหรือบริษัทลูก ผู้บริหารต้องมั่นใจได้ว่าองค์ประกอบต่างๆ ตามที่ได้กล่าวมาข้างต้น สามารถระบุในข้อตกลงการใช้บริการระหว่าง สง. กับบริษัทในเครือหรือบริษัทลูกที่ให้บริการ รวมทั้งแสดงความชัดเจนของรายการธุรกรรมระหว่างบริษัทในเครือ/ในกลุ่ม (Arms-length transaction) **สาระสำคัญของข้อตกลงระหว่างสถาบันการเงินกับผู้ให้บริการที่เป็นบริษัทในเครือหรือบริษัทลูก จะต้องเหมือนกับหรืออย่างน้อยต้องให้ประโยชน์กับสถาบันการเงินเท่ากับข้อตกลงระหว่างสถาบันการเงินกับผู้ให้บริการที่ไม่มีส่วนเกี่ยวข้องกับสถาบันการเงิน**

2.2.2 การคัดเลือกผู้ให้บริการ

<u>สรุปแนวทางการปฏิบัติ</u>

ผู้บริหารควร

- ประเมินข้อเสนอของผู้ให้บริการตามความต้องการของสถาบันการเงิน โดยพิจารณาเทียบสิ่งที่ผู้ให้บริการเสนอกับข้อเสนอชักชวนของสถาบันการเงิน
- ทำการประเมินผู้ให้บริการอย่างถี่ถ้วน
- มีความมั่นใจว่าการเลือกผู้ให้บริการที่เป็นบริษัทในเครือ ดำเนินการภายใต้ลักษณะ arms length และเป็นไปตามที่กฎหมายกำหนด
- ประเมินผู้ให้บริการที่อยู่ต่างประเทศตามแนวทางที่จะกล่าวถึงในส่วนนี้และในภาคผนวก: ผู้ให้บริการภายนอกที่อยู่ต่างประเทศ

หลังจากที่ได้มีการระบุงานที่ต้องดำเนินการและการควบคุมที่จำเป็นแล้ว สถาบันการเงินก็จะยื่นข้อเสนอชักชวนส่งไปให้ผู้ให้บริการต่างๆ ตามรายชื่อที่สถาบันการเงินกำหนด ซึ่งเรียกว่า Request for Proposal (RFP) และจะเป็นสิ่งที่นำไปใช้ในการเจรจาต่อรองสัญญาต่อไป

(1) <u>Request for Proposal</u>

ข้อมูลที่ได้ในขั้นตอนกำหนดความต้องการจะนำมาใช้ในการจัดทำ RFP โดยทั่วไปแล้ว RFP จะระบุถึงวัตถุประสงค์ของสถาบันการเงิน ขอบเขตและลักษณะของงานที่จะดำเนินการ ระดับการให้บริการที่คาดหวัง ระยะเวลาส่งมอบงาน ตัวชี้วัด มาตรการควบคุม นโยบายรักษาความปลอดภัยของสถาบันการเงิน แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง การควบคุมการเปลี่ยนแปลง นอกจากนี้ยังระบุให้ผู้ให้บริการตอบกลับโดยเทียบกับความต้องการที่สถาบันการเงินกำหนด พร้อมทั้งระบุค่าใช้จ่ายมาด้วย ทั้งนี้การจัดทำ RFP อาจมีรายละเอียดที่แตกต่างกันไปตามการจัดซื้อ/จัดหาแต่ละครั้ง

หลังจากที่ผู้บริหารยื่นข้อเสนอชักชวนและมีผู้ให้บริการตอบกลับข้อเสนอดังกล่าวแล้ว สถาบันการเงินควรนำสิ่งที่ผู้ให้บริการเสนอมาประเมินเปรียบเทียบกับความต้องการของสถาบันการเงิน ซึ่งอาจพบว่าข้อเสนอของผู้ให้บริการไม่ตรงกับ RFP ทั้งหมดโดยสมบูรณ์ ตัวอย่างเช่น บริการที่ผู้ให้บริการเสนออาจเกี่ยวข้องกับขั้นตอนการประมวลผลและการรายงาน และใช้สูตรหรือเทคนิคการกำหนดราคา ที่แตกต่างไปจากของสถาบันการเงิน **ซึ่งสถาบันการเงินควรมีการพิจารณาข้อแตกต่างและประเมินผลกระทบที่มีต่อวัตถุประสงค์และความคาดหวังในบริการของสถาบันการเงิน** ทั้งนี้ สถาบันการเงินควรประเมินข้อแตกต่างที่มีนัยสำคัญโดยใช้กระบวนการเช่นเดียวกับที่ใช้ในการจัดทำความต้องการ และ**ควรเจรจากับผู้ให้บริการเพื่อให้ได้แนวทางแก้ไขข้อแตกต่าง ก่อนดำเนินการเจรจาสัญญาต่อไป**

(2) <u>Due Diligence (การประเมินอย่างถี่ถ้วน)</u>

สถาบันการเงินควรประเมินตัวผู้ให้บริการและข้อเสนอตอบกลับ RFP ของผู้ให้บริการอย่างถี่ถ้วน การประเมินอย่างถี่ถ้วนดังกล่าวเป็นเสมือนเครื่องมือตรวจสอบและวิเคราะห์เพื่อให้ความมั่นใจว่าผู้ให้บริการจะสามารถปฏิบัติตามความต้องการของสถาบันการเงินได้ **การประเมินอย่างถี่ถ้วนนี้ควรสามารถยืนยันและประเมินข้อมูลที่เกี่ยวกับผู้ให้บริการ ดังต่อไปนี้**

- ประวัติการดำเนินธุรกิจ
- คุณลักษณะ ประสบการณ์ และชื่อเสียงขององค์กร รวมถึงการตรวจสอบประวัติอาชญากรรม
- บริษัทอื่นที่ใช้บริการคล้ายๆ กับของสถาบันการเงินจากผู้ให้บริการ ที่ได้รับการติดต่อให้เป็นแหล่งอ้างอิง

- ฐานะการเงิน รวมถึงการสอบทานงบการเงินที่ผ่านการตรวจสอบแล้ว
- กลยุทธ์และชื่อเสียง
- ความสามารถในการส่งมอบการให้บริการ สถานะ และความมีประสิทธิผลของสิ่งที่ส่งมอบ
- โครงสร้างทางเทคโนโลยีและระบบงาน
- สภาพแวดล้อมการควบคุมภายใน ประวัติด้านการรักษาความปลอดภัย และขอบเขตของการตรวจสอบ
- การปฏิบัติตามกฎระเบียบทางการ รวมถึงข้อร้องเรียน และการฟ้องร้องดำเนินคดี หรือการต้องโทษจากหน่วยงานภาครัฐ
- การพึ่งพาหรือความเกี่ยวข้องกับผู้ให้บริการที่เป็นบุคคลที่สาม
- ขอบเขตการประกันภัย
- ความสามารถในการปฏิบัติได้ตามข้อกำหนดเรื่องความต่อเนื่องของธุรกิจและการกู้จากเหตุการณ์ภัยพิบัติต่าง ๆ

องค์ประกอบที่สำคัญอีกประการ คือ การตรวจสอบข้อมูลของสิ่งที่จับต้องไม่ได้ เช่น ปรัชญาการให้บริการของบุคคลที่สาม ความคิดริเริ่มทางด้านคุณภาพ และรูปแบบการบริหารงาน ซึ่งวัฒนธรรมองค์กร และรูปแบบการดำเนินธุรกิจควรเข้ากันได้กับของสถาบันการเงิน กรณีที่สถาบันการเงินพิจารณาผู้ให้บริการที่อยู่ต่างประเทศ ควรมีการประเมินตามรายการที่ระบุไว้ข้างต้นและที่ระบุในภาคผนวก: ผู้ให้บริการภายนอกที่อยู่ต่างประเทศ

สถาบันการเงินอาจทำการประเมินดังกล่าว กับผู้ให้บริการมากกว่า 1 ราย ที่ตอบกลับข้อเสนอชักชวนของสถาบันการเงิน ซึ่งความละเอียดหรือรูปแบบของการประเมินที่เป็นทางการจะต้องดำเนินการมากหรือน้อย ขึ้นอยู่กับความเสี่ยงของการใช้บริการจากภายนอก ความคุ้นเคยกับผู้ให้บริการ และขั้นตอนการคัดเลือกผู้ให้บริการ

หลังจากที่สถาบันการเงินได้ออก RFP ไปให้ผู้ให้บริการ และได้รับคำตอบกลับของผู้ให้บริการ พร้อมทั้งทำการประเมินอย่างถี่ถ้วนแล้ว ก็จะเข้าสู่ขั้นตอนการเจรจาเรื่องสัญญากับผู้ให้บริการซึ่งอาจจะมีมากกว่า 1 ราย ที่สถาบันการเงินพิจารณาแล้วว่าจะสามารถให้บริการได้ตรงกับความต้องการของตนมากที่สุด

2.2.3 ประเด็นเกี่ยวกับสัญญา

สรุปแนวทางการปฏิบัติ

ก่อนลงนามในสัญญา ผู้บริหารควร

- มีความมั่นใ จว่าสัญญาได้ระบุขอบเขตงาน สิทธิและความรับผิดชอบของคู่สัญญาแต่ละฝ่ายไว้อย่างชัดเจน ในระดับที่เหมาะสมรวมถึงข้อยกเว้น หรือเงื่อนไขของแต่ละฝ่าย
- มีความมั่นใจว่าสัญญาครอบคลุมข้อตกลงของระดับการให้บริการ (Service Level Agreement) อย่างเพียงพอและสามารถวัดได้ทั้งเชิงปริมาณและคุณภาพ
- มีความมั่นใจว่าสัญญากับบริษัทในเครือมีความชัดเจนสะท้อนความสัมพันธ์ในลักษณะของบริษัทในกลุ่มหรือบริษัทในเครือ (Arms-length) รวมถึงค่าใช้จ่ายและการให้บริการที่ให้ประโยชน์กับ สง. เสมือนกับคู่สัญญาไม่ได้มีส่วนเกี่ยวข้องกับ สง.
- เลือกวิธีกำหนดราคาที่เหมาะสมกับความต้องการของ สง
- มีความมั่นใจว่าสัญญาไม่มีข้อกำหนดหรือการชักนำใดๆ ที่อาจส่งผลกระทบในทางลบอย่างมีนัยสำคัญต่อ สง
- มอบหมายให้ที่ปรึกษาทางกฎหมายสอบทานสัญญาก่อน
- ประเมินผู้ให้บริการภายนอกที่เป็นนิติบุคคลต่างประเทศตามแนวทางที่จะกล่าวในส่วนนี้และในภาคผนวก: ผู้ให้บริการภายนอกที่อยู่ต่างประเทศ
- มีการกำหนดระดับของการให้บริการที่ชัดเจน ระบุตัววัด บทปรับ บทลงโทษ หากการให้บริการไม่เป็นไปตามสัญญา

หลังจากที่ได้ทำการเลือกบริษัทผู้ให้บริการแล้ว ผู้บริหารของ สง. ควรเจรจาต่อรองให้เงื่อนไขสัญญาตรงกับความต้องการของตน RFP และข้อเสนอตอบกลับของผู้ให้บริการสามารถนำมาใช้ในกระบวนการนี้ สัญญาเป็นเอกสารที่มีผลผูกพันทางกฎหมายที่ระบุแง่มุมทั้งหมดของการให้บริการระหว่างคู่สัญญา ซึ่งควรมีการจัดทำเป็นลายลักษณ์อักษร ทั้งนี้รวมถึงใน**กรณีที่ให้บริษัทในเครือของ สง เป็นผู้ให้บริการด้วย โดย สง ควรพิจารณาดูแลเรื่องค่าใช้จ่ายและคุณภาพของบริการเสมือนว่า สง. ดำเนินการกับผู้ให้บริการที่ไม่มีส่วนเกี่ยวข้องกับ สง.** เนื่องจากสัญญาจัดเป็นเครื่องมือควบคุมหนึ่งที่สำคัญในกระบวนการใช้บริการจากภายนอก ดังนั้น ผู้บริหารควร

- ตรวจสอบความถูกต้องของรายละเอียดในสัญญาโดยตัวแทนหรือฝ่ายที่เกี่ยวข้อง

- พิจารณาให้มั่นใจว่าสัญญาระบุเป็นลายลักษณ์อักษรอย่างชัดเจนและครอบคลุมรายละเอียดที่แสดงสิทธิและความรับผิดชอบของคู่สัญญาแต่ละฝ่ายอย่างครบถ้วน

- ให้หน่วยงานด้านกฎหมายหรือที่ปรึกษาทางกฎหมายเข้ามามีส่วนเกี่ยวข้องในกระบวนการตั้งแต่เริ่มต้นเพื่อช่วยจัดเตรียมและสอบทานร่างสัญญาของผู้ให้บริการ

ตัวอย่างขององค์ประกอบที่ควรกำหนดไว้ในสัญญา

ขอบเขตของบริการ สัญญาควรระบุรายละเอียดถึงสิทธิและความรับผิดชอบของคู่สัญญาแต่ละฝ่าย โดยควรพิจารณาให้ครอบคลุมเรื่อง ดังต่อไปนี้

- รายละเอียดของกิจกรรมที่ต้องดำเนินการ ระยะเวลาในการดำเนินการ และการมอบหมายความรับผิดชอบ ซึ่งข้อกำหนดในการดำเนินการควรครอบคลุมระบบงานที่ใช้อยู่ในปัจจุบันและระบบงานอื่นที่เกี่ยวข้องซึ่งจะถูกพัฒนาโดยผู้ให้บริการรายอื่น (เช่น ระบบอินเตอร์เน็ตแบงกิ้ง ที่มีการใช้งานร่วมกับระบบงานหลักหรือระบบที่ได้รับการแก้ไขอื่นๆ)

- ข้อบังคับ และบริการที่ต้องดำเนินการโดยผู้ให้บริการ ได้แก่ การสนับสนุนและบำรุงรักษาระบบงาน การฝึกอบรมพนักงาน หรือบริการลูกค้า

- ข้อบังคับของ สง.

