คปภ.

สำนักงานคณะกรรมการกำกับและส่งเสริม
การประกอบธุรกิจประกันภัย(คปภ.)

แนวปฏิบัติเรื่อง
หลักเกณฑ์การกำกับดูแลการใช้บริการจาก
ผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ
พ.ศ. ๒๕๖๔

ที่มา / หลักการ	**ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต / ประกันวินาศภัย พ.ศ. ๒๕๖๓**

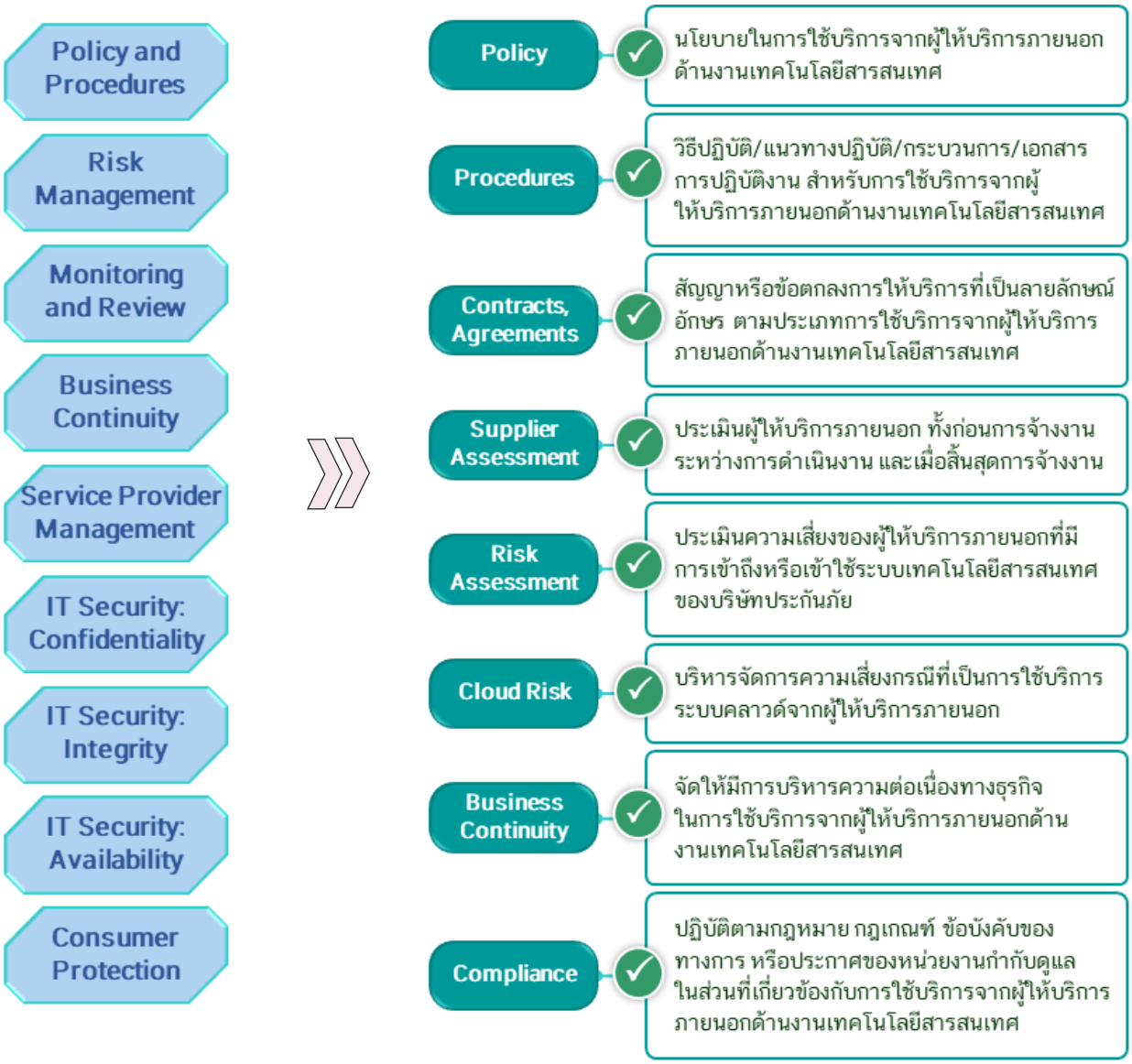
ปัจจุบัน ธุรกิจประกันภัยได้มีการใช้บริการจากผู้ให้บริการภายนอกมากขึ้น เพื่อให้การพัฒนาระบบเทคโนโลยีสารสนเทศ และการจัดสรรทรัพยากรด้านงานเทคโนโลยีสารสนเทศของบริษัทอย่างมีประสิทธิภาพ ทั้งในด้านการจัดเก็บข้อมูล การประมวลผล หรือการดำเนินการใดๆ ที่เกี่ยวข้องกับข้อมูลผู้เอาประกันภัย หรือข้อมูลสำคัญของบริษัท สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) ได้เล็งเห็นความสำคัญของการกำกับดูแลและสร้างมาตรฐานให้บริษัทประกันภัย ในการกำกับดูแล การบริหารจัดการความเสี่ยง และการควบคุมความเสี่ยงที่อาจเกิดขึ้นเนื่องจากผู้ให้บริการภายนอก (third party management) หรือมีพันธมิตรทางธุรกิจที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัท หรือสามารถเข้าถึงข้อมูลสำคัญของบริษัท หรือของลูกค้าของบริษัท ได้ รวมทั้งการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ และสอดคล้องตามข้อกำหนดใน “ประกาศ คปภ. เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต / ประกันวินาศภัย พ.ศ. ๒๕๖๓” (ประกาศ IT risk management) **“<u>ข้อ ๒๓</u> ในกรณีที่บริษัทมีการจัดจ้างผู้ให้บริการภายนอก (third party management) หรือมีพันธมิตรทางธุรกิจที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัท หรือสามารถเข้าถึงข้อมูลสำคัญของบริษัท หรือของลูกค้าของบริษัทได้ บริษัทต้องมีการกำหนดกระบวนการและหลักเกณฑ์ในการประเมินและคัดเลือกผู้ให้บริการภายนอก โดยต้องจัดทำสัญญาจ้างในการให้บริการ และกำหนดเงื่อนไขให้ผู้ให้บริการภายนอกปฏิบัติตามนโยบายการรักษาความปลอดภัยของบริษัท รวมถึงต้องกำหนดข้อตกลงระดับการให้บริการ (service level agreement : SLA) พร้อมทั้งมีการตรวจสอบและติดตามการให้บริการอย่างสม่ำเสมอ”**

ในการนี้ เพื่อเป็นประโยชน์ต่อบริษัทในการทำความเข้าใจ และสามารถปฏิบัติตามข้อกำหนดในเรื่องดังกล่าวได้อย่างถูกต้องครบถ้วน เป็นไปตามเจตนารมณ์ของสำนักงานในการออกประกาศฉบับนี้ สำนักงาน คปภ. จึงได้จัดทำแนวปฏิบัติฉบับนี้ขึ้น เพื่อเป็นส่วนหนึ่งของประกาศ IT risk management และใช้ประกอบการพิจารณาหรือออกคำสั่ง เพื่อให้บริษัทดำเนินการเกี่ยวกับการกำกับดูแล การบริหารจัดการความเสี่ยง และการควบคุมความเสี่ยงที่อาจเกิดขึ้นเนื่องจากผู้ให้บริการภายนอก (third party management) หรือมีพันธมิตรทางธุรกิจที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัท หรือสามารถเข้าถึงข้อมูลสำคัญของบริษัท หรือของลูกค้าของบริษัทได้ รวมทั้งการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ ที่เหมาะสมสอดคล้องตาม ลักษณะ ขนาด ความซับซ้อนเทคโนโลยีที่ใช้ในการดำเนินธุรกิจ และความเสี่ยงที่อาจเกิดขึ้น

นิยามคำศัพท์

การใช้บริการจากผู้ให้บริการภายนอก	การใช้บริการจากผู้ให้บริการภายนอกในการดำเนินการด้านงานเทคโนโลยีสารสนเทศ (IT outsourcing) ของบริษัท ซึ่งโดยปกติแล้วบริษัทต้องดำเนินการเอง และให้รวมถึงผู้ให้บริการภายนอกที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัท หรือสามารถเข้าถึงข้อมูลสำคัญของบริษัท หรือของลูกค้าของบริษัทได้ และการใช้บริการระบบคลาวด์ (cloud computing) และให้หมายความรวมถึง IT third party ด้วย
การใช้บริการระบบคลาวด์ (cloud computing)	การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศในงานด้านโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ หรือระบบงานด้านเทคโนโลยีสารสนเทศที่มีการนำเทคโนโลยี cloud computing มาใช้ในการให้บริการผ่านเครือข่ายอินเตอร์เน็ต เพื่อประโยชน์ในการจัดเก็บข้อมูล การประมวลผล หรือการดำเนินการใดๆ เกี่ยวกับข้อมูล หรือระบบงานให้แก่บริษัท
บริการที่มีความเสี่ยงหรือนัยสำคัญ	บริการหรือระบบที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือระบบงานด้านเทคโนโลยีสารสนเทศที่มีการเชื่อมต่อ หรือมีการเข้าถึงจากบุคคลภายนอก โดยจะมีการเข้าถึงข้อมูลที่มีความสำคัญ เช่น ข้อมูลผู้เอาประกันภัย ข้อมูลลูกค้า ข้อมูลเกี่ยวกับแผนธุรกิจ ข้อมูลทางการเงิน ข้อมูลเกี่ยวกับการพัฒนาผลิตภัณฑ์หรือเทคโนโลยี เป็นต้น

ภาพรวมการกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอก



<u>ส่วนที่ ๑ : การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอก</u>

การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ และการใช้บริการจากผู้ให้บริการภายนอกที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัท หรือสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลูกค้าของบริษัทได้ (การใช้บริการจากผู้ให้บริการภายนอก) บริษัทต้องจัดให้มีการกำกับดูแลและการบริหารจัดการความเสี่ยงจากการใช้บริการที่อาจเกิดขึ้นในรูปแบบที่เปลี่ยนแปลงไปจากการดำเนินงานตามปกติที่กระทำโดยบริษัทเอง รวมทั้งรับผิดชอบต่อการให้บริการอย่างต่อเนื่องแก่ผู้ใช้บริการ โดยคงความน่าเชื่อถือของการให้บริการเช่นเดียวกับบริษัทเป็นผู้ดำเนินการด้วยตนเอง

คณะกรรมการบริษัท มีหน้าที่ในการกำกับดูแลให้บริษัทมีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรักษาความปลอดภัยจากภัยไซเบอร์ ที่ครอบคลุมการใช้บริการจากผู้ให้บริการภายนอกโดยดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

(๑) กำหนดกลยุทธ์ที่ชัดเจนในการตัดสินใจใช้บริการจากผู้ให้บริการภายนอก เช่น เหตุผลความจำเป็นทางธุรกิจ ประโยชน์ที่ได้รับและต้นทุน รวมทั้งต้องพิจารณาว่าการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศนั้นไม่ขัดต่อกฎหมายและข้อบังคับที่บริษัทต้องปฏิบัติตาม และไม่ก่อให้เกิดช่องโหว่ที่นำไปสู่การเกิดการทุจริตที่ร้ายแรง หรือก่อให้เกิดภัยคุกคามด้านเทคโนโลยีสารสนเทศทั้งจากภายในและภายนอก

(๒) จัดให้มีโครงสร้าง และกำหนดหน้าที่ความรับผิดชอบเกี่ยวกับการบริหารจัดการผู้ให้บริการภายนอกเป็นไปตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ ๓ ระดับ (three lines of defense) เพื่อให้มีการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจนและมีการถ่วงดุลอำนาจในการทำหน้าที่ในแต่ละระดับอย่างเหมาะสม

(๓) กำกับดูแล และพิจารณาให้ความเห็นชอบการใช้บริการ IT outsourcing ของบริษัทให้สอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจ

ทั้งนี้ สำหรับกรณีที่บริษัทพิจารณาแล้วว่า การใช้บริการจากผู้ให้บริการภายนอกเป็นงานด้านเทคโนโลยีสารสนเทศที่มีความสำคัญต่อบริษัท เช่น ศูนย์คอมพิวเตอร์หลัก (data center) ศูนย์คอมพิวเตอร์สำรองที่ทำงานร่วมกับระบบหลักอยู่ตลอดเวลา (DR site – hot site) ระบบเครือข่ายสื่อสารหลักหรือระบบเครือข่ายสื่อสารส่วนกลางที่ทำหน้าที่เป็นศูนย์กลางของเครือข่ายทั้งหมด (core network) ระบบ ERP หรือระบบหลักที่เชื่อมโยงระบบงานต่างๆ ขององค์กรเข้าด้วยกันในส่วนที่ต้องทำงานตลอดเวลา ระบบฐานข้อมูลลูกค้า ระบบฐานข้อมูลกลางที่จัดเก็บ รวบรวม หรือประมวลผลข้อมูลลูกค้าของบริษัทที่มีการดำเนินการรวมอยู่ส่วนกลางเป็นแหล่งเดียว รวมถึงระบบจ่ายค่าสินไหมทดแทน และระบบบันทึกข้อมูลกรมธรรม์ประกันภัยอัตโนมัติ (กรณีที่ไม่มีระบบงานสำรองอื่น) เป็นต้น บริษัทต้องนำเสนอรายละเอียดของการใช้บริการจากผู้ให้บริการภายนอก พร้อมผลการประเมินความเสี่ยงโดยละเอียดให้กับคณะกรรมการบริษัท หรือคณะกรรมการชุดย่อย หรือผู้บริหารที่ได้รับมอบหมาย เพื่อเป็นข้อมูลประกอบการพิจารณาให้ความเห็นชอบทั้งก่อนเริ่มใช้บริการ หรือเมื่อมีการเปลี่ยนการใช้บริการอย่างมีนัยสำคัญตามที่บริษัทกำหนด หรือการต่ออายุสัญญา

(๔) กำหนดนโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) และนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ให้ครอบคลุมการใช้บริการจากผู้ให้บริการภายนอก โดยแนวทางการบริหารความเสี่ยง ควรสอดคล้องกับความเสี่ยงที่อาจเกิดขึ้นภายใต้กรอบหลักการด้านเทคโนโลยีที่สำคัญ ๓ ประการ คือ ๑) การรักษาความลับ (confidentiality) ๒) การรักษาความถูกต้องเชื่อถือได้ (integrity) และ ๓) ความพร้อมใช้ (availability) ของระบบเทคโนโลยีสารสนเทศของบริษัท

(๕) กำกับดูแลให้บริษัทมีการบริหารจัดการความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการผู้ให้บริการภายนอกอย่างเหมาะสม โดยมีการประเมินตนเอง (self-assessment) มีการควบคุม และจัดการความเสี่ยงอย่างมีประสิทธิภาพ

(๖) กำกับดูแลให้มีการติดตามผลการดำเนินการจากการใช้บริการจากผู้ให้บริการภายนอก ทั้งนี้ ในกรณีที่ผู้ให้บริการภายนอกมีการให้ผู้ให้บริการภายนอกรายอื่นรับช่วงจัดการงานด้านเทคโนโลยีสารสนเทศที่ให้บริการแก่บริษัท (sub-contract) หรือการใช้บริการจากผู้ให้บริการภายนอกรายอื่นเป็นทอดๆ บริษัทต้องมั่นใจว่าผู้ให้บริการภายนอกจะรับผิดชอบต่อการให้บริการด้านงานเทคโนโลยีสารสนเทศแก่บริษัทเสมือนกับที่ผู้ให้บริการภายนอกเป็นผู้ให้บริการด้วยตนเอง

ทั้งนี้ คณะกรรมการบริษัทสามารถมอบหมาย หรือแต่งตั้งคณะกรรมการชุดย่อย หรือผู้บริหารดำเนินการในเรื่องดังกล่าวข้างต้นได้ตามความเหมาะสม

<u>ส่วนที่ ๒ : การบริหารจัดการความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอก</u>

บริษัทต้องจัดให้มีการบริหารจัดการความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอก รวมถึงการใช้บริการระบบคลาวด์ โดยกำหนดนโยบายการบริหารจัดการความเสี่ยง ให้ครอบคลุมความเสี่ยงจากการใช้บริการเป็นลายลักษณ์อักษร และสอดคล้องกับนโยบายการบริหารจัดการความเสี่ยงโดยรวมของบริษัท และนโยบายอื่นที่เกี่ยวข้อง เช่น นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) คำนึงถึงขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการและความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ

ทั้งนี้ นโยบายดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย และได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งควรสื่อสารนโยบายให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึงและควบคุมดูแลให้ปฏิบัติตามนโยบาย

นโยบายการบริหารจัดการความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอก ควรครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(๑) โครงสร้างการบริหารความเสี่ยง และหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องในการกำกับดูแลและบริหารจัดการความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอก รวมทั้งแนวทางและผู้รับผิดชอบในการบริหารจัดการความเสี่ยง