- สิทธิของคู่สัญญาในการเปลี่ยนแปลงแก้ไขบริการที่ใช้อยู่ในปัจจุบันภายใต้สัญญา[1]

- แนวทางสำหรับการเพิ่ม บริการใหม่หรือบริการอื่น และแนวทางสำหรับการเจรจาสัญญาใหม่

มาตรฐานการดำเนินงาน สัญญาควรระบุถึงมาตรฐานการดำเนินงานโดยกำหนดระดับการให้บริการขั้นต่ำและแนวทางปรับปรุงแก้ไขให้ได้ตามมาตรฐาน ตัวอย่าง เช่น Percent System Uptime ระยะเวลาการประมวลผล Batch จำนวนความผิดพลาดของการประมวลผล เป็นต้น ซึ่งอาจให้มาตรฐานของอุตสาหกรรมเป็นระดับอ้างอิงก็ได้ สง. ควรสอบทานมาตรฐานการดำเนินงานเป็นประจำเพื่อให้มั่นใจว่ายังคงสามารถปฏิบัติได้ตามเป้าหมายและวัตถุประสงค์ โปรดอ่านรายละเอียดเกี่ยวกับข้อตกลงของระดับการให้บริการที่จะกล่าวในส่วนถัดไป

[1] สง. อาจเห็นว่าการทำสัญญามากกว่า 3 ปี จะทำให้เกิดข้อได้เปรียบในแง่ของค่าใช้จ่ายในการจัดทำสัญญาและค่าใช้จ่ายในการเปลี่ยนแปลงผู้ให้บริการ รวมทั้งในเรื่องของราคาที่ผู้ให้บริการอาจเสนอให้ได้ดีกว่า เนื่องจากสภาพแวดล้อมของเทคโนโลยีสารสนเทศเปลี่ยนแปลงอย่างรวดเร็ว ดังนั้น สัญญาควรมีความยืดหยุ่นต่อสถานการณ์ต่างๆ นอกจากนั้น สัญญาควรยืดหยุ่นต่อการเปลี่ยนแปลงระดับการให้บริการ การเพิ่มหรือลดขอบเขตของกระบวนการดำเนินงาน บริการ หรือระบบงานที่เกิดจากการเปลี่ยนแปลง เป้าหมายและวัตถุประสงค์ของ สง. รวมทั้งการปรับเป้าหมายรายปีขององค์ประกอบต่างๆ ที่เกี่ยวข้อง

การรักษาความปลอดภัยและความลับ สัญญาควรระบุถึงความรับผิดชอบของผู้ให้บริการในการรักษาความปลอดภัยและความลับของทรัพยากรของ สง. เช่น ข้อมูล เครื่องและอุปกรณ์คอมพิวเตอร์ เป็นต้น ข้อตกลงควรห้ามผู้ให้บริการ ซึ่งรวมถึงตัวแทนของผู้ให้บริการใช้หรือเปิดเผยข้อมูลของ สง. เว้นแต่มีความจำเป็นหรือเป็นไปตามข้อกำหนดในสัญญา และสัญญาควรปกป้องการใช้งานโดยไม่ได้รับอนุญาต เช่น การเปิดเผยข้อมูลให้กับบริษัทคู่แข่ง เป็นต้น ถ้าผู้ให้บริการได้รับข้อมูลส่วนบุคคลของลูกค้าของ สง. ซึ่งเป็นข้อมูลที่ไม่ได้เปิดเผยต่อสาธารณะ สง. ควรตรวจสอบให้แน่ใจว่าผู้ให้บริการปฏิบัติตามกฎมายส่วนบุคคลและที่เกี่ยวข้องต่างๆ ทั้งหมด สง. ควรกำหนดให้ผู้ให้บริการเปิดเผยการละเมิดระบบรักษาความปลอดภัยทั้งหมดที่ก่อให้เกิดการบุกรุกเข้าไปถึงทรัพย์สินของผู้ให้บริการโดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อ สง. และลูกค้า ผู้ให้บริการควรรายงานต่อ สง. เมื่อมีเหตุการณ์บุกรุกเกิดขึ้น รวมถึงผลกระทบต่อ สง. และแนวทางแก้ไข

การควบคุม ผู้บริหารควรพิจารณาวิธีการดำเนินการตามข้อตกลงของสัญญาซึ่งครอบคลุมการควบคุม ดังต่อไปนี้

- การควบคุมภายในของผู้ให้บริการ
- การปฏิบัติตามข้อกำหนดของกฎหมาย
- ข้อตกลงในการบำรุงรักษาข้อมูลสำหรับผู้ให้บริการ
- การเข้าถึงข้อมูลโดย สง.
- ข้อตกลงในการแจ้งและสิทธิในการอนุมัติการเปลี่ยนแปลงของบริการระบบงาน และการควบคุม บุคลากรหลักของโครงการ และสถานที่ให้บริการ ที่สำคัญ
- การกำหนดและติดตามค่าพารามิเตอร์สำหรับงานด้านการเงิน เช่น การประมวลผลรายการชำระเงิน หรือการขยายสินเชื่อ ซึ่งผู้ให้บริการดำเนินการแทน สง.
- ขอบเขตของการประกันภัยซึ่งดำเนินการโดยผู้ให้บริการ

การตรวจสอบ สง. ควรระบุประเภทของรายงานตรวจสอบที่ควรได้รับไว้ในสัญญาด้วย เช่น รายงานการตรวจสอบด้านการเงิน การควบคุม และรายงานการสอบทานระบบรักษาความปลอดภัย เป็นต้น สัญญาควรระบุความถี่ของการตรวจสอบ ค่าใช้จ่ายในการตรวจสอบ และสิทธิของ สง. และหน่วยงานกำกับดูแลทางการที่จะได้รับผลการตรวจสอบในระยะเวลาที่เหมาะสม นอกจากนั้นสัญญาควรระบุถึงสิทธิในการได้รับเอกสารประกอบการแก้ไขตามข้อสังเกตของผู้ตรวจสอบ และสิทธิในการเข้าตรวจสอบสถานที่ อุปกรณ์ เครื่องมือต่างๆ ที่ใช้ในการประมวลผลและการปฏิบัติงานของผู้ให้บริการ ผู้บริหารควรใช้กระบวนการประเมินความเสี่ยงในการพิจารณาว่าการตรวจสอบภายในของผู้ให้บริการมีความน่าเชื่อถือและเพียงพอ รวมทั้งพิจารณาความจำเป็นที่จะต้องมีการตรวจสอบหรือสอบทานโดยผู้ตรวจสอบอิสระ

สำหรับบริการที่เกี่ยวข้องกับการเข้าถึงเครือข่ายที่เป็นระบบเปิด (Open networks) เช่น อินเตอร์เน็ต ผู้บริหารควรให้ความสนใจในเรื่องการรักษาความปลอดภัยเป็นพิเศษ สัญญาควรกำหนดให้มีการสอบทานการควบคุมโดยอิสระอย่างต่อเนื่องเป็นประจำ ได้แก่ การทดสอบเจาะระบบ การตรวจจับการบุกรุก การสอบทานค่าติดตั้ง Firewall และการสอบทานการควบคุมโดยอิสระอื่นๆ สง. ควรได้รับรายงานผลการตรวจสอบ/ สอบทานโดยละเอียดเพื่อประเมินระบบรักษาความปลอดภัยของผู้ให้บริการ

การรายงาน เงื่อนไขสัญญาควรครอบคลุมความถี่และประเภทของรายงานที่ สง. ควรได้รับ เช่น รายงานผลการดำเนินงาน การตรวจสอบการควบคุม งบการเงิน การรักษาความปลอดภัย รายงานทดสอบการกู้ธุรกิจกลับคืนสู่สภาพปกติ เป็นต้น สัญญาควรกล่าวถึงแนวทางและค่าใช้จ่ายของการได้รับรายงานดังกล่าวด้วย

แผนการกู้ธุรกิจกลับคืนสู่สภาพปกติและแผนสำรองฉุกเฉิน สัญญาควรระบุความรับผิดชอบของผู้ให้บริการในการสำรองและปกป้องข้อมูลซึ่งรวมถึงอุปกรณ์ โปรแกรมและไฟล์ข้อมูล และการบำรุงรักษาแผนกู้ระบบงานจากภัยพิบัติและแผนสำรองฉุกเฉิน สัญญาควรกำหนดความรับผิดชอบของผู้ให้บริการในการทดสอบแผนเป็นประจำและรายงานผลการทดสอบให้ สง. รับทราบ ในการทดสอบแผนกู้ธุรกิจกลับคืนสู่สภาพปกติ สง. ควรพิจารณาประเด็นเกี่ยวกับการพึ่งพาผู้ให้บริการหลายราย ผู้ให้บริการควรจัดส่งสำเนาแผนสำรองฉุกเฉินที่ระบุขั้นตอนการปฏิบัติงานภายใต้สภาวการณ์ฉุกเฉินให้กับ สง. ด้วย ซึ่งสัญญาควรกำหนดระยะเวลาที่ใช้ในการกู้ธุรกิจกลับคืนสู่สภาวะปกติที่เป็นไปตามข้อตกลงทางธุรกิจของ สง. และ สง. ควรมีความมั่นใจว่าสัญญาจะไม่มีข้อกำหนดใดๆ ที่จะยกเว้นผู้ให้บริการในการใช้แผนสำรองฉุกเฉิน

การทำสัญญารับจ้างช่วงงานต่อและความสัมพันธ์กับผู้ให้บริการหลายราย ในการให้บริการแก่ สง. **ผู้ให้บริการอาจจัดทำสัญญากับบุคคลที่สาม ซึ่งผู้ให้บริการต้องแจ้งให้ สง. รับทราบและอนุมัติการทำสัญญารับจ้างช่วงงานต่อทุกกรณีที่เกี่ยวข้อง** ในสัญญาควรมีการกำหนดผู้ให้บริการหลัก เพื่อรับหน้าที่และความรับผิดชอบต่อ สง. นอกจากนั้นควรระบุไว้ด้วยว่าผู้ให้บริการหลักมีความรับผิดชอบต่อบริการที่ระบุไว้ในสัญญาโดยไม่คำนึงว่าใครเป็นผู้ดำเนินการ สง. ควรกำหนดให้มีการแจ้งและอนุมัติการเปลี่ยนแปลงผู้รับจ้างช่วงงานต่อของผู้ให้บริการด้วย

ค่าใช้จ่าย สัญญาควรอธิบายรายละเอียดเกี่ยวกับการคำนวณค่าใช้จ่ายของบริการขั้นพื้นฐาน ได้แก่ การพัฒนา การเปลี่ยนแปลง การบริการต่อเนื่อง เป็นต้น รวมทั้งค่าใช้จ่ายที่ขึ้นอยู่กับปริมาณของกิจกรรมหรือค่าใช้จ่ายสำหรับคำขอพิเศษ สัญญาควรระบุความรับผิดชอบและค่าใช้จ่ายส่วนเพิ่มที่เกิดจากการซื้อและการบำรุงรักษาอุปกรณ์และระบบงาน เงื่อนไขที่ทำให้โครงสร้าง

ค่าใช้จ่ายเปลี่ยนแปลงไปควรมีระบุไว้ในสัญญาโดยละเอียด รวมถึงเพดานจำกัดการเพิ่มค่าใช้จ่ายด้วย โปรดอ่านส่วนวิธีการกำหนดราคาและการรวมกลุ่มของบริการในหน้า 19-20

ความเป็นเจ้าของและลิขสิทธิ์ สัญญาควรระบุความเป็นเจ้าของ สิทธิ และการได้รับอนุญาตให้ใช้งานข้อมูล อุปกรณ์ เอกสารประกอบระบบงาน ระบบปฏิบัติการ โปรแกรมระบบงาน และสิทธิในทรัพย์สินทางปัญญาอื่นๆ เช่น ชื่อ สัญลักษณ์ของบริษัท เครื่องหมายการค้า ลิขสิทธิ์อื่น Domain Name รูปแบบของ Web Site ผลิตภัณฑ์ที่พัฒนาโดยผู้ให้บริการเพื่อ สง. ในกรณีข้อมูลของ สง. ความเป็นเจ้าของข้อมูลจะต้องเป็นของ สง.

อายุของสัญญา หากมีการเจรจาในเรื่องของอายุสัญญาและการต่ออายุสัญญา สง. ควรพิจารณาประเภทของเทคโนโลยีและสถานะของอุตสาหกรรมในปัจจุบัน ในขณะที่สัญญาที่ครอบคลุมระยะเวลายาวอาจให้ประโยชน์หลายอย่าง แต่การเปลี่ยนแปลงของเทคโนโลยีที่เป็นไปอย่างรวดเร็วอาจทำให้การพิจารณาจัดทำสัญญาที่ครอบคลุมในช่วงเวลาสั้นกว่ามีความเหมาะสมกว่า อย่างไรก็ตาม สง. ควรพิจารณากำหนดระยะเวลาที่เหมาะสมในการแจ้งเรื่องการไม่ต่ออายุสัญญาก่อนวันหมดอายุของสัญญา สง. ควรพิจารณาวันหมดอายุสัญญาของบริการอื่นที่เกี่ยวข้องด้วย เช่น บริการ Web Site บริการระบบสื่อสารโทรคมนาคม งานเขียนโปรแกรม งานสนับสนุนระบบเครือข่าย เป็นต้น โดยให้มีความสอดคล้องกัน เพื่อลดความเสี่ยงในการยกเลิกสัญญาก่อนหมดอายุและการเสียค่าปรับที่สืบเนื่องจากการยกเลิกสัญญาของบริการอื่น

การแก้ไขข้อพิพาท สัญญาควรมีข้อกำหนดเกี่ยวกับกระบวนการแก้ไขกรณีพิพาทอย่างรวดเร็วและข้อกำหนดเกี่ยวกับความต่อเนื่องของการให้บริการในช่วงที่มีกรณีพิพาท

การชดใช้ความเสียหาย ข้อกำหนดเกี่ยวกับการชดใช้ความเสียหายควรระบุให้ผู้ให้บริการไม่กระทำการใดๆ รวมทั้งเปิดเผยความลับ ที่ทำให้ สง. เกิดความเสียหายอันเนื่องมาจากความตั้งใจหรือประมาทเลินเล่อของผู้ให้บริการ ที่ปรึกษาทางกฎหมายควรสอบทานข้อกำหนดนี้เพื่อให้มั่นใจว่า สง. จะไม่ตกอยู่ในภาวะที่ต้องรับผิดชอบต่อความเสียหายซึ่งเป็นผลมาจากความตั้งใจหรือประมาทของผู้ให้บริการ

ขีดจำกัดของความรับผิดชอบต่อความเสียหาย สัญญามาตรฐานของผู้ให้บริการบางรายอาจระบุให้มีการจำกัดความรับผิดชอบต่อความเสียหายที่เกิดจากผู้ให้บริการ ซึ่งผู้บริหารของ สง.. ควรประเมินความเพียงพอของขีดจำกัดที่กำหนดต่อผลขาดทุนของ สง. ที่อาจเกิดจากความล้มเหลวในการปฏิบัติตามข้อตกลงของผู้ให้บริการ

การยกเลิกสัญญา ผู้บริหารควรประเมินระยะเวลาและค่าใช้จ่ายของการยกเลิกสัญญา สิทธิในการยกเลิกอาจแตกต่างกันไปตามบริการต่างๆ สัญญาควรระบุสิทธิในการยกเลิกสำหรับกรณีต่างๆ ได้แก่ การเปลี่ยนแปลงการควบคุม (ที่สืบเนื่องจากการควบรวมกิจการ) การเปลี่ยนแปลงในการ

อำนวยความสะดวก ค่าใช้จ่ายที่เพิ่มขึ้น การที่ไม่สามารถปฏิบัติได้ตามระดับการให้บริการบ่อยครั้ง ความล้มเหลวในการให้บริการที่สำคัญ การล้มละลาย การปิดกิจการ และความไม่สามารถชดใช้หนี้สินได้ สัญญาควรกำหนดระยะเวลาและการแจ้งสำหรับกรณีดังกล่าวอย่างเพียงพอเพื่อให้สามารถโอนถ่ายงาน คืนข้อมูลและทรัพยากรอื่นๆในรูปของ Machine Readable Format รวมทั้ง Knowledge Transfer กลับมาให้ สง. ได้ทันเวลา ซึ่งควรมีการระบุค่าใช้จ่ายไว้อย่างชัดเจนด้วย

การโอนสิทธิ สัญญาควรห้ามมิให้มีการโอนสัญญาไปให้บุคคลอื่นหากไม่ได้รับการยินยอมจาก สง. ข้อกำหนดดังกล่าวควรครอบคลุมกรณีเปลี่ยนแปลงผู้รับจ้างช่วงงานต่อด้วย

ผู้ให้บริการที่เป็นนิติบุคคลต่างประเทศ สัญญาควรครอบคลุมประเด็นและข้อกำหนดเพิ่มเติม โปรดอ่านในภาคผนวก: ผู้ให้บริการภายนอกที่อยู่ต่างประเทศ

การปฏิบัติตามกฎหมาย สัญญาที่ทำกับผู้ให้บริการควรครอบคลุมข้อตกลงการให้บริการที่ถูกต้องตามกฎหมายและแนวทางของทางการ โดยผู้ให้บริการจะต้องยอมรับที่จะให้ข้อมูลที่ถูกต้องและให้หน่วยงานที่กำกับดูแลของทางการสามารถเข้าถึงข้อมูลได้ในระยะเวลาที่เหมาะสมโดยขึ้นอยู่กับประเภทและระดับของการให้บริการที่เสนอต่อ สง.