(๒) เกณฑ์การจัดระดับความเสี่ยง สอดคล้องกับระดับความมีนัยสำคัญของการใช้บริการ รวมทั้งการเชื่อมต่อ หรือการสามารถเข้าถึงข้อมูลของผู้ให้บริการภายนอก

(๓) การบริหารจัดการความเสี่ยงที่ครอบคลุมวงจรการใช้บริการจากผู้ให้บริการภายนอก และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ครอบคลุมตามหลักการ CIA

(๔) เกณฑ์การขออนุมัติเพื่อพิจารณาให้ความเห็นชอบ และการรายงานต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย

(๕) การตรวจสอบการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลของผู้ให้บริการภายนอก

(๖) แนวทางในการเตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้น และมีผลกระทบต่อบริษัทอย่างมีนัยสำคัญ เพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง

(๗) การรายงานผลการบริหารความเสี่ยงให้คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสม

ทั้งนี้ บริษัทควรมีความรู้ความเข้าใจเทคโนโลยีที่ใช้บริการจากผู้ให้บริการภายนอก และสามารถประเมินความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการได้

<u>ตัวอย่าง ประเด็นสถานการณ์ความเสี่ยงจากการใช้บริการ IT outsourcing (risk scenarios)</u>

สถานการณ์ความเสี่ยง	ตัวอย่างประเด็นสถานการณ์ความเสี่ยง	ตัวอย่างมาตรการ/แนวทางการจัดการความเสี่ยง
การคัดเลือก/ประสิทธิภาพของผู้ให้บริการภายนอก (selection/performance of third-party)	(๑) การสนับสนุนและการให้บริการของผู้ขายหรือผู้ให้บริการ มีไม่เพียงพอ ไม่เป็นไปตามข้อตกลงระดับการให้บริการ	- ข้อกำหนดระดับการให้บริการในสัญญา (SLA) - การติดตามและตรวจทานรายงานการให้บริการ - การประชุมรายงานความคืบหน้า (เช่น รายเดือน)
	(๒) ผู้ให้บริการภายนอกไม่มีประสิทธิภาพเพียงพอ สำหรับข้อตกลงการใช้บริการ	- ข้อกำหนดคุณสมบัติของบุคลากรและการเปลี่ยนบุคลากร (คุณสมบัติ วุฒิบัตรวิชาชีพ หนังสือรับรองบุคลากรของผู้ให้บริการ)

สถานการณ์ความเสี่ยง	ตัวอย่างประเด็นสถานการณ์ความเสี่ยง	ตัวอย่างมาตรการ/แนวทางการจัดการความเสี่ยง
	จากภายนอก ที่เป็นโครงการขนาดใหญ่และมีระยะเวลานานในการดำเนินการ	- ข้อกำหนดแผนงานโครงการ และข้อกำหนดสิ่งส่งมอบงานรายงวด - การประชุมรายงานความคืบหน้า (เช่น รายเดือน)
	(๓) ผู้ให้บริการภายนอกไม่มีประสิทธิภาพเพียงพอ สำหรับเทคโนโลยีใหม่ๆ หรือที่ต้องการความเชี่ยวชาญเฉพาะด้าน	- ข้อกำหนดความต้องการของระบบ - ข้อกำหนดตัวอย่างระบบ / Proof of Concept (PoC) - ข้อกำหนดคุณสมบัติของบุคลากรและการเปลี่ยนบุคลากร (คุณสมบัติ วุฒิบัตรวิชาชีพการรับรองบุคลากรของผู้ให้บริการ)
	(๔) ผู้ให้บริการภายนอกมีการปรับเปลี่ยนบุคลากรในทีมบ่อยครั้ง ทำให้ขาดความต่อเนื่องในการดำเนินการ	- ข้อกำหนดคุณสมบัติของบุคลากรและการเปลี่ยนบุคลากร (คุณสมบัติ วุฒิบัตรวิชาชีพหนังสือรับรองบุคลากรของผู้ให้บริการ)
	(๕) ผู้ให้บริการเข้าถึงข้อมูลสำคัญหรือนำข้อมูลออกจากระบบคอมพิวเตอร์ของบริษัท โดยไม่ได้รับอนุญาต	- การประเมินความเสี่ยงประเภทการเข้าถึงระบบ/ข้อมูลของบริษัทโดยผู้ให้บริการ - การลงนามเอกสารไม่เปิดความลับ (non-disclosure agreement) - การรับทราบและยินยอมปฏิบัติตามนโยบายและมาตรการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท
	(๖) การให้บริการได้อย่างต่อเนื่องของผู้ให้บริการ ไม่มีประสิทธิภาพ หรือมีไม่เพียงพอ เมื่อเกิดเหตุฉุกเฉินในภาวะวิกฤต	- ข้อกำหนดระดับการให้บริการในสัญญา (SLA) - แผนฉุกเฉิน แผนสำรอง หรือแผนรองรับการดำเนินงานต่อเนื่องของผู้ให้บริการ ในการให้บริการตามข้อกำหนด
	(๗) การกระจุกตัวของการให้บริการโดยผู้ให้บริการ (concentration risk)	- ข้อกำหนดระดับการให้บริการในสัญญา (SLA) - แผนฉุกเฉิน แผนสำรอง หรือแผนรองรับการดำเนินงานต่อเนื่องของผู้ให้บริการ ในการให้บริการตามข้อกำหนด
	(๘) การทิ้งงานของผู้ให้บริการภายนอก	- ข้อกำหนดบทปรับ/บทลงโทษ/ข้อกำหนดสงวนสิทธิตามกฎหมาย
	(๙) ไม่มีการกำหนดข้อตกลงการให้บริการ (SLA) หรือเงื่อนไขในการปฏิบัติงาน ในสัญญาจ้างผู้ให้บริการภายนอก	- ข้อกำหนดระดับการให้บริการในสัญญา (SLA) การติดตามและตรวจทานรายงานการให้บริการ การประชุมรายงานความคืบหน้า (เช่น รายเดือน)
	(๑๐) ไม่มีการกำหนดแนวปฏิบัติ/กระบวนการในกรณีที่มีการเปลี่ยนแปลงเงื่อนไข/ข้อตกลงกับผู้ให้บริการภายนอก	- ข้อกำหนดกรณีมีการเปลี่ยนแปลงขอบเขต ระยะเวลา ค่าใช้จ่าย หรือเงื่อนไขอื่นใดตามสัญญา - กระบวนการ/การประชุมร่วมเพื่อพิจารณาแนวทางดำเนินการตามการเปลี่ยนแปลง

สถานการณ์ความเสี่ยง	ตัวอย่างประเด็นสถานการณ์ความเสี่ยง	ตัวอย่างมาตรการ/แนวทางการจัดการความเสี่ยง
	(๑๑) ไม่มีการประเมินผู้ให้บริการภายนอก ก่อนเริ่มดำเนินการ	- การประเมินก่อนเริ่มดำเนินการ - การประเมินความเสี่ยงในการใช้งานผู้ให้บริการภายนอก - ข้อกำหนดระดับการให้บริการในสัญญา (SLA) รายการสิ่งส่งมอบตามสัญญา
	(๑๒) ไม่มีการประเมินผู้ให้บริการภายนอก ในระหว่างดำเนินการตามสัญญา	- การประเมินความเสี่ยงในการใช้งานผู้ให้บริการภายนอก - ข้อกำหนดระดับการให้บริการในสัญญา (SLA) - การติดตามและตรวจทานรายงานการให้บริการ การตรวจรับงาน/สิ่งส่งมอบ
	(๑๓) ไม่มีการประเมินผู้ให้บริการภายนอก เมื่อสิ้นสุดสัญญา	- การประเมินความเสี่ยงในการใช้งานผู้ให้บริการภายนอก - ข้อกำหนดระดับการให้บริการในสัญญา (SLA) - การติดตามและตรวจทานรายงานการให้บริการ - การตรวจรับงาน/สิ่งส่งมอบ - การประเมินผู้ให้บริการเมื่อสิ้นสุดสัญญา

ตัวอย่าง ความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศที่บริษัทควรพิจารณา