(1) <u>ข้อตกลงของระดับการให้บริการ (Service Level Agreements- SLAs)</u>

ข้อตกลงของระดับการให้บริการเป็นเอกสารทางการที่ระบุถึงข้อตกลงในการให้บริการ เป้าหมาย หรือบทลงโทษหากปฏิบัติไม่ได้ตามเป้าหมายที่ได้มีการตกลงกันไว้ล่วงหน้าระหว่างคู่สัญญา สง. ควรจัดทำ SLA ให้เชื่อมโยงกับเป้าหมาย บทลงโทษ หรือบทปรับ การยกเลิกสัญญา เพื่อปกป้องประโยชน์ของ สง ในกรณีที่ผู้ให้บริการไม่สามารถปฏิบัติตามข้อตกลง

ในการพัฒนา SLA ผู้บริหารควรเริ่มจากการระบุองค์ประกอบของบริการที่สำคัญซึ่งควรสัมพันธ์กับงาน เช่น อัตราของการประมวลผลผิดพลาด System up-time (ระยะเวลาการทำให้ระบบกลับมาทำงานได้ตามปกติ) เป็นต้น หรืออาจจะเป็นเรื่องในแง่การบริหารองค์กร เช่น อัตราการลาออกของพนักงาน เป็นต้น หลังจากที่ระบุองค์ประกอบของบริการได้แล้ว ผู้บริหารควรกำหนดวิธีการวัดผลการดำเนินงานขององค์ประกอบเหล่านั้นอย่างเที่ยงธรรม รวมทั้งกำหนดความถี่ของการวัดผลและช่วงระดับของผลการดำเนินงานที่ยอมรับได้ เพื่อใช้เป็นดัชนีชี้ว่าผู้ให้บริการปฏิบัติตามข้อตกลงได้หรือไม่

ถึงแม้ว่า มาตรฐานการดำเนินงานแต่ละเรื่องอาจแตกต่างกันไปขึ้นอยู่กับลักษณะของบริการที่ส่งมอบ ผู้บริหารควรพิจารณา SLA ให้ครอบคลุมประเด็น ดังต่อไปนี้

- ความพร้อมใช้ของบริการและความเหมาะสมของระยะเวลาการให้บริการ
- ความลับและความถูกต้องเชื่อถือได้ของข้อมูล
- การควบคุมการเปลี่ยนแปลง

- การปฏิบัติตามมาตรฐานการรักษาความปลอดภัย รวมถึงการจัดการจุดอ่อนและการเจาะระบบรักษาความปลอดภัย

- การปฏิบัติตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

- การช่วยเหลือสนับสนุน (Help desk support)

เงื่อนไขของ SLA ที่เกี่ยวกับความต่อเนื่องของธุรกิจควรสามารถวัดความรับผิดชอบตามสัญญาของผู้ให้บริการในการสำรองข้อมูล การเก็บรักษาข้อมูล การป้องกันข้อมูล การบำรุงรักษา แผนกู้ระบบและแผนสำรองฉุกเฉิน เงื่อนไขใน SLA ควรสามารถทดสอบข้อกำหนดในเรื่องของระยะเวลาในการกู้ธุรกิจกลับคืนสู่สภาวะปกติ และควรมีการทดสอบแผนเป็นประจำ สัญญาหรือ SLA ไม่ควรยกเว้นผู้ให้บริการจากการใช้แผนสำรองฉุกเฉิน (สัญญาว่าจ้างผู้ให้บริการภายนอกควรระบุให้ครอบคลุมถึงเหตุการณ์ที่ไม่คาดคิดซึ่ง สง. ไม่ได้ดำเนินการเตรียมการไว้)

(2) <u>วิธีการกำหนดราคา</u>

สง. ควรมีทางเลือกหลายๆ ทางในการกำหนดราคาของการใช้บริการภายนอก ผู้บริหารควรพิจารณาทางเลือกในการกำหนดราคาต่างๆ เหล่านั้น และเลือกใช้วิธีที่เหมาะสมกับแต่ละสัญญา ตัวอย่างของวิธีการกำหนดราคา มีดังนี้

- Cost plus – ผู้ให้บริการรับชำระค่าใช้จ่ายที่เกิดขึ้นจริง พร้อมกับส่วนต่างของผลกำไรที่ได้มีการตกลงไว้ล่วงหน้า หรือราคาส่วนเพิ่ม (Markup) (ซึ่งมักจะเป็นร้อยละของค่าใช้จ่ายจริง) ตัวอย่างเช่น ผู้ให้บริการพัฒนา Web Site ด้วยค่าใช้จ่าย $5,000 บวก ส่วนเพิ่ม 10% ดังนั้น สง. ชำระ $5,500

- Fixed price – ราคาที่ผู้ให้บริการกำหนดในแต่ละรอบเท่ากันตลอดอายุสัญญา ข้อดีของวิธีนี้คือ สง. มีความแน่ชัดในค่าใช้จ่ายของแต่ละเดือน แต่ สง. จะต้องกำหนดขอบเขตของบริการหรือกระบวนการที่เพียงพอเพื่อไม่ให้เกิดปัญหาขึ้น ผู้ให้บริการมักจะคิดค่าใช้จ่ายเพิ่มเติมสำหรับบริการที่ให้อยู่นอกเหนือขอบเขตที่กำหนด ตัวอย่างเช่น ผู้ให้บริการคิดค่าใช้จ่ายในการบำรุงรักษา Web Site $500 ต่อเดือน ซึ่งหาก สง. ต้องการเพิ่ม link ผู้ให้บริการอาจคิดค่าใช้จ่ายเพิ่มเนื่องจากบริการดังกล่าวไม่ได้กำหนดไว้ชัดเจนในสัญญา

- Unit pricing – ราคาที่ผู้ให้บริการกำหนดตามอัตราหนึ่งของการใช้บริการ และ สง. จ่ายตามการใช้งานจริง ตัวอย่าง ถ้า สง. จ่าย $0.10 ต่อการเรียกใช้งาน Web Site และในเดือนนี้ Web Site ดังกล่าว มีการเรียกใช้งาน 5,000 ครั้งต่อเดือน ดังนั้น สง. จ่าย $500 สำหรับเดือนดังกล่าว

- Variable pricing – ผู้ให้บริการกำหนดราคาของบริการตามตัวแปร เช่น ความพร้อมใช้ของระบบงาน ตัวอย่างเช่น ผู้ให้บริการคิดค่าใช้จ่าย $500, $600 และ $800 ต่อเดือน

สำหรับอัตราความพร้อมใช้งานของระบบที่ 99.00, 99.50 และ 99.75 ตามลำดับ ถ้าในรอบระยะเวลาเรียกเก็บเงิน Web Site มีความพร้อมใช้อยู่ที่ 99.80% สง. จะต้องจ่าย $800

- Incentive-based pricing – การกำหนดเป้าหมายเพื่อกระตุ้นให้ผู้ให้บริการปฏิบัติงานที่ระดับสูงสุดโดยการให้โบนัสสำหรับการมีผลการดำเนินงานที่ดี แต่ผู้ให้บริการจะได้ลดลงหากผลการดำเนินงานไม่ได้ตามระดับที่ยอมรับได้ ตัวอย่างเช่น สง. ต้องการผู้ให้บริการพัฒนา Web Site ซึ่งผู้ให้บริการตกลงที่จะใช้เวลา 90 วัน โดยคิดค่าใช้จ่าย $5,000 แต่ถ้าผู้ให้บริการสามารถทำได้ภายใน 45 วัน สง.จะจ่าย $6,500 และถ้าผู้ให้บริการไม่สามารถทำได้เสร็จภายใน 90 วัน สง.จะจ่าย $3,500

- Future price change - ผู้ให้บริการจะระบุข้อกำหนดที่อาจมีการเพิ่มค่าใช้จ่ายในอนาคตไม่ว่าจะเป็นการเพิ่มในรูปอัตราร้อยละหรือจำนวน และสง. บางแห่งอาจกำหนดสถานการณ์ที่จะมีการลดราคา เช่น ค่าอุปกรณ์ลดลง เป็นต้น

(3) <u>การรวมกลุ่มของบริการ (Bundling)</u>

ผู้ให้บริการอาจชักจูงให้ สง. ซื้อระบบงาน กระบวนการดำเนินงาน หรือบริการมากกว่า 1 อย่าง โดยคิดราคาเดียว เรียกว่า Bundling ลักษณะดังกล่าวส่งผลให้ สง. ได้รับใบเสร็จรับเงินรวม 1 ใบ ซึ่งอาจจะไม่ได้ระบุราคาของแต่ละระบบงาน กระบวนการปฏิบัติงาน หรือบริการ ถึงแม้ว่าลักษณะของการรวมบริการดังกล่าวจะมีราคาถูกกว่า แต่ สง. อาจจะไม่สามารถวิเคราะห์ค่าใช้จ่ายแยกสำหรับแต่ละบริการได้ และการรวมกลุ่มของบริการ อาจครอบคลุมกระบวนการดำเนินงานและบริการที่ สง. ไม่ต้องการใช้งาน รวมทั้ง สง. อาจไม่สามารถยกเลิกระบบงาน กระบวนการ หรือบริการเฉพาะอย่าง ถ้าจะยกเลิกบางระบบ ก็ต้องมีการเจรจาต่อรองสัญญาใหม่ทั้งหมด

(4) <u>การหลบเลี่ยงด้วยเงื่อนไขของสัญญา</u>

สง. ไม่ควรลงนามในสัญญาการว่าจ้างบริการที่มีเงื่อนไขหลบเลี่ยงอันจะส่งผลกระทบในทางลบต่อ สง. เช่น การขยายระยะเวลา (มากกว่า 10 ปี) การเพิ่มค่าใช้จ่ายหลังจาก 2-3 ปีแรก และ/หรือค่าปรับจากการยกเลิกสัญญา นอกจากนี้ สัญญาบริการบางอย่างแฝงการหลบเลี่ยงที่ไม่เหมาะสมอันเป็นผลทำให้ สง. ต้องรักษาหรือเพิ่มเงินทุนโดยการทยอยรับรู้ผลประกอบการที่ขาดทุนหรือหลีกเลี่ยงการรับรู้เป็นค่าใช้จ่ายโดยทันที ซึ่งจะส่งผลให้ สง. มีปัญหาเรื่องเงินกองทุน

การหลบเลี่ยงสามารถทำได้หลายรูปแบบ เช่น

- ผู้ให้บริการซื้อทรัพย์สิน เช่น อุปกรณ์คอมพิวเตอร์ หรือ ทรัพย์สินรอการขาย เป็นต้น หรือซื้อหุ้นทุนจาก สง. ตามมูลค่าทางบัญชี ซึ่งมากกว่ามูลค่าทางตลาด

- ผู้ให้บริการเสนอให้เงินพิเศษแก่ สง. หลังจากที่ปฏิบัติตามข้อตกลงเสร็จสิ้น

- ผู้ให้บริการเสนอจ่ายเงินสดล่วงหน้าแก่ สง. โดยในสัญญาระบุว่า สง. จะได้รับประโยชน์ในการใช้สิทธิดังกล่าวเพื่อการประหยัดค่าใช้จ่าย หรือแต่งผลกำไรที่ให้โอกาส สง. ทยอยรับรู้ในอนาคตเสมือนว่าการปฏิบัติงานมีประสิทธิภาพสูงขึ้น และก็ไม่ได้มีการกำหนดเกณฑ์วัดที่สามารถอ้างอิงได้ชัดเจน

- การไม่รับรู้ค่าใช้จ่ายที่เกิดจากการเปลี่ยน/ ถ่าย/ โอน (Conversion) หรือค่าใช้จ่ายในการประมวลผลเป็นค่าใช้จ่ายในทันที

- การคิดค่าใช้จ่ายในการติดตั้งและการเปลี่ยน/ ถ่าย/ โอน (Conversion) ต่ำโดยแลกกับค่าใช้จ่ายในการสนับสนุนและการบำรุงรักษาระบบงานในอนาคต

จะเห็นได้ว่าการหลีกเลี่ยงอาจให้ประโยชน์ในระยะสั้นแก่ สง. แต่ผู้ให้บริการมักจะเอาทุนคืนโดยการคิดค่าใช้จ่ายเพิ่มเติมสำหรับบริการประมวลผล ซึ่งอาจส่งผลกระทบต่อฐานะการเงินของ สง. ในระยะยาว นอกจากนั้น สง. ควรตระหนักประเด็นการหลีกเลี่ยงดังกล่าวตามมาตรฐานการบัญชี และข้อกำหนดของทางการ

ดังนั้น เมื่อมีการเจรจาต่อรองสัญญา สง. ควรมั่นใจได้ว่าผู้ให้บริการจะสามารถปฏิบัติตามระดับการให้บริการที่ตรงกับความต้องการของ สง. ตลอดอายุของสัญญา สง. ควรดูแลการบันทึกบัญชีที่เกี่ยวข้องกับสัญญาให้เป็นไปตามมาตรฐานการบัญชี การจัดทำสัญญาให้มีค่าใช้จ่ายของบริการที่สูงเกินไป หรือการไม่บันทึกบัญชีอย่างเหมาะสมถือเป็นการปฏิบัติที่ไม่ถูกต้องและไม่น่าเชื่อถือ ซึ่ง สง. ควรดูแลให้มั่นใจว่าการบันทึกบัญชีตามข้อตกลงในสัญญาสะท้อนความมีนัยสำคัญของธุรกรรม ไม่ใช่เพียงแค่ถูกต้องตามรูปแบบของการลงบัญชีเท่านั้น

2.2.4 การติดตามอย่างต่อเนื่อง

<u>สรุปแนวทางปฏิบัติ</u>

ผู้บริหารควรติดตามผลการดำเนินงานของผู้ให้บริการและการเปลี่ยนแปลงความต้องการของ สง. ที่อาจเกิดขึ้นตลอดอายุของสัญญา การติดตามควรครอบคลุมเรื่อง ดังต่อไปนี้

- SLA ที่สำคัญ และข้อกำหนดในสัญญา
- ฐานะการเงินของผู้ให้บริการ
- สภาพแวดล้อมการควบคุมทั่วไปของผู้ให้บริการ โดยดูจากรายงานตรวจสอบและรายงานสอบทานการควบคุมของผู้ให้บริการ
- การเปลี่ยนแปลงสภาพแวดล้อมภายนอกที่อาจเกิดขึ้น