ประเภทความเสี่ยง	ตัวอย่างความเสี่ยง
ความเสี่ยงด้านกลยุทธ์ (strategic risk)	ผู้ให้บริการภายนอกดำเนินงานไม่สอดคล้องกับกลยุทธ์ของบริษัท
ความเสี่ยงด้านปฏิบัติการ (operational risk)	- ความผิดพลาดจากระบบงาน - กระบวนการจัดการภายในของผู้ให้บริการภายนอกไม่มีประสิทธิภาพ - เกิดกรณีทุจริต - ความเสี่ยงที่บริษัทจะไม่สามารถตรวจสอบผู้ให้บริการภายนอก
ความเสี่ยงด้านการปฏิบัติตามกฎหมาย (compliance risk)	- ผู้ให้บริการภายนอกไม่ดำเนินการตามกฎหมายที่เกี่ยวข้อง - ผู้ให้บริการภายนอกไม่ดำเนินการตามกฎหมายคุ้มครองผู้บริโภค - ผู้ให้บริการภายนอกไม่มีระบบการกำกับดูแลการปฏิบัติตามกฎหมายและควบคุมเพียงพอ
ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT-related risk)	- ความผิดพลาดจากระบบงาน - กระบวนการจัดการสิทธิ์ใช้งานระบบที่ไม่มีประสิทธิภาพ - การหยุดชะงักของระบบเครือข่ายสื่อสารหรือโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ - ความเสี่ยงด้านบุคลากรที่ไม่มีบุคลากรสำรองหรือผู้เชี่ยวชาญทดแทน - ความเสี่ยงจากที่ไม่มีการสำรองข้อมูล หรือการสำรองข้อมูลที่ไม่มีประสิทธิผล - ข้อมูลสำคัญถูกเปิดเผยหรือเปลี่ยนแปลงแก้ไขโดยมิชอบ - ความเสี่ยงที่บริษัทไม่สามารถเข้าถึงข้อมูลของผู้ให้บริการภายนอกที่จำเป็นต่อการตรวจสอบภายใน การตรวจสอบของหน่วยงานกำกับดูแล หรือองค์กรอื่นๆ ตามกฎหมาย

หมายเหตุ

ตัวอย่างการกำหนดสถานการณ์ความเสี่ยงข้างต้น เป็นเพียงการให้ตัวอย่างและแนวคิดเพื่อให้บริษัททำความเข้าใจ และนำไปปรับใช้ โดยควรพิจารณาให้เหมาะสมกับความเสี่ยงเพื่อให้การประเมินผลกระทบสะท้อนกับความเสี่ยงที่อาจเกิดขึ้นของบริษัท

ทั้งนี้ ในการประเมินความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ ควรครอบคลุมความเสี่ยงอย่างน้อยในเรื่องดังต่อไปนี้

- ความเสี่ยงในการใช้บริการระบบคลาวด์
- ความเสี่ยงที่เกี่ยวข้องกับการรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคล (data privacy)
- การพึ่งพิงการใช้บริการจากผู้ให้บริการภายนอกจนอาจทำให้การเปลี่ยนแปลงหรือยกเลิกการใช้บริการทำได้ยาก (vendor lock-in)
- ผลกระทบต่อระบบงานที่สำคัญของบริษัท

ในกรณีที่บริษัทมีการใช้บริการจากผู้ให้บริการภายนอกในต่างประเทศ โดยเฉพาะการจัดเก็บข้อมูล ประมวลผล หรือการดำเนินการใดๆ เกี่ยวกับข้อมูล ให้บริษัทพิจารณาถึงความเสี่ยงและอุปสรรคที่อาจเกิดขึ้นจากประเทศที่ผู้ให้บริการภายนอกตั้งอยู่หรือประกอบธุรกิจ และควรมีการประเมินความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการในต่างประเทศนั้นๆ เช่น ความเสี่ยงจากการไม่สามารถเข้าถึงข้อมูล อันเนื่องมาจากการขัดข้องหรือการปิดกั้นเครือข่ายสื่อสาร หรือระบบสื่อสารระหว่างประเทศ (information access risk) ความเสี่ยงด้านกฎหมายที่เกี่ยวข้องกับการปฏิบัติตามหลักเกณฑ์ของต่างประเทศ (cross-border compliance) เป็นต้น

ตัวอย่าง : ภัยคุกคามที่เกี่ยวข้องกับการใช้บริการระบบคลาวด์ (cloud threats)

ภัยคุกคาม (threats)	ประเด็นปัจจัยความเสี่ยง (risk factors)	ตัวอย่างมาตรการ / แนวทางการจัดการความเสี่ยง
๑. ภัยคุกคามด้านเทคนิค (technical threats)		
(๑) ช่องโหว่ของการบริหารจัดการควบคุมการเข้าถึงระบบ vulnerable access management (infrastructure and application, public cloud)	S1.D legal transborder requirements S3.F identity and access management D1.B full sharing of the cloud (data pooling) D2.C sharing of the cloud	• สัญญา/ข้อตกลงที่มีผลตามกฎหมาย • คำร้องขอ/การแจ้งผู้ให้บริการระบบคลาวด์ ระบุข้อกำหนดทางเทคนิคในรายละเอียดสำหรับมาตรการควบคุมการเข้าถึงระบบ ildentity and access management) • การดำเนินการมาตรการควบคุมทางเทคนิคขององค์กร (แทนมาตรการควบคุมของผู้ให้บริการระบบคลาวด์)
(๒) ข้อมูลที่เห็นได้โดยผู้ใช้รายอื่นในกรณีการจัดสรรทรัพยากรร่วมในการใช้ระบบคลาวด์	S1.E multitenancy and isolation failure	• สัญญา/ข้อตกลงที่มีผลตามกฎหมาย • การเข้ารหัสสำหรับข้อมูลสารสนเทศที่มีความสำคัญ • คำร้องขอ/การแจ้งให้ผู้ให้บริการระบบคลาวด์ดำเนินการมาตรการควบคุมทางเทคนิคในการลบข้อมูลเมื่อมีการร้องขอ • การใช้ระบบคลาวด์แบบส่วนตัว (private cloud)
(๓) ข้อมูลที่เห็นได้จากการเช่าใช้ระบบคลาวด์ร่วมกัน (multitenancy visibility: routing	S1.E multitenancy and isolation failure D1.B, D2.C	• คำร้องขอ/การแจ้งผู้ให้บริการระบบคลาวด์ให้มีมาตรการควบคุมทางเทคนิคเพิ่มเติมในเรื่องการคุ้มครองข้อมูล (data privacy)

ภัยคุกคาม (threats)	ประเด็นปัจจัยความเสี่ยง (risk factors)	ตัวอย่างมาตรการ / แนวทางการจัดการความเสี่ยง
tables, MAC addresses, internal IP addresses, LAN traffic)		• สัญญา/ข้อตกลงที่มีผลตามกฎหมาย • การใช้ระบบคลาวด์แบบส่วนตัว (private cloud)
(๔) การโจมตีซอฟต์แวร์ (hypervisor attacks)	S1.E multitenancy and isolation failure	• คำร้องขอ/การแจ้งผู้ให้บริการระบบคลาวด์ ดำเนินการข้อตกลงการให้บริการ (service level agreement: SLA) สำหรับการจัดการช่องโหว่ของ hypervisor (VMware) • การใช้ระบบคลาวด์แบบส่วนตัว (Private Cloud)
(๕) การโจมตีระบบงาน (application attacks)	S3.H broad exposure of applications	• คำร้องขอ/การแจ้งผู้ให้บริการระบบคลาวด์ ดำเนินการ application firewall, anti-virus, anti-malware tools
(๖) ความเข้ากันได้ของระบบงาน (application compatibility)	D3.C application compatibility	• การประเมินการออกแบบและข้อกำหนดความต้องการของระบบงาน จากผู้ที่ต้องการใช้ระบบคลาวด์ • คำร้องขอ/การแจ้งผู้ให้บริการระบบคลาวด์ เรื่องการสื่อสารและแจ้งเตือนเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญของระบบ โดยมีการทดสอบความเข้ากันได้ของระบบ
(๗) ความเสียหายที่เกิดจากผู้ใช้รายอื่นหรือปัจจัยรอบข้าง (collateral damage)	D1.C collateral damage	• การขอให้ผู้ให้บริการระบบคลาวด์แจ้งเตือนในกระบวนการจัดการอุบัติการณ์ (incident) จากเหตุการณ์ปัจจัยภายนอกอื่นในกรณีมีการใช้ระบบคลาวด์ร่วมกับผู้ใช้รายอื่น (เช่น การที่การใช้งานระบบคลาวด์ของผู้ใช้รายอื่นถูกโจมตีแบบ DDoS และมีผลต่อการใช้งานของบริษัท) • การเพิ่มข้อกำหนดในสัญญาเรื่องการประกันสมรรถนะของระบบ (capacity) • การใช้ระบบคลาวด์แบบส่วนตัว (private cloud)
(๘) ความมั่นคงปลอดภัยในการเข้าใช้งานระบบคลาวด์ประเภท SaaS (Saas access security)	S3.K browser vulnerabilities	• การปิดช่องโหว่ web browsers และ/หรือ ระบบงานสำหรับผู้ใช้งาน (end-user client applications) โดยมีมาตรการความปลอดภัย เช่น anti-malware, encryption, sandbox) • การใช้ระบบ virtual desktop ที่ปลอดภัย หรือ browser client ที่กำหนดเฉพาะในการเชื่อมต่อระบบงานในคลาวด์
(๙) มาตรการความปลอดภัยที่ล้าสมัยสำหรับการใช้ระบบเสมือน (outdated VM security)	S1.K virtual machine (VM) security maintenance	• จัดทำเอกสารการปฏิบัติงานสำหรับการปรับปรุงความมั่นคงปลอดภัยซอฟต์แวร์ก่อนที่จะดำเนินการใช้งาน VM
๒. ภัยคุกคามด้านการปฏิบัติตามกฎระเบียบ (regulatory threats)		
(๑) ความเป็นเจ้าของทรัพย์สิน (asset ownership)	S2.D application disposal	• การระบุเงื่อนไขในสัญญากับผู้ให้บริการระบบคลาวด์ให้ครอบคลุมเรื่องสิทธิ์ความเป็นเจ้าของตามกฎหมาย

ภัยคุกคาม (threats)	ประเด็นปัจจัยความเสี่ยง (risk factors)	ตัวอย่างมาตรการ / แนวทางการจัดการความเสี่ยง
	S3.C data ownership	แต่ผู้เดียวของบริษัท สำหรับทรัพย์สินที่มีการติดตั้ง/ย้าย/นำไปใช้งานร่วมกับผู้ให้บริการระบบคลาวด์
		• การเข้ารหัสข้อมูลสำหรับข้อมูลสารสนเทศที่สำคัญ ที่มีการติดตั้ง/ย้ายไปยังระบบของผู้ให้บริการระบบคลาวด์
(๒) การลบข้อมูล/การกำจัดทรัพย์สิน (asset disposal)	S1.I data disposal S2.D application didsposal S3.D data disposal	• คำร้องขอ/การแจ้งให้ผู้ให้บริการระบบคลาวด์ดำเนินการมาตรการควบคุมทางเทคนิคในการลบข้อมูลหรือกำจัดสื่อจัดเก็บข้อมูล เมื่อมีการร้องขอ
		• การระบุเงื่อนไขในสัญญา ในการลบข้อมูล เมื่อสิ้นสุดสัญญา หรือเมื่อมีเหตุที่ทำให้สัญญาสิ้นสุด
(๓) สถานที่ตั้ง/จัดเก็บทรัพย์สิน (asset location)	S1.D legal transborder requirements	• คำร้องขอ/การแจ้งให้ผู้ให้บริการระบบคลาวด์ จัดทำรายการสถานที่ตั้งระบบโครงสร้างพื้นฐาน และรับรองว่าปฏิบัติตามข้อกำหนดกฎเกณฑ์ของบริษัท
		• การระบุเงื่อนไขในสัญญาเรื่องการห้ามเคลื่อนย้ายทรัพย์สินของบริษัทหากไม่มีการกำหนดหรือเห็นชอบจากบริษัท
๓. ภัยคุกคามด้านการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ (information security governance threats)		
(๑) ความมั่นคงปลอดภัยทางกายภาพ (physical security)	S1.H physical security	• คำร้องขอ/การแจ้งให้ผู้ให้บริการระบบคลาวด์ ปฏิบัติตามนโยบายความมั่นคงปลอดภัยทางกายภาพ
		• คำร้องขอ/การแจ้งให้ผู้ให้บริการระบบคลาวด์แสดงหลักฐานการสอบทานหรือการตรวจสอบด้านความมั่นคงปลอดภัยโดยผู้ตรวจสอบอิสระ
		• การระบุเงื่อนไขในสัญญาให้ผู้ให้บริการระบบคลาวด์รับทราบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยของบริษัท และยินยอมดำเนินมาตรการควบคุมที่จำเป็นตามที่บริษัทร้องขอ
		• คำร้องขอ/การแจ้งให้ผู้ให้บริการระบบคลาวด์มีแผนฉุกเฉินหรือแผนรองรับการดำเนินงานต่อเนื่อง หรือ มาตรการควบคุมที่สำคัญ/แผนกู้คืนสำหรับกรณีเหตุภัยพิบัติ
(๒) มาตรการความมั่นคงปลอดภัยของผู้ให้บริการ (visibility of the security measures)	S1.F lack of visibility surround technical security measures in place	• คำร้องขอ/การแจ้งให้ผู้ให้บริการระบบคลาวด์ ให้มีแผนหรือมาตรการความมั่นคงปลอดภัยทางเทคนิคที่ซึ่งสอดคล้องกับข้อกำหนดของบริษัท
		• คำร้องขอ/การแจ้งให้ผู้ให้บริการระบบคลาวด์แสดงหลักฐานการสอบทานหรือการตรวจสอบด้านความมั่นคงปลอดภัยโดยผู้ตรวจสอบอิสระ
		• การระบุเงื่อนไขในสัญญาให้ผู้ให้บริการระบบคลาวด์จัดทำรายงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยให้กับบริษัท (เช่น รายงานการจัดการ incident, ข้อมูลการตรวจจับการบุกรุก IDS/IPS log, ฯลฯ)
		• คำร้องขอ/การแจ้งให้ผู้ให้บริการระบบคลาวด์ ให้มีกระบวนการจัดการอุบัติการณ์ (incident) สำหรับ

ภัยคุกคาม (threats)	ประเด็นปัจจัยความเสี่ยง (risk factors)	ตัวอย่างมาตรการ / แนวทางการจัดการความเสี่ยง
		ทรัพย์สินของบริษัท และสอดคล้องตามนโยบายความมั่นคงปลอดภัยฯของบริษัท
(๓) การจัดการสื่อที่ใช้จัดเก็บหรือบันทึกข้อมูล (media management)	S1.I data disposal	• คำร้องขอ/การแจ้งให้ผู้ให้บริการระบบคลาวด์ ให้มีกระบวนการและมาตรการทางเทคนิคในการลบข้อมูลหรือกำจัดสื่อบันทึกข้อมูล และมีการประเมินด้วยว่าสอดคล้องกับข้อกำหนดของบริษัท
(๔) ขั้นตอนด้านความมั่นคงปลอดภัยสำหรับการพัฒนาระบบ/ซอฟต์แวร์ (secure software SDLC)	S3.E lack of visibility into software systems development life cycle (SDLC)	• คำร้องขอ/การแจ้งให้ผู้ให้บริการระบบคลาวด์ ให้มีขั้นตอนรายละเอียดสำหรับการพัฒนาระบบ โดยมีมาตรการความมั่นคงปลอดภัยตั้งแต่กระบวนการออกแบบ และสอดคล้องกับข้อกำหนดของบริษัท
		• คำร้องขอ/การแจ้งให้ผู้ให้บริการระบบคลาวด์ แสดงหลักฐานการสอบทานหรือการตรวจสอบด้านความมั่นคงปลอดภัยโดยผู้ตรวจสอบอิสระ
(๕) นโยบายความมั่นคงปลอดภัยสำหรับระบบคลาวด์แบบกลุ่ม common security policy for community cloud)	D2.C sharing of the cloud	• กำหนดให้มีนโยบายด้านความมั่นคงปลอดภัยที่ใช้ร่วมกัน โดยมีการระบุข้อกำหนดขั้นต่ำสำหรับการใช้งานระบบคลาวด์แบบกลุ่ม (community cloud) ร่วมกันของสมาชิกทุกราย
		• คำร้องขอ/การแจ้งให้ผู้ให้บริการระบบคลาวด์ แสดงหลักฐานการสอบทานหรือการตรวจสอบด้านความมั่นคงปลอดภัยโดยผู้ตรวจสอบอิสระ
(๖) ข้อกำหนดการสิ้นสุดการให้บริการ (service termination issues)	S3.G exit strategy	• การระบุข้อกำหนดในสัญญาหรือข้อตกลงการให้บริการที่ตกลงร่วมกับผู้ให้บริการระบบคลาวด์ ในการปฏิบัติเมื่อสิ้นสุดสัญญา หรือ เมื่อมีเหตุหรือช่วงเวลาที่ระบุถึงการถอดถอนทรัพย์สินของบริษัท
		• การดำเนินการตามแผนกู้คืน สำหรับกรณีการหยุดชะงักการให้บริการโดยสิ้นเชิงของผู้ให้บริการระบบคลาวด์
(๗) การกำกับดูแลของบริษัท (solid enterprise governance)	S3.I ease to contract aSaaS	• การดำเนินการมาตรการควบคุมภายในสำหรับการกำกับดูแลโดยบริษัท ในมาตรการที่จำเป็น (ด้านกฎหมาย การปฏิบัติตามกฎเกณฑ์ ด้านการเงิน ฯลฯ) ในระหว่างดำเนินการเพื่อใช้บริการระบบคลาวด์
(๘) การสนับสนุนสำหรับการตรวจสอบความมั่นคงปลอดภัยและการตรวจสอบทางนิติวิทยาศาสตร์ (support for audit and forensic investigations)	S3.F identity and access management S1.L data Disposal	• คำร้องขอ/การแจ้งให้ผู้ให้บริการระบบคลาวด์ เรื่องสิทธิของบริษัทในการตรวจสอบ โดยเป็นส่วนหนึ่งของสัญญาหรือข้อตกลงการให้บริการ การร้องขอรายงานผลการตรวจสอบโดยผู้ตรวจสอบอิสระ
		• คำร้องขอ/การแจ้งให้ผู้ให้บริการระบบคลาวด์ ให้การสนับสนุน ในการตรวจสอบข้อมูล (log, traces, hard disk images) ในกรณีการตรวจสอบทางนิติวิทยาศาสตร์ โดยเป็นส่วนหนึ่งของสัญญาหรือข้อตกลงการให้บริการ ทั้งนี้ การตรวจสอบทางนิติวิทยาศาสตร์ที่เชื่อถือได้โดยผู้ตรวจสอบอิสระ เมื่อมีการร้องขอ