สง. ควรมีการติดตามดูแลเพื่อให้มั่นใจว่าผู้ให้บริการสามารถส่งมอบบริการให้ได้ตามคุณภาพและปริมาณตามที่สัญญากำหนดและเพื่อใช้เป็นข้อมูลในการปรับปรุง SLA ต่อไป การติดตามควรครอบคลุมเรื่องที่เป็นเป้าหมายของการใช้บริการภายนอกโดยการใช้เทคนิคการติดตามที่มีประสิทธิภาพ ได้แก่ การควบคุมการรักษาความปลอดภัย ความแข็งแกร่งทางการเงิน ผลกระทบของเหตุการณ์ภายนอก ระดับของเครื่องมือและบุคลากรที่ใช้ในการติดตามขึ้นอยู่กับความสำคัญและความซับซ้อนของระบบงาน กระบวนการ หรือบริการที่ว่าจ้าง

เพื่อเพิ่มความมีประสิทธิผลของการติดตาม **ผู้บริหารควรจัดลำดับความสัมพันธ์ระหว่างงานที่ใช้บริการจากผู้ให้บริการแต่ละรายกับความเสี่ยงและผลกระทบเป็นประจำ** โดยพิจารณาความเสี่ยงส่วนที่เหลือ (Residual Risk) ซึ่งไม่สามารถกำจัดหรือลดได้ด้วยการควบคุม กรณีของงานใช้บริการที่มีความเสี่ยงสูงควรได้รับการติดตามดูแลอย่างใกล้ชิด โดยทำการวิเคราะห์อย่างถี่ถ้วน (Due Diligence) การสอบทานผลการดำเนินงาน (ทั้งด้านการเงินและการปฏิบัติงาน) รวมถึงการสอบทานผลการประเมินการควบคุมที่ประเมินโดยผู้ประเมินที่มีความเป็นอิสระ อย่างไรก็ดี ผู้ให้บริการบางรายอาจไม่มีนโยบายในการเปิดเผยข้อมูลผลการตรวจสอบหรือผลการประเมินให้บุคคลภายนอกทราบ ดังนั้น สง. ควรระบุเงื่อนไขเรื่องการเปิดเผยข้อมูลฐานะการดำเนินงานและข้อมูลการเปลี่ยนแปลงที่ส่งผลกระทบต่อฐานะการดำเนินงานของผู้ให้บริการไว้ในสัญญาการให้บริการในกรณีการใช้บริการที่มีความเสี่ยงและผลกระทบที่มีนัยสำคัญ

การรวมกลุ่มของผู้ใช้งานเป็นอีกกลไกหนึ่งที่ สง. สามารถใช้ติดตามและกำกับผู้ให้บริการได้ โดยกลุ่มผู้ใช้งานสามารถมีส่วนร่วมและกำกับการทดสอบของผู้ให้บริการในเรื่องต่างๆ เช่น การทดสอบระบบรักษาความปลอดภัย การทดสอบแผนการกู้ระบบกลับคืนสู่สภาวะปกติ และการทดสอบระบบงาน เป็นต้น รวมทั้งเพิ่มความสำคัญของประเด็นปัญหาการใช้งานซึ่งจะมีผลถึงการปรับปรุงแก้ไขของผู้ให้บริการ **การรวมกลุ่มของผู้ใช้งานมักจะทำให้การติดตามและกำกับผู้ให้บริการได้ผลกว่ากรณีการติดตามโดยผู้ใช้งานแต่ละราย**

(1) <u>ข้อตกลงเรื่องระดับการให้บริการและข้อกำหนดในสัญญาที่สำคัญ</u>

ผู้บริหารควรกำหนด SLA ในสัญญาการใช้บริการของผู้ให้บริการ เพื่อระบุและแสดงความชัดเจนถึงความคาดหวังต่อผลการดำเนินงานและหน้าที่ความรับผิดชอบ SLA ดังกล่าวสามารถใช้เป็นเกณฑ์การวัดผลการดำเนินงาน ซึ่งอาจกำหนดได้ทั้งในเชิงปริมาณและเชิงคุณภาพ ผู้บริหารสามารถติดตามการปฏิบัติตาม SLA ที่สำคัญ ของผู้ให้บริการอย่างใกล้ชิด ดังนั้น **สง. ควรพัฒนาเรื่องดังต่อไปนี้ เพื่อให้มีการติดตามดูแลผลการดำเนินงานของผู้ให้บริการที่มีประสิทธิภาพ**

- นโยบายที่กำหนดขึ้นอย่างเป็นทางการ ซึ่งกำหนดให้มีการใช้ SLA
- กระบวนการติดตาม SLA

- กระบวนการรองรับกรณีที่ไม่สามารถปฏิบัติได้ตาม SLA
- กระบวนการรายงานประเด็นปัญหาต่อผู้บริหาร
- กระบวนการแก้ไขข้อพิพาท
- กระบวนการยกเลิกการใช้บริการ

(2) <u>ฐานะการเงินของผู้ให้บริการ</u>

สง. ควรมีการติดตามฐานะการเงินของผู้ให้บริการอย่างต่อเนื่อง เป็นรายปี เพื่อเป็นการปกป้องประโยชน์ของ สง. เอง หรืออาจพิจารณาใช้กระบวนการอื่นๆ ที่สามารถสะท้อนภาพฐานะการเงินและการบริหารความเสี่ยงของผู้ให้บริการ กรณีที่มีแนวโน้มว่าผู้ให้บริการอาจมีฐานะการเงินตกต่ำลงหรือขาดเสถียรภาพ สง. ก็ควรมีการสอบทานทางการเงินถี่ขึ้น ผู้บริหารควรมีการรายงานผลการสอบทานให้คณะกรรมการ สง. หรือคณะกรรมการอื่นที่ได้รับมอบหมายทราบ โดยในขั้นต่ำ การสอบทานของผู้บริหารควรประกอบด้วยการวิเคราะห์งบการเงินโดยละเอียด นอกจากนั้นอาจมีการใช้ข้อมูลอื่นประกอบด้วย เช่น รายงานตรวจสอบโดยผู้ตรวจสอบอิสระ หรือสื่อต่างๆ เช่น นิตยสารการเงิน หนังสือพิมพ์ โทรทัศน์ เป็นต้น

ถ้า สง. พิจารณาแล้วเห็นว่าฐานะการเงินของผู้ให้บริการไม่มั่นคงหรือกำลังตกต่ำลง สง. ก็ควรพิจารณาใช้แผนสำรองฉุกเฉิน ถึงแม้ว่าผู้ให้บริการยังสามารถดำเนินกิจการได้อยู่ก็ตาม **ปัญหาทางการเงินอาจทำให้คุณภาพของบริการและความถูกต้องเชื่อถือได้ของข้อมูลที่อยู่ในครอบครองลดลงได้** และการที่ผู้ให้บริการไม่สามารถให้ข้อมูลฐานะทางการเงินแก่ สง. ได้ ก็อาจเป็นสัญญาณที่ไม่ดีอย่างหนึ่งที่บ่งบอกถึงความสั่นคลอนของฐานะการเงินที่ผู้ให้บริการอาจกำลังประสบอยู่

การยกเลิกบริการที่สืบเนื่องมาจากการล้มละลายของผู้ให้บริการสามารถส่งผลกระทบรุนแรงต่อการดำเนินงานของ สง. ซึ่งผู้ให้บริการอาจจะไม่มีเวลาให้แจ้งล่วงหน้าถึงการยกเลิกการให้บริการ หรือการใช้แผนสำรองฉุกเฉิน หรือการติดต่อบุคลากรของผู้ให้บริการ ในกรณีดังกล่าว สง. จะอยู่ในสภาวะที่ต้องจัดหาศูนย์ประมวลผลสำรองอื่นทดแทนโดยเร่งด่วน

สง. สามารถเตรียมทางเลือกได้หลายทาง ดังนี้

- ชำระค่าธรรมเนียมในการใช้บริการแก่ผู้ให้บริการ และจ้างผู้เชี่ยวชาญอื่นเพื่อมาดำเนินการศูนย์คอมพิวเตอร์แทน
- จัดหาอุปกรณ์และระบบงานที่จำเป็นสำหรับการประมวลผลโดย สง. เอง
- โอนข้อมูลไปให้ผู้ให้บริการรายอื่น

ทางเลือกส่วนใหญ่มีค่าใช้จ่ายสูงและอาจส่งผลให้การปฏิบัติงานมีความล่าช้า

ในบางกรณี ผู้ให้บริการมีลิขสิทธิ์ในโปรแกรมและเอกสารที่ใช้ในการประมวลผลข้อมูลของ สง. **ถ้าสัญญาไม่ได้ระบุถึงการนำ Source Code ไปทำสัญญากับบุคคลที่สามโดย**

ให้สิทธิสง. สามารถนำ Source Code ไปใช้งานได้ตามเงื่อนไขที่กำหนด (Escrow agreement) นั่นก็หมายความว่า สง. ไม่ได้ โปรแกรมและเอกสารประกอบมาด้วย โปรแกรมเหล่านั้นยังคงเป็นทรัพย์สินของผู้ให้บริการ ซึ่งเจ้าหนี้ของผู้ให้บริการมีสิทธิยึดเอาไปได้ และอาจไม่ยอมให้ สง. ใช้งานระบบงานนั้นอีก ถึงแม้ว่าศาลล้มละลายอาจมีแนวทางแก้ไขให้กับ สง. แต่ก็ต้องหลังจากมีคำพิพากษาแล้ว

(3) <u>สภาพแวดล้อมการควบคุมทั่วไปของผู้ให้บริการ</u>

สง. ควรประเมินความเพียงพอของการควบคุมภายในและการรักษาความปลอดภัยของผู้ให้บริการ ผู้บริหารควรกำกับดูแลให้มั่นใจว่าผู้ให้บริการพัฒนาและปฏิบัติตามนโยบาย มาตรฐาน และขั้นตอนปฏิบัติงานอย่างเหมาะสม สง. ควรทำการประเมินโดยพิจารณาผลการตรวจสอบของผู้ตรวจสอบภายในของ สง. หรือของกลุ่มผู้ใช้งาน และผลการตรวจสอบภายนอก รวมถึงการสอบทานการควบคุมโดยผู้เชี่ยวชาญ ซึ่งในคู่มือตรวจสอบการตรวจสอบภายในและภายนอก จะกล่าวถึงรายละเอียดเพิ่มเติมของประเภทการตรวจสอบภายนอกของผู้ตรวจสอบอิสระที่ทำการตรวจสอบผู้ให้บริการ

การสอบทานการตรวจสอบของ สง. ควรครอบคลุมการประเมินปัจจัยดังต่อไปนี้ เพื่อให้สามารถพิจารณาความเพียงพอของการควบคุมภายในและการรักษาความปลอดภัยของผู้ให้บริการ

- ความเป็นไปได้ในทางปฏิบัติในการที่ผู้ให้บริการจัดให้มีผู้ตรวจสอบภายในที่ได้รับการฝึกอบรมและมีประสบการณ์ที่เพียงพอ
- การฝึกอบรมและความรู้พื้นฐานของผู้ตรวจสอบภายนอกของผู้ให้บริการ
- เทคนิคการตรวจสอบของผู้ตรวจสอบภายในด้านเทคโนโลยีสารสนเทศของผู้ให้บริการ

สง. ควรจัดให้มีการตรวจสอบการดำเนินการของผู้ให้บริการอย่างครอบคลุมและเป็นประจำ ซึ่งขอบเขตการตรวจสอบควรครอบคลุมการสอบทานมาตรการควบคุมและขั้นตอนปฏิบัติงานที่จะช่วยปกป้อง สง. จากการสูญเสียที่เกิดจากการปฏิบัติงานโดยไม่สุจริตและความผิดปกติต่าง ๆ

ผู้ตรวจสอบที่ได้รับมอบหมายควรตรวจสอบด้วยวิธี “Around-the-computer” เป็นประจำ ดังนี้

- การพัฒนาเครื่องควบคุมความครบถ้วนของข้อมูล เช่น Proof totals, batch totals, การนับจำนวนเอกสาร, การนับจำนวนบัญชี และ การกำหนดเลขที่เอกสาร เป็นต้น ซึ่งดำเนินการที่ สง. ก่อนส่งให้ผู้ให้บริการ

- การ Spot Check ขั้นตอนการกระทบรายการแบบ เพื่อให้มั่นใจว่า Output Totals ตรงกับ Input Totals หลังหักรายการที่ถูก Reject

- การสุ่มรายการที่ถูกส่งกลับ รายการที่ไม่ได้ลงบัญชี รายการค้าง และรายการที่พักไว้ เพื่อพิจารณาสาเหตุของการไม่ถูกประมวลผล วิธีการแก้ไขและกระบวนการนำรายการเหล่านั้นเข้าไปประมวลผลใหม่อีกครั้ง ในช่วงเวลาที่เหมาะสม

- การสุ่มตรวจสอบความถูกต้องของข้อมูลใน Master File เช่น Service Charge Code และสอบทาน Exception Reports รวมทั้งทำ Crosscheck ระหว่างยอดการให้สินเชื่อกับยอดเงินรับฝาก โดยเทียบกับเอกสารต้นฉบับ

- การ Spot Check การคำนวณของคอมพิวเตอร์ เช่น loan rebates ดอกเบี้ยเงินฝาก ค่าธรรมเนียมล่าช้า ค่าธรรมเนียมบริการ และสินเชื่อค้างชำระ

- การตรวจสอบร่องรอยของรายการเพื่อดูว่ามีการเก็บร่องรอยให้ครบถ้วนจนถึงจุดสิ้นสุดของรายการ

- การสอบทาน Source Input เพื่อให้มั่นใจว่าคำขอเปลี่ยนแปลง Master file ผ่านการอนุมัติโดยผู้บริหารและเจ้าหน้าที่ที่มีอำนาจ

- เยี่ยมชมผู้ให้บริการเพื่อประเมินมาตรการควบคุม เป็นประจำ

- สอบทานผลการตรวจสอบอื่น ๆ

นอกจากนี้ ผู้ตรวจสอบอาจใช้วิธีการตรวจสอบแบบ “Through-the-computer” ซึ่งต้องอาศัยคอมพิวเตอร์ในการตรวจสอบขั้นตอนต่างๆ ของการประมวลผล โดยจะมีการใช้ Audit Software Programs ทำการทดสอบ extensions และ footings รวมถึงจัดเตรียม Direct verification statements โปรแกรมดังกล่าวสามารถทำ Statistical Sample Routine ซึ่งสามารถใช้ผลลัพธ์ที่ได้เป็นหลักฐานยืนยันการตรวจสอบได้ อย่างไรก็ตาม หาก สง . ต้องการใช้โปรแกรมการตรวจสอบดังกล่าว สง. ควรได้รับคำยินยอมจากผู้ให้บริการก่อน

คณะกรรมการของสง. ควรจัดให้มีการตรวจสอบที่มีขอบเขตครอบคลุมอย่างเพียงพอ ว่าข้อมูลจะถูกประมวลผลภายในหรือภายนอก หาก สง. ไม่มีผู้ตรวจสอบที่มีทักษะความเชี่ยวชาญเพียงพอแล้ว การตรวจสอบก็อาจทำได้ไม่ครบถ้วน ในกรณีดังกล่าว สง. ควรจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศจากภายนอกเพื่อมาเสริมการตรวจสอบภายใน

(4) <u>การเปลี่ยนแปลงที่เกิดจากสภาพแวดล้อมภายนอก</u>

สัญญาระหว่าง สง. กับผู้ให้บริการควรเป็นลายลักษณ์อักษรเพื่อแสดงความต้องการของ สง. ในเวลาที่จัดทำสัญญาขึ้น เมื่อเวลาผ่านไปความต้องการอาจมีการเปลี่ยนแปลง ซึ่งอาจเป็นผลมาจากการเปลี่ยนแปลงของกฎหมาย สภาพเศรษฐกิจ หรือปัจจัยอื่น ถึงแม้ว่าสัญญาจะมีความ

ยืดหยุ่นต่อการเปลี่ยนแปลงความต้องการตามที่กล่าว แต่ สง. ก็**ควรที่จะติดตามการเปลี่ยนแปลงและปรับปรุงสัญญาให้มีความทันสมัยอยู่เสมอ**

2.3 ประเด็นอื่นที่เกี่ยวข้อง

สรุปแนวทางปฏิบัติ

สง. ควรดำเนินการในเรื่องต่อไปนี้

- จัดให้มีการติดตามการรักษาความปลอดภัยของข้อมูลและการเตรียมการเพื่อรักษาความต่อเนื่องของธุรกิจที่มีประสิทธิผลและต่อเนื่อง
- บริหารจัดการความสัมพันธ์กับผู้ให้บริการหลายรายอย่างมีประสิทธิภาพ
- ประเมิน ติดตาม และควบคุม Cross-border risk สำหรับกรณีที่มีการใช้บริการจากผู้ให้บริการที่เป็นนิติบุคคลต่างประเทศ

2.3.1 การวางแผนการดำเนินธุรกิจอย่างต่อเนื่อง

สง. แต่ละแห่งควรจัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่องที่มีประสิทธิผล ซึ่งได้มีแนวทางกำหนดไว้ในคู่มือตรวจสอบการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง สง. ควรมีกระบวนการอย่างต่อเนื่องในการติดตามความต่อเนื่องของธุรกิจเพื่อให้มั่นใจว่าผู้ให้บริการทางเทคโนโลยีมีการควบคุมความเสี่ยงที่เกี่ยวข้องกับบริการที่ให้แก่ สง. เช่น การรักษาความปลอดภัยข้อมูลอย่างเพียงพอ **สง. ไม่เพียงแต่มีความรับผิดชอบต่อแผนการรองรับการดำเนินธุรกิจอย่างต่อเนื่องสำหรับส่วนที่ดำเนินการเองเท่านั้น แต่ต้องรับผิดชอบไปถึงส่วนที่ผู้ให้บริการภายนอกดำเนินการแทน สง. ด้วย** ซึ่งในการพัฒนาแผนงานภายในของ สง. ก็ควรมีการพิจารณาในเรื่องแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องสำหรับส่วนที่ผู้ให้บริการภายนอกดำเนินการแทน

แผนการบริหารความเสี่ยงที่เกิดจากการใช้บริการภายนอก ควรมีการระบุความรับผิดชอบของแต่ละฝ่ายในการรักษาความปลอดภัยข้อมูลและการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง ซึ่งควรมีการพิจารณาความสำคัญของบริการทางการเงินที่พึ่งพาบริการจากผู้ให้บริการภายนอกด้วย เช่น ผู้ให้บริการดูแลสายสื่อสารโทรคมนาคม และระบบเครือข่ายที่สำคัญ เป็นต้น

สง. ควรมีความเข้าใจข้อกำหนดต่างๆ ของแผนการดำเนินธุรกิจอย่างต่อเนื่องของผู้ให้บริการ และนำข้อกำหนดเหล่านั้นมาผนวกรวมกับแผนการดำเนินธุรกิจอย่างต่อเนื่องของ สง. รวมทั้งติดตามดูแลผู้ให้บริการทดสอบแผนเป็นประจำทุกปี รายงานผลการทดสอบให้ผู้บริหาร สง. ทราบ และหากมีการเปลี่ยนแปลงแก้ไขแผนฯ ก็ต้องแจ้งให้ผู้บริหาร สง. ทราบด้วย นอกจากนั้น ควรมี

การผนวกรวมแผนฯ ของผู้ให้บริการกับแผนฯ ของ สง. เข้าด้วยกัน **และสื่อสารแผนฯให้กับเจ้าหน้าที่ที่เกี่ยวข้องทราบทั่วกัน** รวมทั้งมีกระบวนการบำรุงรักษาและสอบทานแผนที่ผนวกรวมกันแล้วเป็นประจำ

สง. หลายแห่งมีการใช้บริการการประมวลผลข้อมูลของผู้ให้บริการภายนอก ซึ่งการหยุดชะงักเป็นเวลานาน หรือการยกเลิกบริการจะส่งผลกระทบต่อการดำเนินงานตามปกติของ สง. หากจะมีการยกเลิกบริการ ก็ควรปฏิบัติให้เป็นไปตามข้อตกลงในสัญญาการใช้บริการ แต่ก็อาจส่งผลให้เกิดเหตุการณ์ที่ไม่คาดคิดขึ้นก็ได้

ถ้าผู้ให้บริการปฏิบัติตามมาตรฐานของอุตสาหกรรมและมีการบำรุงรักษาแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องแล้ว ก็จะลดโอกาสของการหยุดชะงักของบริการ และไม่กระทบต่อข้อตกลงในสัญญา **แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องควรกำหนดให้ผู้ให้บริการจัดเก็บแฟ้มข้อมูล โปรแกรมชุดที่เป็นปัจจุบันที่ศูนย์สำรอง และจัดหาศูนย์ประมวลผลสำรองที่แยกต่างหากออกจากศูนย์หลัก ซึ่งอย่างน้อยควรจะสามารถรองรับการประมวลผลข้อมูลและระบบงานที่สำคัญของ สง. ได้** หากเกิดเหตุการณ์ความเสียหายขึ้น แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของผู้ให้บริการจะเป็นเครื่องมือที่สำคัญในการกู้ระบบงานของ สง. กลับคืนสู่สภาพปกติ ซึ่งแผนฯ ของผู้ให้บริการควรสอดคล้องกับแผนของ สง. ด้วย

เหตุการณ์ที่อาจส่งผลต่อความพร้อมใช้ของเทคโนโลยีของ สง. ได้แก่ ภัยธรรมชาติ อุบัติภัย โปรแกรมระบบงานทำงานผิดพลาด อุปกรณ์ Hardware เสียหาย ไฟฟ้าดับ ตลอดจนถึงความไม่มีเสถียรภาพทางสังคม การเมือง และเศรษฐกิจ ถึงแม้ว่า สง. จะมอบหมายผู้ให้บริการภายนอกดำเนินการแทน แต่ สง. ก็ควรดำเนินการให้มั่นใจว่ามีการสำรองข้อมูลและระบบการประมวลผลที่สำคัญอย่างเหมาะสม ซึ่งการมีกระบวนการสำรองที่มีประสิทธิผลจะช่วยให้ สง. สามารถประมวลผลข้อมูลได้ในช่วงที่ระบบสื่อสารข้อมูลได้รับความเสียหาย ซึ่งมีหลายทางเลือกให้ผู้บริหารพิจารณา เช่น การประมวลผลด้วย Batch ทดแทนการประมวลผลแบบ Real-time การใช้ PC ในลักษณะ Offline การเก็บรวบรวมข้อมูล (Data Capture) ที่ Controller ถ้าสายสื่อสารได้รับความเสียหาย หรือการจัดเตรียมสายสื่อสารสำรอง โมเด็มสำรอง หรือการเปลี่ยนเส้นทางในวงจรจากสายโทรศัพท์ท้องถิ่น (Rerouted circuit from local telephone carrier) สง. ที่ดำเนินการเก็บรวมรวมข้อมูล (Data Capture) หรือดำเนินงานอื่นเอง ควรจัดเตรียมสถานที่ปฏิบัติงานสำรอง หรือระบุวิธีการอื่นในแผนสำรองที่จะใช้กู้การดำเนินงานเหล่านั้นกลับคืนสู่สภาวะปกติ

สง. ควรมีแผนสำรองที่ระบุขั้นตอนการปฏิบัติงานต่างๆอย่างครอบคลุม โดยควรครอบคลุมรายละเอียดของวิธีจัดหาและใช้งานอุปกรณ์และบุคลากรด้วย สง. ควรทดสอบอุปกรณ์

ระบบงาน ข้อมูลสำรองเหล่านั้นเป็นประจำ เพื่อให้มั่นใจว่ามีการป้องกันที่เหมาะสมและพนักงานมีความคุ้นเคยกับแผนฯ

ในการติดตามและบำรุงรักษาแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง สง. ควร

- สอบทานแผนฯของผู้ให้บริการเป็นประจำ เพื่อให้มั่นใจว่าบริการสำคัญของ สง. จะสามารถกู้กลับคืนได้ในระยะเวลาที่ยอมรับได้

- **สอบทานแผนการทดสอบแผนสำรองฉุกเฉินของผู้ให้บริการ ซึ่งควรมีการทดสอบแผนดังกล่าวของบริการสำคัญอย่างน้อยปีละครั้ง**

- ประเมินการพึ่งพาระหว่างกันของผู้ให้บริการสำหรับบริการและระบบงานที่สำคัญ

2.3.2 การใช้บริการด้านการรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

นอกเหนือจากการกำกับดูแลบริการทางการเงินและทางเทคโนโลยีของผู้ให้บริการภายนอกแล้ว สำหรับสง. ที่มีการใช้บริการด้านการรองรับการดำเนินธุรกิจอย่างต่อเนื่องทั้งหมดหรือบางส่วนจากภายนอก ก็ควรพิจารณาปัจจัยดังต่อไปนี้

- บุคลากร – ผู้ให้บริการควร**มีพนักงานที่มีความรู้เพียงพอต่อการให้บริการสนับสนุนทางเทคนิค**เพื่อให้มั่นใจว่าจะสามารถกู้การดำเนินงานกลับคืนสู่สภาพปกติที่ศูนย์สำรองได้ทันเวลา

- Processing Time Availability – ผู้ให้บริการควรจัดสรรเวลา ทรัพยากรที่ใช้ในการประมวลผล และการควบคุมการรักษาความปลอดภัยอย่างเพียงพอต่อการให้บริการแก่ลูกค้าหลายราย **สง. ควรมั่นใจได้ว่าระบบการประมวลผลสามารถรองรับปริมาณรายการในระดับปกติได้ภายในระยะเวลาตามที่กำหนด**

- สิทธิการเข้าถึง – **ผู้ให้บริการควรเปิดเผยข้อจำกัดในการเข้าถึง และควรรับประกันได้ว่า สง. มีสิทธิใช้ศูนย์ได้หากเกิดเหตุการณ์ฉุกเฉินขึ้น** หรือ สง. ควรทำความเข้าใจกับผู้ให้บริการถึงลำดับการใช้งาน ตัวอย่างเช่น บางศูนย์จะให้บริการแบบ First come, First serve จนกระทั่งมีการใช้งานเต็มศักยภาพ แต่บางแห่งอาจจัดลำดับการใช้งานไว้ล่วงหน้าตามข้อตกลงของสัญญา

- Hardware และ Software – **ศูนย์สำรองควรจัดหา Hardware และ Software ที่สอดคล้องกันกับที่ใช้งานอยู่จริง** สง. ควรติดตามความสอดคล้องกันของ Hardware และ Software เพื่อให้เป็นไปตามข้อตกลง ซึ่งสัญญาควรกำหนดให้มีการแจ้ง สง. ทราบ หากมีการเปลี่ยนแปลง Hardware, Software หรืออุปกรณ์ต่างๆ ในศูนย์สำรอง

- การควบคุมการรักษาความปลอดภัย – สง. ควรมีจัดให้มีมาตรการควบคุมการรักษาความปลอดภัยทั้งทางกายภาพและตรรกที่ศูนย์สำรอง

- การทดสอบ – **สัญญาการใช้บริการควรกำหนดครอบคลุมเรื่องการทดสอบที่ศูนย์สำรองเป็นประจำ** ในขั้นต่ำ สง. ต้องมีสิทธิเข้าศูนย์สำรองเพื่อดำเนินการทดสอบเต็มรูปแบบปีละครั้ง ซึ่งรวมถึงการตรวจสอบสมรรถนะของระบบสื่อสารโทรคมนาคมด้วย ในทางเดียวกัน สง. ควรให้ความมั่นใจว่า ผู้ให้บริการจะดำเนินการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของตนเองเป็นประจำ และส่งผลการทดสอบมาให้ สง. ด้วย

- ความลับของข้อมูล – **สง. ควรติดตามดูแลผู้ให้บริการรักษาความลับของข้อมูลทางธุรกิจและข้อมูลของลูกค้า** ผู้ให้บริการควรจัดให้มีการควบคุมที่เพียงพอเพื่อให้มั่นใจถึงความปลอดภัยและความลับของข้อมูล โดยให้สอดคล้องกับนโยบายการรักษาความปลอดภัยของ สง. **กรณีที่ศูนย์สำรองให้บริการแก่ลูกค้าหลายราย ความลับของข้อมูลเป็นเรื่องมีความสำคัญมากขึ้น** ผู้บริหารควรพิจารณาให้ผู้ให้บริการระบุประเด็นดังกล่าวไว้ในสัญญาด้วย

- การสื่อสารโทรคมนาคม – สง. ควรสอบทานระบบสื่อสารโทรคมนาคมสำรองและสมรรถนะของศูนย์สำรองที่จะรองรับ การสื่อสารระหว่าง สง. กับศูนย์สำรอง

- ข้อตกลงซึ่งกันและกัน (Reciprocal Agreement) – สง. ที่ทำสัญญากับ สง. อื่นเพื่อเป็นศูนย์สำรองซึ่งกันและกัน ควรพิจารณาประเด็นเรื่องบุคลากร ความพร้อมสำหรับการใช้งาน ประมวลผล สิทธิการเข้าใช้ศูนย์สำรอง การทดสอบศูนย์สำรอง ความสอดคล้องกันของระบบและอุปกรณ์ต่างๆ การรักษาความปลอดภัย สมรรถนะของศูนย์ สง. ทั้ง 2 แห่งควรดูแลสมรรถนะของศูนย์ให้ได้ตาม Recovery Time Objectives และ ระดับของบริการขั้นต่ำ

- พื้นที่ – ศูนย์สำรองควรมีพื้นที่สำหรับเป็นส่วนที่พักของพนักงานที่ปฏิบัติงานในสภาวะฉุกเฉินของ สง.