หมายเหตุ

ตัวอย่างภัยคุกคามที่เกี่ยวข้องกับการใช้บริการระบบคลาวด์ข้างต้น เป็นเพียงการให้ตัวอย่างและแนวคิดเพื่อให้บริษัททำความเข้าใจ และนำไปปรับใช้ในแง่ของการพิจารณาระบุความเสี่ยงหรือภัยคุกคามที่อาจจะเกิดขึ้นจากการใช้บริการคลาวด์ ทั้งนี้บริบทความเสี่ยงลักษณะของการใช้บริการควรพิจารณาให้เหมาะสม

ส่วนที่ ๓ : หลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอก

การใช้บริการจากผู้ให้บริการภายนอก รวมถึงการใช้บริการระบบคลาวด์ บริษัทต้องมีการบริหารจัดการผู้ให้บริการภายนอก อย่างน้อยครอบคลุมในเรื่องดังต่อไปนี้

๑. บริษัทต้องกำหนดกระบวนการและหลักเกณฑ์ที่ชัดเจนในการคัดเลือกผู้ให้บริการภายนอก และมีการตรวจสอบความพร้อม และพิจารณาความเหมาะสมของผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกจะสามารถให้บริการได้อย่างต่อเนื่อง และสามารถตอบสนองความต้องการของบริษัทได้ ทั้งนี้ การตัดสินใจในการใช้บริการที่มีความเสี่ยงหรือมีนัยสำคัญต้องได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

ทั้งนี้ ปัจจัยสำคัญที่บริษัทควรพิจารณา เพื่อประเมินศักยภาพผู้ให้บริการภายนอกที่ครอบคลุมตามระดับความมีนัยสำคัญ และความเสี่ยงที่เกี่ยวข้องกับการใช้บริการ อย่างน้อยในเรื่องดังต่อไปนี้

(๑) ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์ และความสามารถในการให้บริการในช่วงที่ผ่านมา และระบบการบริหารงานภายใน

(๒) การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน

(๓) ศักยภาพและความสามารถในการให้บริการทั้งในภาวะปกติและไม่ปกติ โดยเฉพาะอย่างยิ่งกรณีที่ผู้ให้บริการภายนอกนั้นมีการให้บริการแก่ผู้ใช้บริการหลายราย (concentration risk)

(๔) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(๕) การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ต่างๆ

(๖) การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เช่น การขอตรวจสอบเอกสารหลักฐานหรือใบรับรองจากบุคคลภายนอกในการดำเนินการตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เป็นต้น

(๗) การปฏิบัติตามมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ เช่น การขอตรวจสอบ หรือสามารถแสดงเอกสารหลักฐานการได้รับการรองรับตามมาตรฐาน ISO 27001 เป็นต้น โดยการรับรองการปฏิบัติตามมาตรฐานสากลบริษัทควรพิจารณาว่าบุคคลภายนอกได้รับการรับรองการให้บริการในส่วนที่สาคัญ เช่น ศูนย์คอมพิวเตอร์ และ/หรือ ได้รับการรับรองครอบคลุมทั้งองค์กร ทั้งนี้ การพิจารณาคัดเลือกผู้ให้บริการระบบคลาวด์ บริษัทควรคำนึงถึงความพร้อม และมาตรฐานในการให้บริการของผู้ให้บริการดังกล่าว โดยผู้ให้บริการระบบคลาวด์ควรได้รับการรับรองมาตรฐานสากลที่เกี่ยวข้อง เช่น มาตรฐานสากลในเรื่องการรักษาความมั่นคงปลอดภัยของระบบงานและข้อมูล เป็นต้น

(๘) ปัจจัยภายนอกที่อาจกระทบต่อการให้บริการของบุคคลภายนอก เช่น สถานการณ์ทางการเมืองสภาวะเศรษฐกิจ ข้อจำกัดด้านกฎหมายของประเทศที่บุคคลภายนอกตั้งอยู่หรือประกอบธุรกิจ

(๙) การใช้เทคโนโลยีแบบเปิด (open technology) เพื่อให้สามารถนำระบบไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้ (interoperability) และลดข้อจำกัดในการย้าย หรือเปลี่ยนแปลงเทคโนโลยีผู้ให้บริการ รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง

๒. บริษัทต้องมีการจัดทำสัญญาการใช้บริการจากผู้ให้บริการภายนอก หรือมีการจัดทำข้อตกลงการให้บริการ (service level agreement: SLA) เป็นลายลักษณ์อักษร โดยรายละเอียดของสัญญาและข้อตกลงการให้บริการ ให้บริษัทพิจารณาให้ครอบคลุมตามระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ โดยมีรายละเอียดอย่างน้อยดังนี้

(๑) ขอบเขตงานเทคโนโลยีสารสนเทศที่ใช้บริการ และเงื่อนไขในการให้บริการของผู้ให้บริการภายนอก รวมทั้งบทบาทหน้าที่และความรับผิดชอบของผู้ให้บริการภายนอก

(๒) มาตรฐานขั้นต่ำในการปฏิบัติงานสำหรับผู้ให้บริการภายนอก เช่น มาตรฐานด้านการรักษาความมั่นคงปลอดภัยและความลับของข้อมูล การห้ามนำข้อมูลไปใช้ นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงการให้บริการ ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ เป็นต้น

(๓) ระบบการควบคุมภายในของผู้ให้บริการภายนอก

(๔) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศสำหรับการใช้บริการที่สอดคล้องกับแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศของบริษัท

(๕) การติดตามและรายงานผลการปฏิบัติงานของผู้ให้บริการภายนอก ซึ่งครอบคลุมถึงการรายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดขึ้นจากการให้บริการ

(๖) ความรับผิดชอบของบริษัทและผู้ให้บริการภายนอก ในกรณีที่เกิดปัญหาในการให้บริการ เงื่อนไขหรือแนวทางในการเปลี่ยนแปลงหรือยกเลิกสัญญา เช่น การทำลายข้อมูลของผู้ใช้บริการของบริษัท และข้อมูลของบริษัททั้งหมดเมื่อสิ้นสุด หรือยกเลิกการใช้บริการจากผู้ให้บริการภายนอก เป็นต้น

(๗) การระบุสิทธิในการเข้าตรวจสอบของบริษัท สำนักงาน คปภ. ผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากบริษัทหรือสำนักงาน คปภ. เพื่อให้สามารถเข้าตรวจสอบการดำเนินงาน การควบคุมภายใน และเรียกดูข้อมูลที่เกี่ยวข้องกับการใช้บริการของบริษัทได้

๓. บริษัทต้องมีแนวทางในการติดตามการใช้บริการจากผู้ให้บริการภายนอก โดยอย่างน้อยครอบคลุมในเรื่องดังต่อไปนี้

(๑) กำหนดให้มีผู้รับผิดชอบในการติดตามผลการปฏิบัติงานของผู้ให้บริการภายนอกอย่างต่อเนื่อง โดยพิจารณาตามระดับความเสี่ยงและระดับความมีนัยสำคัญของการใช้บริการ เช่น กำหนดให้ผู้ให้บริการภายนอกมีการรายงานผลการปฏิบัติงานอย่างสม่ำเสมอ เป็นต้น เพื่อให้บริษัทมีการติดตามประสิทธิภาพในการให้บริการของผู้ให้บริการภายนอกอย่างต่อเนื่อง