- ศักยภาพของการจัดพิมพ์ – ศูนย์สำรองควรมีเครื่องพิมพ์ที่เพียงพอต่อความต้องการของ สง. โดยมีประสิทธิภาพในระดับที่ยอมรับได้

- การติดต่อ – **ผู้บริหารของ สง. ควรรับทราบขั้นตอนการประกาศภาวะฉุกเฉิน รวมถึงเจ้าหน้าที่ที่มีอำนาจประกาศภาวะฉุกเฉินและอนุมัติให้เริ่มใช้ศูนย์สำรอง สง. ควรปรับปรุงรายชื่อของผู้ติดต่อของศูนย์สำรองพร้อมเบอร์โทรศัพท์ และรับทราบขั้นตอนปฏิบัติในการติดต่อกับผู้ให้บริการ**

การใช้บริการสำหรับการเตรียมการรองรับการดำเนินธุรกิจอย่างต่อเนื่องจากภายนอกสามารถประหยัดค่าใช้จ่ายให้แก่ สง. ขนาดเล็ก เมื่อเทียบกับค่าใช้จ่ายในการสร้างและบำรุงรักษาศูนย์สำรอง สง. ควรมีการทดสอบศูนย์สำรองอย่างครอบคลุมเป็นประจำ อย่างน้อยปีละครั้ง

2.3.3 การป้องกันและรักษาความปลอดภัยของข้อมูล

ข้อมูลเป็นทรัพย์สินที่มีคุณค่า ซึ่ง สง. ควรมั่นใจว่าในการใช้บริการจากภายนอก ได้มีการปกป้องความปลอดภัยของข้อมูลไว้อย่างเพียงพอ สง. มีความรับผิดชอบตามกฎหมายในการดูแลให้ผู้ให้บริการดำเนินมาตรการที่เหมาะสมกับเป้าหมายของแนวทางการรักษาความปลอดภัยข้อมูล มาตรการเหล่านั้นควรฝังอยู่ในกระบวนการรักษาความปลอดภัยของ สง. และควรมีระบุไว้ในสัญญาระหว่างสง. กับผู้ให้บริการ โปรดอ่านรายละเอียดเพิ่มเติมในคู่มือตรวจสอบการรักษาความปลอดภัยข้อมูล

ในการคัดเลือกผู้ให้บริการ ผู้บริหารควรจัดให้มีการวิเคราะห์อย่างถี่ถ้วน (Due Diligence) เพื่อให้มั่นใจว่ามีการป้องกันทรัพย์สินของ สง. และลูกค้า สง. ควรติดตามดูแลมาตรฐานการรักษาความปลอดภัยของผู้ให้บริการว่าเป็นไปตามหรือสูงกว่ากับมาตรฐานที่กำหนดโดย สง. ก่อนที่จะทำสัญญากับผู้ให้บริการ และตลอดระยะเวลาของการใช้บริการ สง. ควรมั่นใจได้ว่า ผู้ให้บริการได้รับสิทธิการเข้าถึงข้อมูลและระบบงานที่จำเป็นต่อดำเนินงานเท่านั้น ผู้บริหารควรจำกัดสิทธิเข้าถึงระบบงานของ สง. และควบคุมติดตามการใช้งานระบบของผู้ให้บริการและ สง. อย่างเหมาะสม

2.3.4 การใช้บริการของผู้ให้บริการหลายราย

การใช้บริการของผู้ให้บริการหลายรายเป็นลักษณะที่ผู้ให้บริการมากกว่า 2 ราย ขึ้นไปร่วมกันดำเนินงานให้ สง.

วิธีการบริหารจัดการความสัมพันธ์กับผู้ให้บริการหลายรายมี 2 วิธี ซึ่งสง. อาจเลือกใช้วิธีใดวิธีหนึ่งก็ได้ อย่างไรก็ตาม สง. ก็ต้องมีความเข้าใจและติดตามสภาพแวดล้อมการควบคุมผู้ให้บริการทุกรายที่สามารถเข้าถึงระบบ ข้อมูล หรือทรัพยากรอื่น ของ สง. วิธีแรกคือการแต่งตั้งผู้ให้บริการหลัก เพื่อบริหารจัดการผู้ให้บริการรายอื่น วิธีที่ 2 คือ การใช้ข้อตกลงการปฏิบัติงานกับผู้ให้บริการแต่ละราย หรือเป็นลักษณะ Stand-alone contracts

- วิธีที่ 1 สัญญาควรกำหนดให้ผู้ให้บริการหลักแจ้ง สง. ถึงประเด็นที่เกี่ยวกับการควบคุมและการดำเนินงานที่เกี่ยวข้องกับกิจกรรมที่ใช้บริการ ซึ่งผู้บริหารควรมั่นใจได้ว่าผู้ให้บริการจัดให้มีสภาพแวดล้อมการควบคุมเป็นไปตามหรือสูงกว่าความคาดหวังของ สง. เช่น สภาพแวดล้อมการควบคุมภายในองค์กรของผู้ให้บริการหลัก

- วิธีที่ 2 คือ การจัดทำสัญญากับผู้ให้บริการแต่ละราย ซึ่ง สง. ต้องมีการบริหารจัดการผู้ให้บริการแต่ละรายด้วย ในขณะที่การทำสัญญากับผู้ให้บริการหลักรายเดียว สามารถลดความจำเป็นของการมีส่วนเกี่ยวข้องโดยตรงของ สง. หากผู้รับจ้างช่วงงานต่อไม่สามารถปฏิบัติงานได้ อย่างไรก็ตาม สง. ยังคงมีความรับผิดชอบในการติดตามการควบคุมภายในและการรักษาความ

ปลอดภัยของผู้รับจ้างช่วงงานต่อ โดยพิจารณาผ่านทางการบริหารจัดการของผู้ให้บริการหลัก เนื่องจาก สง. จะมีอำนาจในการควบคุมลดลงในกรณีที่ใช้วิธีแต่งตั้งผู้ให้บริการหลัก สัญญาการใช้บริการควรกำหนดให้ผู้ให้บริการแจ้งให้ สง. ทราบว่ามีการว่าจ้างผู้รับจ้างช่วงงานต่อทุกราย

2.3.5 การใช้บริการของผู้ให้บริการที่อยู่ต่างประเทศ

สง. ที่มีการใช้บริการจากผู้ให้บริการที่อยู่ต่างประเทศ ถึงแม้ว่าจะได้รับประโยชน์ในเรื่องต้นทุน ทักษะความเชี่ยวชาญ และอื่นๆ ก็ตาม สง. ก็ควรมีการวิเคราะห์ผู้ให้บริการอย่างถี่ถ้วนเสมือนกับการใช้บริการจากผู้ให้บริการในประเทศ นอกจากนั้นความเสี่ยงจากการใช้บริการจากผู้ให้บริการที่อยู่ต่างประเทศจะมีลักษณะเฉพาะที่แตกต่างออกไป เช่น ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านชื่อเสียง ความเสี่ยงด้านเครดิต ความเสี่ยงด้านสภาพคล่อง ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงของภูมิภาค และการปฏิบัติตามกฎหมาย เป็นต้น ซึ่ง สง. ควรมีการระบุ ประเมิน ป้องกัน และควบคุมความเสี่ยงดังกล่าว โปรดอ่านรายละเอียดเพิ่มเติมในภาคผนวก: ผู้ให้บริการภายนอกที่อยู่ต่างประเทศ

<u>ส่วนที่ 3</u> แนวทางการตรวจสอบ

3.1 วัตถุประสงค์ของการตรวจสอบ

เพื่อประเมินประสิทธิผลของกระบวนการบริหารความเสี่ยงของ สง. ที่เกี่ยวข้องกับการใช้บริการเทคโนโลยีสารสนเทศจากภายนอก

- **การตรวจสอบทั่วไป (Tier 1)** มีเป้าหมายและขั้นตอนการตรวจสอบที่เกี่ยวกับกระบวนการระบุและบริหารความเสี่ยงที่เกิดจากการใช้บริการภายนอก

- **การตรวจสอบเชิงลึก (Tier 2)** มีเป้าหมายและขั้นตอนการตรวจสอบที่เกี่ยวกับการใช้เทคนิคการทดสอบกระบวนการปฏิบัติงานและพิสูจน์หลักฐานเพื่อยืนยันความเสี่ยงที่พบ

ผู้ตรวจสอบสามารถเลือกใช้ แนวทางการตรวจสอบใน Tier 1 และ Tier 2 ตามความเหมาะสมและสอดคล้องกับวัตถุประสงค์ของการตรวจสอบ

3.2 วัตถุประสงค์และกระบวนการตรวจสอบทั่วไป (Tier 1)

<u>วัตถุประสงค์ที่ 1</u> **:** พิจารณากำหนดขอบเขตของการตรวจสอบ

1. สอบทานข้อมูลในอดีตเพื่อประเมินจุดอ่อนของการใช้บริการจากภายนอก โดยพิจารณา
   - รายงานตรวจสอบ สง. และ ผู้ให้บริการของผู้กำกับดูแลทางการ
   - รายงานตรวจสอบภายในและภายนอกของสง. และผู้ให้บริการ (ถ้ามี)
2. ประเมินคำชี้แจงของผู้บริหารต่อข้อสังเกตของผู้ตรวจสอบครั้งล่าสุด
   - การแก้ไขที่ต้นเหตุ แทนที่จะแก้ไขปัญหาทีละอย่าง
   - ประเด็นที่ยังไม่ได้แก้ไข
3. สัมภาษณ์ผู้บริหารและสอบทานข้อมูลของ สง. เพื่อระบุ
   - ความสัมพันธ์กับผู้ให้บริการในปัจจุบัน และที่มีการเปลี่ยนแปลง จากการตรวจสอบครั้งล่าสุด รวมทั้งระบุผู้รับจ้างช่วงงานต่อที่สำคัญ ผู้ให้บริการที่เป็นบริษัทในเครือหรือบริษัทที่เกี่ยวข้อง และผู้ให้บริการภายนอกที่อยู่ในต่างประเทศ
   - **ปริมาณรายการปัจจุบันของงานแต่ละอย่างที่ใช้บริการจากภายนอก**
   - ปัญหาจากการใช้บริการที่สำคัญ
   - ผู้ให้บริการที่มีจุดอ่อนในด้านการเงินและการควบคุมที่สำคัญ และ
   - **มีการแจ้งให้หน่วยงานกำกับดูแลทราบถึงการใช้บริการจากภายนอก ตามที่กฎหมายกำหนดหรือไม่**

วัตถุประสงค์ที่ 2 : ประเมินความเสี่ยงเชิงปริมาณที่เกิดจากการใช้บริการจากภายนอก

1. ประเมินระดับความเสี่ยงจากการใช้บริการภายนอก โดยพิจารณาความเสี่ยงที่เกี่ยวข้องกับ

- งานที่ใช้บริการ
- ผู้ให้บริการ ในกรณีผู้ให้บริการอยู่ต่างประเทศ ให้พิจารณาความเสี่ยงที่มีลักษณะเฉพาะของผู้ให้บริการที่อยู่ต่างประเทศด้วย
- เทคโนโลยีที่ใช้

วัตถุประสงค์ที่ 3 : ประเมินคุณภาพของการบริหารความเสี่ยง

1. ประเมินกระบวนการใช้บริการจากภายนอกโดยพิจารณาความเหมาะสมกับขนาดและความซับซ้อนของ สง. โดยให้ความสำคัญกับองค์ประกอบดังต่อไปนี้

- สง. มีการประเมินการปฏิบัติงานของผู้ให้บริการว่ามีความสอดคล้องตามขอบเขตและความสำคัญของบริการที่ว่าจ้าง
- ข้อกำหนดที่ใช้ในการติดตามอย่างต่อเนื่อง

2. ประเมินกระบวนการกำหนดความต้องการ

- ตรวจสอบให้แน่ชัดว่าผู้เกี่ยวข้องทุกฝ่ายเข้ามามีส่วนร่วมในการกำหนดความต้องการ และความต้องการที่กำหนดถูกนำไปใช้ในการจัดทำ RFP สัญญา และการติดตามรวมทั้งมีการจัดทำเอกสารประกอบการดำเนินงาน
- ตรวจสอบให้แน่ชัดว่าการกำหนดความต้องการมีความชัดเจนและสามารถสนับสนุนการควบคุมการคัดเลือกผู้ให้บริการ การจัดเตรียมสัญญา และการติดตามในอนาคตได้อย่างสมบูรณ์

3. ประเมินกระบวนการคัดเลือกผู้ให้บริการ

- พิจารณาว่า RFP ครอบคลุมองค์ประกอบของความต้องการของ สง. ได้อย่างครบถ้วน และมีรายละเอียดเพียงพอที่จะสนับสนุนการจัดทำ RFP การร่างสัญญา และการติดตามต่อไป
- พิจารณาว่ามีการประเมินความแตกต่างระหว่าง RFP กับสิ่งที่ผู้ให้บริการที่ได้รับการคัดเลือกเสนออย่างเหมาะสม และ สง ดำเนินการที่เหมาะสมในการลดความเสี่ยงที่อาจไม่ได้ตามความต้องการ
- พิจารณา สง. มีการวิเคราะห์อย่างถี่ถ้วนครอบคลุมความสัมพันธ์กับผู้ให้บริการในทุกแง่มุม เช่น ฐานะการเงิน ชื่อเสียง ของผู้ให้บริการ (ในกรณี ชื่อเสียง สง. อาจตรวจสอบ

กับแหล่งอ้างอิงก็ได้) รวมทั้ง การควบคุม บุคลากรหลัก แผนการกู้ระบบกลับคืนสู่สภาวะปกติและการทดสอบ การประกันภัย สมรรถนะของระบบสื่อสาร และการใช้ผู้รับจ้างช่วงต่อ

4. ประเมินกระบวนการทำสัญญากับผู้ให้บริการ โดยพิจารณา

- สัญญาระบุข้อตกลงเรื่องระดับการให้บริการที่เพียงพอและวัดได้
- วิธีการกำหนดราคาจะไม่ส่งผลกระทบในทางลบต่อความมั่นคงและเสถียรภาพของ สง. ซึ่งรวมความสมเหตุสมผลของการเปลี่ยนแปลงราคาในอนาคต
- มีการกำหนดสิทธิและความรับผิดชอบของคู่สัญญาโดยมีรายละเอียดที่ชัดเจนเพียงพอ
- สัญญาครอบคลุมประเด็นที่สำคัญ เช่น การรายงานด้านการเงินและการควบคุม สิทธิในการเข้าตรวจสอบ ลิขสิทธิ์ของข้อมูลและโปรแกรม ความลับของข้อมูล ผู้รับจ้างช่วงงานต่อ และความต่อเนื่องของบริการ เป็นต้น
- หน่วยงานด้านกฎหมายหรือที่ปรึกษาทางกฎหมายสอบทานสัญญาและได้มีการแก้ไขประเด็นทางกฎหมายจนเป็นที่พอใจแล้ว
- ประเด็นการหลบเลี่ยงด้วยเงื่อนไขของสัญญา ได้ผ่านการพิจารณาอย่างเพียงพอแล้ว

5. ประเมินกระบวนการติดตามความเสี่ยงที่เกิดจากการใช้บริการภายนอกของ สง. ตรวจสอบให้แน่ชัดว่า การติดตามครอบคลุมเรื่องต่อไปนี้

- ข้อตกลงเรื่องระดับการให้บริการและข้อกำหนดในสัญญาที่สำคัญ
- ฐานะการเงินของผู้ให้บริการ
- สภาพแวดล้อมการควบคุมทั่วไปของผู้ให้บริการ โดยสอบทานจากรายงานตรวจสอบภายใน ภายนอก และรายงานตรวจสอบของทางการ
- แผนการกู้ระบบกลับคืนสู่สภาวะปกติและการทดสอบ
- การรักษาความปลอดภัยข้อมูล
- ขอบเขตของการประกันภัย
- การบริหารจัดการผู้รับจ้างช่วงงานต่อ รวมถึงประเด็นเรื่องการเปลี่ยนแปลงและการควบคุม
- การบริหารจัดการผู้ให้บริการที่อยู่ต่างประเทศ
- การเปลี่ยนแปลงที่เกิดจากสภาพแวดล้อมภายนอก เช่น การแข่งขัน แนวโน้มของอุตสาหกรรม

6. สอบทานนโยบายที่เกี่ยวข้องกับการจัดลำดับผู้ให้บริการตามความเสี่ยงเป็นประจำ เพื่อใช้ในการตัดสินใจกำหนดระดับความเข้มในการติดตาม เช่น การประเมินความเสี่ยงกระบวนการตัดสินใจ ควร

- ครอบคลุมเกณฑ์ที่เป็นรูปธรรม
- สนับสนุนความสอดคล้องกับระบบงาน
- พิจารณาระดับที่ผู้ให้บริการสนับสนุนกลยุทธ์และความต้องการของธุรกิจที่สำคัญของ สง.
- ระบุกิจกรรมที่ต้องดำเนินการต่อไป หากมีการเปลี่ยนแปลงลำดับของผู้ให้บริการ

7. ประเมินว่า สง. มีการใช้ประโยชน์จากการรวมกลุ่มของผู้ใช้งาน และกลไกอื่นในการติดตามและกำกับผู้ให้บริการ

<u>วัตถุประสงค์ที่ 4</u> **:** หารือถึงแนวทางการดำเนินการแก้ไข และแจ้งผลการตรวจสอบ

1. พิจารณาความจำเป็นที่ต้องใช้แนวทางการตรวจสอบเชิงลึก (Tier 2) เพื่อตรวจพิสูจน์หลักฐานสนับสนุนข้อสรุปที่ได้มาจากการตรวจสอบทั่วไป (Tier 1)

2. สอบทานสรุปผลการตรวจสอบเบื้องต้นร่วมกับ EIC โดยพิจารณา

- ประเด็นการละเมิดกฎหมาย ระเบียบทางการ
- ประเด็นสั่งการ
- ผลกระทบต่อความเสี่ยงและการจัดลำดับความเสี่ยงรวมและด้านเทคโนโลยีสารสนเทศ

3. หารือผลการตรวจสอบกับผู้บริหาร และขอคำชี้แจงถึงแนวทางการดำเนินการแก้ไขสำหรับประเด็นที่สำคัญ

4. จัดทำเอกสารสรุปผลการตรวจสอบเพื่อเสนอต่อ EIC

5. จัดเก็บกระดาษทำการที่ใช้ในการตรวจสอบให้เป็นระบบ

3.3 วัตถุประสงค์และกระบวนการตรวจสอบเชิงลึก (Tier 2)

ก. การกำหนดความต้องการด้านเทคโนโลยีสารสนเทศ

1. สอบทานเอกสารสนับสนุนกระบวนการกำหนดความต้องการเพื่อให้มั่นใจว่าเอกสารมีความครอบคลุมเรื่อง ดังต่อไปนี้

- ขอบเขตและลักษณะ
- มาตรฐานสำหรับการควบคุม
- ลักษณะขั้นต่ำที่ยอมรับได้ของผู้ให้บริการ

- การติดตามและการรายงาน
- ข้อกำหนดในการโอนงาน/ส่งมอบงาน (Transition Requirement)
- ระยะเวลาของสัญญา การยกเลิกสัญญา และการมอบหมายสิทธิ
- การคุ้มครองความเสียหายตามสัญญา

ข. การวิเคราะห์อย่างถี่ถ้วน

1 ประเมินการสอบทานฐานะความมั่นคงทางการเงินของผู้ให้บริการ

- วิเคราะห์งบการเงินที่ผ่านการรับรองโดยผู้ตรวจสอบและรายงานประจำปีของผู้ให้บริการ
- ประเมินระยะเวลาในการดำเนินธุรกิจและส่วนแบ่งทางการตลาด
- พิจารณาความซับซ้อนของสัญญาเทียบกับขนาดของบริษัทผู้ให้บริการ
- สอบทานระดับการลงทุนด้านเทคโนโลยีของผู้ให้บริการเพื่อให้มั่นใจว่าจะมีการสนับสนุนอย่างต่อเนื่อง
- ประเมินผลกระทบจากความเสี่ยงด้านเศรษฐกิจ การเมือง หรือสภาพแวดล้อมที่มีต่อความมั่นคงของผู้ให้บริการ

2. ประเมินการทำการวิเคราะห์อย่างถี่ถ้วนของ สง. ครอบคลุมเรื่อง ดังต่อไปนี้

- สอบถามข้อมูลเกี่ยวกับชื่อเสียงและผลการดำเนินงานของผู้ให้บริการจากแหล่งอ้างอิง ได้แก่ผู้ใช้บริการหรือกลุ่มผู้ใช้บริการปัจจุบัน
- ประสบการณ์และความสามารถของผู้ให้บริการในอุตสาหกรรม
- ประสบการณ์และความสามารถของผู้ให้บริการในการดำเนินงานกับสถานการณ์ที่คล้ายคลึงกับสภาพแวดล้อมและการดำเนินงานของ สง.
- ค่าใช้จ่ายในการเพิ่มระบบใหม่และการแปลงข้อมูลหรือการสร้าง Interface
- ข้อบกพร่องในการให้บริการของผู้ให้บริการซึ่ง สง. จะต้องหาแนวทางเพื่อมาลดความเสี่ยงดังกล่าว
- การเสนอขอใช้บุคคลภายนอก ผู้รับจ้างช่วงงานต่อ หรือหุ้นส่วนเพื่อสนับสนุนการให้บริการแก่ สง.
- ความสามารถของผู้ให้บริการในการรับมือกับเหตุการณ์ความเสียหายซึ่งส่งผลกระทบต่อการให้บริการ
- เจ้าหน้าที่หลักของผู้ให้บริการที่ได้รับมอบหมายให้มาดูแล สง.
- ความสามารถของผู้ให้บริการในการปฏิบัติตามกฎหมาย ระเบียบของทางการ ซึ่งผู้บริหาร สง. ควรมีการประเมินความสามารถในการปฏิบัติตามกฎหมายของผู้ให้บริการ

- ความเสี่ยงของประเทศ ภูมิภาค และท้องถิ่น

ค. สัญญาการใช้บริการ

1. ตรวจสอบว่าหน่วยงานด้านกฎหมายหรือที่ปรึกษากฎหมายสอบทานสัญญาก่อนการลงนามในสัญญาหรือไม่

- พิจารณาว่ามีหน่วยงานด้านกฎหมายหรือที่ปรึกษาทางกฎหมายที่มีคุณสมบัติเพียงพอที่จะสอบทานสัญญา โดยเฉพาะสำหรับกรณีที่สัญญาอยู่ภายใต้กฎหมายของต่างประเทศ

- การสอบทานทางกฎหมายควรครอบคลุมการประเมินการมีผลใช้บังคับตามข้อกำหนดต่างๆในสัญญาและตามกฎหมายของต่างประเทศ

2. ตรวจสอบสัญญามีการระบุเรื่องดังต่อไปนี้อย่างเหมาะสม

- ขอบเขตของบริการ
- มาตรฐานการดำเนินงาน
- การกำหนดราคา
- การควบคุม
- การรายงานทางการเงินและการควบคุม
- สิทธิในการเข้าตรวจสอบ
- ความเป็นเจ้าของข้อมูลและโปรแกรม
- การรักษาความลับและความปลอดภัย
- การปฏิบัติตามกฎระเบียบทางการ
- การชดใช้ความเสียหาย
- ขีดจำกัดความรับผิดชอบต่อความเสียหาย
- การแก้ไขข้อพิพาท
- อายุของสัญญา
- ข้อจำกัดหรือการอนุมัติล่วงหน้ากรณีมีผู้รับจ้างช่วงงานต่อ
- การยกเลิกและการโอนสิทธิ ซึ่งรวมถึงการคืนข้อมูลในรูป machine-readable format มาให้ สง. ได้ทันเวลา
- ขอบเขตของการประกันภัย
- ข้อได้เปรียบทางกฎหมาย (ถ้ามี)
- การเลือกใช้กฎหมาย (การใช้บริการจากต่างประเทศ)
- การเข้าถึงข้อมูลเพื่อการตรวจสอบโดยผู้ตรวจสอบทางการ

- การวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

3. สอบทานข้อตกลงระดับการให้บริการเพื่อให้มั่นใจว่าข้อตกลงดังกล่าวมีความเพียงพอและวัดได้ โดยพิจารณาเรื่องดังต่อไปนี้

- องค์ประกอบที่สำคัญของบริการมีระบุไว้ชัดเจนและเป็นไปตามความต้องการของ สง. ที่กำหนด
- มีการระบุเป้าหมายที่จะวัดสำหรับแต่ละองค์ประกอบ
- มีการกำหนดให้รายงานการวัดผล
- การวัดผลสามารถแสดงถึงผลการดำเนินงานที่ไม่เพียงพอ
- มีการกำหนดโทษที่เหมาะสมหากผลการดำเนินงานไม่ได้ตามเป้าหมาย เช่น ลดค่าธรรมเนียม หรือยกเลิกสัญญา เป็นต้น

4. สอบทานกระบวนการของ สง. ในการตรวจสอบความถูกต้องของการคิดค่าใช้จ่ายและการติดตามว่าการรวมกลุ่มของบริการสามารถประหยัดค่าใช้จ่ายได้จริง

ง. การติดตามความสัมพันธ์กับผู้ให้บริการ

1. ประเมิน กระบวนการติดตามผู้ให้บริการของ สง. ในเรื่องต่อไปนี้

- ระยะเวลาของการสอบทาน ซึ่งควรมีความเหมาะสมกับความเสี่ยงของการใช้บริการ
- การเปลี่ยนแปลงความเสี่ยงของการใช้บริการ
- การเปลี่ยนแปลงที่เกิดกับผู้ให้บริการ เช่น ฐานะการเงิน หรือสภาพแวดล้อมการควบคุมเปลี่ยนแปลง เป็นต้น
- การปฏิบัติตามสัญญา รวมถึงข้อตกลงของระดับการให้บริการ
- รายงานตรวจสอบและรายงานอื่นที่กล่าวถึงความต่อเนื่องของธุรกิจ การรักษาความปลอดภัย และแง่มุมอื่นๆ ของการใช้บริการจากผู้ให้บริการภายนอก

2. สอบทานการจัดอันดับความเสี่ยงของผู้ให้บริการเพื่อให้มั่นใจว่า

- มีการปฏิบัติด้วยความสม่ำเสมอ
- มีการปฏิบัติตามนโยบาย

3. สอบทานการดำเนินการของผู้บริหารในกรณีที่มีการเปลี่ยนแปลงอันดับของผู้ให้บริการ เพื่อให้มั่นใจมีการดำเนินการที่สอดคล้องกับนโยบาย หากการจัดอันดับสะท้อนความเสี่ยงที่เพิ่มขึ้น

4. สอบทานผู้ให้บริการ หรือสัญญาการใช้บริการได้ระบุถึงการบริหารจัดการผู้รับจ้างช่วงงานต่อที่สำคัญ

- ผู้บริหารสอบทานสภาพแวดล้อมการควบคุมของผู้รับจ้างช่วงงานต่อทุกรายที่เกี่ยวข้องว่ามีการปฏิบัติตามข้อกำหนดและแนวทางการรักษาความปลอดภัยของ สง. หรือไม่

- สง. ติดตาม และจัดทำเอกสารที่เกี่ยวข้องกับการบริหารจัดการความสัมพันธ์กับผู้รับจ้างช่วงงานต่อ โดยรวมถึงการเปลี่ยนแปลงความสัมพันธ์และประเด็นการควบคุม

ภาคผนวก : ผู้ให้บริการภายนอกที่อยู่ต่างประเทศ

กรณีที่ สง มีการใช้บริการจากผู้ให้บริการที่อยู่ในต่างประเทศ ผู้ตรวจสอบควรพิจารณาใช้แนวทางในส่วนนี้เพิ่มเติมจากแนวทางอื่นที่กล่าวในคู่มือ เนื้อหาในส่วนนี้จะกล่าวถึงความเสี่ยงหลักที่อาจเกิดจากการใช้บริการของผู้ให้บริการที่อยู่ในต่างประเทศ[2] ขั้นตอนที่ สง. พึงปฏิบัติในการบริหารความเสี่ยง และส่วนอื่นที่เกี่ยวข้อง

ที่มา

ปัจจุบันแนวโน้มการใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการที่อยู่ในต่างประเทศหรือผู้ให้บริการในประเทศที่มีผู้รับจ้างช่วงงานต่อดำเนินการอยู่ในต่างประเทศสูงขึ้น

การใช้บริการจากผู้ให้บริการที่อยู่ต่างประเทศเป็นแนวปฏิบัติทางธุรกิจปกติ ที่จะทำให้ธุรกิจสามารถประหยัดต้นทุนจากการประมวลผลเองหรือการใช้บริการจากผู้ให้บริการที่อยู่ในประเทศ อย่างไรก็ตาม แนวปฏิบัติดังกล่าวทำให้เกิดประเด็นที่ควรพิจารณาเพิ่มเติม ได้แก่ ความเสี่ยงของประเทศ การปฏิบัติตามกฎหมายและกฎระเบียบของผู้กำกับดูแลของสถาบันการเงินและผู้ให้บริการ การผูกพันโดยสัญญา ความเสี่ยงด้านชื่อเสียง ความเสี่ยงด้านปฏิบัติการ และความเสี่ยงด้านกลยุทธ์ เป็นต้น ในการบริหารความเสี่ยงดังกล่าว ผู้บริหารควรมีการประเมินความเสี่ยงและวิเคราะห์อย่างถี่ถ้วน รวมทั้งพิจารณาเงื่อนไขสัญญาโดยละเอียด นอกจากนี้ ผู้บริหารควรจัดให้มีกระบวนการติดตามและการกำกับดูแลอย่างต่อเนื่อง

การบริหารความเสี่ยง

ผู้บริหารระดับสูงของ สง. มีความรับผิดชอบในการทำความเข้าใจความเสี่ยงที่เกี่ยวข้องกับการใช้บริการของผู้ให้บริการที่อยู่ต่างประเทศ และดูแลให้มีการบริหารความเสี่ยงที่มีประสิทธิผล **ผู้บริหารควรพิจารณาความสอดคล้องของการใช้บริการจากผู้ให้บริการที่อยู่ในต่างประเทศเทียบกับกลยุทธ์การดำเนินธุรกิจและกลยุทธ์ทางด้านเทคโนโลยีของ สง. รวมทั้งพิจารณาความสามารถของ สง. ในการควบคุมหรือลดความเสี่ยงที่เกิดขึ้นให้อยู่ในระดับที่ยอมรับได้** ผู้บริหารควรพิจารณาประเด็น เช่น การเลือกใช้กฎหมาย และขอบเขตอำนาจของกฎหมาย เป็นต้น ก่อนที่จะมีการลงนามในสัญญาการใช้บริการ นอกจากนี้ ควรมีการวิเคราะห์อย่างถี่ถ้วนและกำหนดนโยบายการ