(๒) กำหนดให้มีการรายงานเหตุการณ์ผิดปกติจากการให้บริการของผู้ให้บริการภายนอกที่เกิดขึ้นระหว่างการดำเนินงานที่เกี่ยวข้องกับการใช้บริการต่อบริษัทอย่างทันการณ์ เพื่อประเมินผลกระทบที่อาจเกิดขึ้นอย่างมีนัยสำคัญต่อการดำเนินธุรกิจของบริษัท

(๓) กำหนดให้มีการทบทวน เพื่อประเมินประสิทธิภาพ และความเสี่ยงจากการใช้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ ทั้งในด้านประสิทธิภาพการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการปฏิบัติตามกฎหมาย และมีการรายงานผลการประเมินดังกล่าวให้คณะกรรมการบริษัท หรือคณะกรรมการชุดย่อย หรือผู้บริหารที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสม

๔. บริษัทต้องมีแนวทางในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ อันเนื่องมาจากการใช้บริการจากผู้ให้บริการภายนอก โดยอย่างน้อยครอบคลุมในเรื่องดังต่อไปนี้

(๑) กำหนดหน้าที่และความรับผิดชอบระหว่างบริษัท และผู้ให้บริการภายนอกอย่างชัดเจนในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ รวมถึงให้แจ้งบริษัททราบเหตุการณ์ผิดปกติที่เกิดขึ้นและเกี่ยวข้องกับอย่างเพียงพอและทันการณ์

(๒) กรณีเหตุการณ์ผิดปกติที่เกิดขึ้น ส่งผลกระทบต่อการดำเนินธุรกิจของบริษัทอย่างมีนัยสำคัญ บริษัทควรมีส่วนร่วมในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติ

(๓) กำหนดให้ผู้ให้บริการภายนอกมีช่องทาง ระบบ หรือเครื่องมือเพื่อรองรับกรณีที่บริษัทตรวจพบและต้องการรายงานเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศต่อผู้ให้บริหารภายนอกทราบ และสามารถติดตามสถานการณ์และการดำเนินการแก้ไขของผู้ให้บริการภายนอกต่อเหตุการณ์ผิดปกติที่เกิดขึ้นได้

(๔) กำหนดให้ผู้ให้บริการภายนอกมีผู้ประสานงานหลักกับบริษัท เพื่อสื่อสารและประสานงานเกี่ยวกับการดำเนินการตอบสนองต่อเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ

๕. บริษัทต้องจัดให้มีการบริหารความต่อเนื่องทางธุรกิจ (business continuity management: BCM) โดยอย่างน้อยครอบคลุมในเรื่องดังต่อไปนี้

(๑) มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity plan: BCP) ที่ครอบคลุมถึงการใช้บริการจากผู้ให้บริการภายนอก สอดคล้องกับขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ รวมถึงผลกระทบของการใช้บริการที่มีต่อ การดำเนินธุรกิจของบริษัท

(๒) มีแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (disaster recovery plan: DRP) เพื่อรองรับกรณีการเกิดปัญหาหรือเหตุการณ์ผิดปกติจากการใช้บริการจากผู้ให้บริการภายนอก และเพื่อลดผลกระทบที่อาจเกิดขึ้น โดยบริษัทต้องมั่นใจว่า มีข้อมูลพร้อมใช้ภายในประเทศสำหรับการดำเนินธุรกิจและการให้บริการแก่ลูกค้าอย่างต่อเนื่อง

ทั้งนี้ แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรคำนึงถึงปัจจัยสำคัญ หรือความเสี่ยงที่อาจเกิดขึ้นที่ส่งผลต่อการหยุดชะงักของการให้บริการและการดำเนินธุรกิจ

(๓) มีการทบทวนและทดสอบแผนรองรับการดำเนินธุรกิจและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้สามารถปฏิบัติงานได้จริง รวมทั้งสอบทานแผนของผู้ให้บริการภายนอก โดยควรพิจารณาความสอดคล้องกับแผนของบริษัท เช่น การกำหนด maximum tolerable period of disruption (MTPD), recovery time objective (RTO) และ recovery point objective (RPO) เป็นต้น

๖. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการใช้บริการจากผู้ให้บริการภายนอก

ในการใช้บริการจากผู้ให้บริการภายนอก ซึ่งรวมถึงการใช้บริการระบบคลาวด์ บริษัทต้องมั่นใจได้ว่าผู้ให้บริการภายนอกมีกระบวนการ ขั้นตอนในการประเมิน และการควบคุม ความเสี่ยงอย่างน้อยตามกรอบหลักการที่สำคัญ ๓ ประการ คือ

(๑) การรักษาความลับ (confidentiality)

(๒) ความถูกต้องเชื่อได้ (integrity) และ

(๓) ความพร้อมใช้งาน (availability)

สอดคล้องตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) และมาตรฐานสากลด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่เกี่ยวข้อง ตามขนาด ปริมาณธุรกรรม ความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ให้บริการ และความเสี่ยงที่เกี่ยวเนื่องกับการให้บริการ รวมทั้งจัดให้มีกระบวนการติดตาม ประเมินผล และตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานด้านการรักษาความมั่นคงปลอดภัยตามที่ตกลงไว้ ครอบคลุมด้านการรักษาความลับของระบบงานและข้อมูล ด้านการรักษาความถูกต้องและเชื่อถือได้ของระบงานและข้อมูล และด้านความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ให้บริการตามที่ตกลงไว้กับบริษัท

ทั้งนี้ บริษัทสามารถกำหนดให้ผู้ให้บริการภายนอกมีการประยุกต์ใช้แนวทางการควบคุมด้านงานเทคโนโลยีสารสนเทศที่ดีเป็นมาตรฐานสากล และได้รับการยอมรับโดยทั่วไปได้ตามความเหมาะสม เช่น มาตรฐาน International Organization for Standardization (ISO) หรือ Telecommunications Industry Association (TIA) เป็นต้น

๖.๑ การรักษาความมั่นคงปลอดภัยและการรักษาความลับ (confidentiality)

ในการใช้บริการจากผู้ให้บริการภายนอก บริษัทต้องมีการรักษาความมั่นคงปลอดภัยและความลับของระบบงานและข้อมูล โดยควรพิจารณาอย่างน้อยในเรื่องดังต่อไปนี้

(๑) ผู้ให้บริการภายนอกมีแนวทางหรือมาตรฐานในการรักษาความมั่นคงปลอดภัยและความลับของระบบงานและข้อมูล ทั้งข้อมูลของผู้ใช้บริการของบริษัท และข้อมูลของบริษัท

<u>สำหรับกรณีที่บริษัทมีการใช้บริการระบบคลาวด์</u> ให้บริษัทพิจารณาถึงแนวทางการรักษาความมั่นคงปลอดภัยผู้ให้บริการระบบคลาวด์ต่อข้อมูลสำคัญของผู้ใช้บริการของบริษัท และข้อมูลสำคัญของบริษัทตาม

วิธีการและมาตรฐานสากล เช่น การเข้ารหัสข้อมูล (data encryption) การควบคุมกุญแจที่ใช้เข้าถึงและเข้ารหัสข้อมูลบนระบบคลาวด์ (key management) เป็นต้น

(๒) บริษัทมีกระบวนการ หรือระบบในการนำข้อมูลของผู้ใช้บริการของบริษัท และข้อมูลของบริษัททั้งหมดกลับมาจากผู้ให้บริการภายนอก และมั่นใจได้ว่า ผู้ให้บริการภายนอกมีขั้นตอน หรือระบบในการทำลายข้อมูลของผู้ใช้บริการของบริษัท และข้อมูลของบริษัททั้งหมดเมื่อมีการสิ้นสุดหรือยกเลิกการใช้บริการจากผู้ให้บริการภายนอก

(๓) ผู้ให้บริการภายนอกมีแนวทางหรือมาตรฐานในการดูและป้องกันข้อมูลสำคัญของผู้ใช้บริการและข้อมูลของบริษัท เป็นไปตามกฎหมายข้อบังคับที่เกี่ยวข้อง และมาตรฐานสากลของงานเทคโนโลยีสารสนเทศนั้น

๖.๒ ความถูกต้องเชื่อถือได้ (integrity)

ในการใช้บริการจากผู้ให้บริการภายนอก บริษัทต้องดำเนินการเพื่อให้มั่นใจว่าระบบงานและข้อมูลมีความถูกต้องเชื่อถือได้ โดยควรพิจารณาให้ ผู้ให้บริการภายนอกมีแนวทางหรือมาตรฐานในการรักษาความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล ซึ่งครอบคลุมตั้งแต่ การพัฒนา หรือการเปลี่ยนแปลงแก้ไขระบบงาน การควบคุมทั้งในส่วนของการบันทึกข้อมูลเข้าสู่ระบบ (input validation) การประมวลผล (processing control) และการนำข้อมูลออกจากระบบ (output control) รวมทั้ง มีการดำเนินการให้งานเทคโนโลยีสารสนเทศที่ให้บริการสามารถทำได้อย่างมีประสิทธิภาพ และถูกต้องเชื่อถือได้