[2] คำว่า ผู้ให้บริการภายนอกที่อยู่ต่างประเทศ หรือ ผู้ให้บริการที่อยู่ต่างประเทศ หมายถึง ผู้ให้บริการ รวมถึงที่เป็นบริษัทในเครือหรือบริษัทที่มีส่วนเกี่ยวข้องกับ สง. มีการดำเนินงานในส่วนที่เกี่ยวข้องกับการให้บริการอยู่ในต่างประเทศ และการดำเนินการอยู่ภายใต้กฎหมายของประเทศอื่น ซึ่งรวมถึงผู้ให้บริการที่อยู่นอกประเทศไทยและให้บริการกับสาขาธนาคารพาณิชย์ไทยในต่างประเทศ และครอบคลุมถึงกรณีผู้รับจ้างช่วงงานต่อของผู้ให้บริการในประเทศมีการดำเนินงานอยู่ต่างประเทศ

บริหารความเสี่ยง รวมถึงมีกระบวนการกำกับดูแลและติดตามที่เหมาะสม นโยบายและขั้นตอนปฏิบัติงานดังกล่าวควรครอบคลุมความเสี่ยงที่เกิดจากการใช้บริการของผู้ให้บริการภายนอกที่อยู่ในประเทศ ซึ่งมีการใช้บริการของผู้ให้บริการที่อยู่ต่างประเทศเช่นเดียวกัน เพิ่มเติมจากการพิจารณาความเสี่ยงที่มีลักษณะเฉพาะกับผู้ให้บริการที่อยู่ในต่างประเทศ เช่น ความเสี่ยงของประเทศ ความเสี่ยงของการปฏิบัติตามกฎหมายของประเทศอื่นที่มิใช่ประเทศเดียวกับผู้ใช้บริการ เป็นต้น

ความเสี่ยงของประเทศ

ความเสี่ยงของประเทศเป็นความเสี่ยงที่เกิดจากสภาพเศรษฐกิจ สังคมและการเมืองในประเทศอื่นที่มิใช่ประเทศผู้ใช้บริการ ส่งผลกระทบในทางลบต่อความสามารถของผู้ให้บริการในการปฏิบัติงานให้ได้ตามข้อตกลงของระดับการให้บริการ ในบางสถานการณ์ ความเสี่ยงของประเทศส่งผลให้เกิดความเสียหายแก่ข้อมูล การวิจัย และการพัฒนา และในการบริหารความเสี่ยงของประเทศ สง. จะต้องรวบรวมและประเมินข้อมูลที่เกี่ยวกับสภาพเศรษฐกิจ เหตุการณ์ทางสังคมและการเมืองต่างประเทศ เพื่อประเมินความเสี่ยงของการใช้บริการของผู้ให้บริการที่อยู่ในประเทศนั้น **กระบวนการบริหารความเสี่ยงควรครอบคลุมเรื่องการจัดทำแผนสำรองฉุกเฉินและแผนรองรับความต่อเนื่องของการให้บริการ รวมทั้งกลยุทธ์การยกเลิกบริการ (Exit Strategies) ในกรณีที่ผู้ให้บริการไม่สามารถให้บริการได้**

ความเสี่ยงของการปฏิบัติตามกฎหมาย

การใช้บริการของผู้ให้บริการที่อยู่ในต่างประเทศอาจส่งผลกระทบต่อการปฏิบัติตามกฎหมายท้องถิ่นของประเทศผู้ใช้บริการ **ซึ่งการใช้บริการของผู้ให้บริการที่อยู่ในต่างประเทศไม่ควรทำให้การดำเนินงานของ สง. ขัดต่อกฎหมายของประเทศตนเอง** สง. ควรพิจารณาผลกระทบและข้อกำหนดในการปฏิบัติงานตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือกฎระเบียบทางการของต่างประเทศ[3] รวมถึงการกำหนดโทษ และข้อกำหนดเกี่ยวกับการส่งเทคโนโลยีที่เกี่ยวข้องกับการเข้ารหัสออกนอกประเทศ ซึ่งจะกล่าวในส่วนต่อไป

การควบคุมการส่งออก

กฎหมายของประเทศสหรัฐอเมริกาจำกัดการส่งออกของ Software และรายการอื่นๆ ซึ่งรวมถึงการเข้ารหัสทุกรูปแบบ สง. ควรพิจารณาให้มั่นใจว่าผู้ให้บริการปฏิบัติตามกฎหมายการส่งออก ซึ่งควรมีระบุไว้ในสัญญาด้วย

[3] สง. ควรระบุและทำความเข้าใจกฎหมายของต่างประเทศที่เกี่ยวข้องกับข้อมูลที่โอนข้ามประเทศผ่านทางอินเตอร์เน็ต และข้อมูลที่จัดเก็บและประมวลผลด้วยคอมพิวเตอร์ในต่างประเทศด้วย

การวิเคราะห์อย่างถี่ถ้วน

ผู้บริหารของ สง. ที่อยู่ระหว่างพิจารณาการใช้บริการจากผู้ให้บริการที่อยู่ในต่างประเทศควรดำเนินการวิเคราะห์อย่างถี่ถ้วนเช่นเดียวกับการใช้บริการจากผู้ให้บริการที่อยู่ในประเทศ ก่อนคัดเลือกและจัดทำสัญญากับผู้ให้บริการ กระบวนการควรครอบคลุมการประเมินฐานะความมั่นคงทางการเงินข้อผูกมัดในการให้บริการ และผลกระทบของกฎหมาย มาตรฐานการบัญชีและวิธีปฏิบัติทางธุรกิจของประเทศนั้นๆ นอกจากนั้น ผู้บริหารควรพิจารณาปัจจัยเรื่อง ระยะทาง ภาษา การเปลี่ยนแปลงทางสังคม เศรษฐกิจและการเมืองที่ส่งผลกระทบต่อความสามารถในการให้บริการได้ตรงตามความต้องการของ สง. ผู้บริหารควรพิจารณาค่าใช้จ่ายและความสมเหตุสมผลของการบริหารความสัมพันธ์ข้ามชาติ ได้แก่ ค่าใช้จ่ายในการบริหารและติดตามผู้ให้บริการในต่างประเทศ

สัญญา

สัญญาการใช้บริการควรระบุให้ครอบคลุมความเสี่ยงตามที่ได้มีการประเมินและวิเคราะห์อย่างถี่ถ้วน เมื่อทำการตรวจสอบสัญญาการใช้บริการ ผู้ตรวจสอบควรพิจารณาหัวข้อดังต่อไปนี้

การรักษาความปลอดภัย ความลับ และความเป็นเจ้าของข้อมูล

ผู้บริหารควรจัดทำข้อตกลงในสัญญาให้ปกป้องข้อมูลส่วนบุคคลของลูกค้าและความลับของข้อมูล สง. โดยให้เป็นไปตามกฎหมายและระเบียบทางการ

ข้อตกลงกับผู้ให้บริการที่อยู่ต่างประเทศควรครอบคลุมการโอนข้อมูลไปให้หน่วยงานที่อยู่ในต่างประเทศ ซึ่ง สง. จะต้องยังคงมีลิขสิทธิ์ในข้อมูลนั้น ไม่ว่าข้อมูลจะถูกประมวลผล จัดเก็บ ทำสำเนา หรือนำไปแปรรูปใหม่ด้วยวิธีการใดก็ตาม

อำนาจของผู้กำกับดูแล

การใช้บริการของผู้ให้บริการที่อยู่ในต่างประเทศจะต้องเป็นไปตามกฎระเบียบของผู้กำกับดูแลทางการของ สง. และของผู้ให้บริการ มีกรณีที่บางประเทศมีข้อกำหนดให้หน่วยงานที่จะเข้าตรวจสอบการดำเนินงานของผู้ให้บริการที่อยู่ในประเทศนั้นๆ ต้องได้รับความยินยอมจากหน่วยงานที่กำกับดูแลผู้ให้บริการก่อนและบางประเทศมีข้อห้ามในการเปิดเผยรายงานตรวจสอบของหน่วยงานกำกับดูแลทางการให้ผู้กำกับดูแลต่างประเทศหรือผู้ให้บริการในต่างประเทศ เว้นแต่จะได้รับอนุญาตจากผู้กำกับดูแล ซึ่ง สง. ต้องมีหนังสือแจ้งการขออนุญาตดังกล่าวเป็นลายลักษณ์อักษร

การเลือกใช้กฎหมาย

ก่อนลงนามในสัญญากับผู้ให้บริการ สง. ควรพิจารณาอย่างรอบคอบว่าการใช้บริการอยู่ภายใต้กรอบกฎหมายใด และควรมีการหารือแนวทางแก้ไขหากเกิดกรณีพิพาทขึ้นกับทุกฝ่ายที่เกี่ยวข้องก่อนด้วย

ข้อกำหนดต้องมุ่งเรื่องการรักษาความต่อเนื่องของบริการ การเข้าถึงข้อมูล และการป้องกันข้อมูลลูกค้า ซึ่งจะยิ่งทวีความสำคัญมากขึ้นสำหรับกรณีการใช้บริการจากผู้ให้บริการที่อยู่ในต่างประเทศ เนื่องจากต้องพิจารณาว่ามีกฎหมายของประเทศใดบ้างที่จะใช้ควบคุมการดำเนินงานของแต่ละฝ่ายที่เกี่ยวข้อง ซึ่งกฎหมายของแต่ละประเทศอาจมีความแตกต่างกันไป โดยเฉพาะประเด็นในเรื่องการคุ้มครองลูกค้าของ สง. ด้วยเหตุนี้ การวิเคราะห์อย่างถี่ถ้วนจึงต้องครอบคลุมประเด็นเรื่องกฎหมายท้องถิ่น ซึ่งควรมีที่ปรึกษาทางกฎหมายที่มีศักยภาพในการประเมินการมีผลบังคับใช้ของเงื่อนไขของสัญญาแต่ละข้อ

การติดตามและการกำกับดูแล

การติดตามผู้ให้บริการที่อยู่ในต่างประเทศใช้ขั้นตอน/กระบวนการเช่นเดียวกับการติดตามผู้ให้บริการในประเทศ นอกจากนั้น ควรต้องปฏิบัติตามแนวทางที่จะกล่าวในส่วนนี้ด้วย ผู้บริหารควรติดตามการดำเนินงานและฐานะภายในประเทศนั้น

สง. ควรพิจารณาว่าผู้ให้บริการที่อยู่ในต่างประเทศจัดให้มีการควบคุมการรักษาความปลอดภัย ขั้นตอนการปฏิบัติงาน การกู้ธุรกิจกลับคืนสู่สภาวะปกติ และแผนสำรองฉุกเฉินด้านเทคโนโลยีสารสนเทศที่เพียงพอ (พร้อมทั้งมีการทดสอบเป็นประจำ) ขอบเขตการทำประกันภัย และการปฏิบัติตามกฎหมาย ในการประเมินความเสี่ยงด้านการรักษาความปลอดภัย สง. ควรติดตามผู้ให้บริการที่อยู่ในต่างประเทศเพื่อให้มั่นใจว่ามีการปฏิบัติงานด้านการรักษาความปลอดภัยที่เป็นไปตามมาตรฐานและระเบียบทางการ

สง. ควรติดตามสภาพเศรษฐกิจและการเมืองของต่างประเทศเพื่อพิจารณาว่าการเปลี่ยนแปลงในเรื่องดังกล่าวจะส่งผลกระทบต่อความสามารถในการให้บริการมากน้อยเพียงใด

การเข้าถึงข้อมูลของผู้กำกับดูแล

ผู้กำกับดูแลควรสามารถตรวจสอบบริการของผู้ให้บริการที่อยู่ในต่างประเทศได้ โดยไม่คำนึงว่าการดำเนินงานจะอยู่ในประเทศหรือต่างประเทศ สง. จะต้องจัดเก็บข้อมูลและเอกสารสนับสนุนการใช้บริการเป็นภาษาอังกฤษ เอกสารดังกล่าว ได้แก่ สัญญาการใช้บริการ ความเห็นของที่ปรึกษาทางกฎหมาย รายงานการวิเคราะห์อย่างถี่ถ้วน ผลการตรวจสอบ งบการเงิน รายงานผลการ

ดำเนินงาน ข้อมูลสำคัญอื่นๆ[4] นอกจากนั้น สง. ควรมีแผนสำรองฉุกเฉินที่เหมาะสมเพื่อให้มั่นใจว่าหากเกิดเหตุกาณ์ฉุกเฉินหรือมีการจำกัดการใช้บริการอันเป็นผลมาจากความเสี่ยงของประเทศ ความเสี่ยงด้านการเงิน และความเสี่ยงด้านปฏิบัติการของผู้ให้บริการ สง. ก็จะยังคงสามารถเข้าถึงข้อมูลสำคัญ ใช้บริการได้อย่างต่อเนื่อง และฟื้นธุรกิจกลับคืนสู่สภาวะปกติได้

ประเด็นพิจารณาในการตรวจสอบ

ผู้กำกับดูแลควรตรวจสอบบริการของผู้ให้บริการที่อยู่ในต่างประเทศในส่วนที่ให้แก่ สง.

ผู้กำกับดูแลจะมุ่งที่การสอบทานความเพียงพอของการวิเคราะห์อย่างถี่ถ้วนของ สง. การประเมินความเสี่ยง และขั้นตอนในการบริหารความเสี่ยงซึ่งรวมความเสี่ยงด้านการปฏิบัติตามกฎหมาย และการเข้าถึงข้อมูลที่สำคัญ รวมทั้งประเมินสัญญาการใช้บริการของ สง. และกระบวนการติดตามหรือกำกับดูแลผู้ให้บริการ และการตรวจสอบภายในและภายนอกของผู้ให้บริการ

การใช้บริการจากผู้ให้บริการที่อยู่ในต่างประเทศ (รวมถึงกรณีการประมวลผลข้อมูลสำคัญอยู่ต่างประเทศ) ต้องไม่จำกัดหรือลดอำนาจของผู้กำกับดูแลในการเข้าตรวจสอบ สง. ด้วยเหตุนี้ สง. ไม่ควรมีการใช้บริการกับผู้ให้บริการที่อยู่ภายใต้กฎหมายที่จำกัดหรือลดอำนาจของผู้กำกับดูแลในการเข้าถึงข้อมูล **ซึ่งหน่วยงานด้านกฎหมายหรือที่ปรึกษาทางกฎหมายควรวิเคราะห์กฎหมายต่างประเทศในประเด็นที่เกี่ยวกับการเข้าถึงข้อมูลเพื่อวัตถุประสงค์ในการตรวจสอบของผู้กำกับดูแลด้วย**

[4] ในกรณีที่สาขาต่างประเทศของ สง. ใช้บริการของผู้ให้บริการที่อยู่ในประเทศนั้น ไม่ว่าจะเป็นส่วนที่เกี่ยวข้องกับการดำเนินงานภายในสาขาหรือส่วนที่เกี่ยวข้องกับธุรกรรมข้ามชาติ สำเนาของข้อมูลจากการใช้บริการดังกล่าวต้องมีการจัดเก็บที่สาขาต่างประเทศของ สง. นั้น รวมทั้งมีการจัดเก็บที่สำนักงานใหญ่ด้วย