๖.๓ ความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (availability)

ในการใช้บริการจากผู้ให้บริการภายนอก บริษัทต้องดำเนินการเพื่อให้มั่นใจถึงความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ โดยควรพิจารณาให้ ผู้ให้บริการภายนอกมีแนวทางหรือมาตรฐานในการทำให้งานเทคโนโลยีสารสนเทศที่ให้บริการแก่บริษัท มีความพร้อมใช้งาน และสามารถให้บริการได้อย่างต่อเนื่องทั้งในภาวะปกติและไม่ปกติ

๗. การคุ้มครองผู้ใช้บริการของบริษัท (consumer protection)

ในการใช้บริการจากผู้ให้บริการภายนอก บริษัทต้องมีการดำเนินการเกี่ยวกับการคุ้มครองผู้ใช้บริการของบริษัท โดยควรพิจารณาอย่างน้อยในเรื่องดังต่อไปนี้

(๑) บริษัทต้องมั่นใจว่า ผู้ให้บริการภายนอกจะไม่นำข้อมูลของผู้ใช้บริการของบริษัท หรือข้อมูลของบริษัทไปเปิดเผยให้กับบุคคลอื่นใด โดยไม่ได้รับความยินยอมจากบริษัท

(๒) บริษัทต้องจัดให้มีกระบวนการในการติดตาม ประเมินผล และตรวจสอบผู้ให้บริการภายนอกเพื่อให้มั่นใจว่าผู้ให้บริการภายนอกสามารถดำเนินการตามแนวทางหรือมาตรฐานด้านการคุ้มครองผู้ใช้บริการของบริษัทที่ได้ตกลงไว้กับบริษัท

(๓) บริษัทต้องจัดให้มีระบบการดูแลและจัดการเรื่องร้องเรียนให้แก่ผู้ใช้บริการของบริษัทอย่างเพียงพอและเหมาะสม และรายงานการจัดการเรื่องร้องเรียนดังกล่าวให้คณะกรรมการชุดย่อย หรือผู้บริหารที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสม

ทั้งนี้ ในกรณีที่ผู้ใช้บริการของบริษัทได้รับความเสียหายจากการใช้บริการจากผู้ให้บริการภายนอก บริษัทควรจัดเตรียมแนวทางหรือแผนรองรับในการชดเชยความเสียหายให้แก่ผู้ใช้บริการของบริษัทอย่างเหมาะสม

<u>ส่วนที่ ๔ : การรายงานต่อสำนักงาน คปภ.</u>

๑. บริษัทมีการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ รวมทั้งการใช้บริการระบบคลาวด์ ที่มีความเกี่ยวข้องกับข้อมูลที่มีความสำคัญ เช่น ข้อมูลผู้เอาประกันภัย ข้อมูลลูกค้า ข้อมูลเกี่ยวกับแผนธุรกิจ ข้อมูลทางการเงิน ข้อมูลเกี่ยวกับการพัฒนาผลิตภัณฑ์หรือเทคโนโลยี เป็นต้น ให้บริษัทรายงานมายังสายพัฒนามาตรฐานการกำกับ สำนักงาน คปภ. ล่วงหน้า ๓๐ วันก่อนเริ่มใช้งานระบบ ผ่านช่องทางอีเมล์ ITRiskMgt@oic.or.th ตามแบบฟอร์มรายงานที่สำนักงานกำหนด โดยสามารถดาวน์โหลดเอกสารแบบฟอร์มการรายงาน การใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT outsourcing) รวมทั้งการใช้บริการระบบคลาวด์ (cloud computing) ได้ที่ www.oic.or.th ที่หัวข้อ IT Risk And Cybersecurity

สำหรับกรณีบริษัทที่มีการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ ก่อนที่ประกาศจะมีผลบังคับใช้ ให้บริษัทรายงานต่อสำนักงาน คปภ. ภายใน ๙๐ วันหลังจากที่ประกาศฯ มีผลบังคับใช้

๒. กรณีที่เกิดปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการใช้บริการจากผู้ให้บริการภายนอก และส่งผลกระทบต่อการให้บริการ หรือระบบ หรือข้อมูลผู้เอาประกันภัย หรือชื่อเสียงของบริษัท และให้รวมถึงการถูกโจมตี หรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ของระบบที่บริษัทใช้บริการจากผู้ให้บริการภายนอก ให้บริษัทดำเนินการตามข้อกำหนดในประกาศ คปภ. ว่าด้วยหลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต / ประกันวินาศภัย

แบบรายงานการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT outsourcing) รวมทั้งการใช้บริการระบบคลาวด์ (cloud computing)

ชื่อบริษัท .....

วันที่บันทึกข้อมูล	ชื่อผู้ให้บริการภายนอก	ประเทศที่จดทะเบียน	ประเภทของผู้ให้บริการภายนอก	ประเภทของการเชื่อมต่อ	รายละเอียดขอบเขตของการทำงาน	การเข้าถึงข้อมูลสำคัญของบริษัทและข้อมูลตาม PDPA, GDPR	วันที่เริ่มสัญญา	วันที่สิ้นสุดสัญญา	ระดับความเสี่ยงของการให้บริการ	SLA ของบริการ	ประเภทของบริการ Cloud	ประเทศที่ตั้งศูนย์คอมพิวเตอร์และข้อมูล
2020-06-30	X-UAble Company Limited	ไทย (TH)	Other IT Outsourcing - Middle and Back office support system	ไม่ได้มีการเชื่อมต่อถึงกัน	Outsource staff - IT Helpdesk and End-User support	มีการเข้าถึงข้อมูลดังกล่าว	2020-05-31	2021-06-1	น้อย	มี SLA	SaaS	TH; SG; JP

หมายเหตุ

ตัวอย่างแบบรายงานข้างต้น จัดทำเพื่อเป็นตัวอย่างในการกรอกข้อมูลตามแบบรายงานที่สำนักงาน คปภ. กำหนด

คำอธิบายเพิ่มเติม

หัวข้อ	คำอธิบาย
๑. ประเภทของผู้ให้บริการภายนอก	ประเภทของบริการด้านเทคโนโลยีสารสนเทศ (IT) และบริการระบบคลาวด์ (cloud computing) ที่ให้บริการโดยผู้ให้บริการภายนอก ดังนี้ ๑. Critical IT Outsourcing - Cloud Service การใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศประเภทบริการระบบคลาวด์ที่มีความสำคัญของบริษัท ๒. Critical IT Outsourcing – Infrastructure การใช้บริการจากผู้ให้บริการภายนอกด้านโครงสร้างพื้นฐานของระบบเทคโนโลยีสารสนเทศที่มีความสำคัญของบริษัท ๓. Critical IT Outsourcing - Service Channel การใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศที่มีความสำคัญของบริษัทในส่วนของช่องทางการให้บริการต่างๆ ให้กับลูกค้า ๔. Critical IT Outsourcing - Processing System การใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศที่มีความสำคัญของบริษัทในด้านของระบบงานประมวลผลของบริษัท ๕. Critical IT Outsourcing - Middle and Back Office Support System การใช้บริการระบบงานส่วนกลาง (middle office support system) และระบบงานให้บริการด้านสำนักงานส่วนหลัง (back office support system) ด้านเทคโนโลยีสารสนเทศที่สำคัญของบริษัทจากผู้ให้บริการภายนอก ๖. Other IT Outsourcing – Infrastructure การใช้บริการจากผู้ให้บริการภายนอกด้านโครงสร้างพื้นฐานงานเทคโนโลยีสารสนเทศประเภทอื่นๆ ๗. Other IT Outsourcing - Service Channel การใช้บริการเทคโนโลยีสารสนเทศประเภทอื่นๆ ด้านช่องทางการให้บริการต่างๆ ให้กับลูกค้า จากผู้ให้บริการภายนอก ๘. Other IT Outsourcing - Processing System การใช้บริการเทคโนโลยีสารสนเทศประเภทอื่นๆ ด้านระบบงานประมวลผล จากผู้ให้บริการภายนอก ๙. Other IT Outsourcing - Middle and Back Office Support System การใช้บริการระบบงานส่วนกลาง (middle office support system) และระบบงานให้บริการด้านสำนักงานส่วนหลัง (back office support system) ด้านเทคโนโลยีสารสนเทศประเภทอื่นๆ จากผู้ให้บริการภายนอก ๑๐. พันธมิตรธุรกิจ (business partner) คือผู้ให้บริการภายนอกมีการทำสัญญาหรือข้อตกลงร่วมกับบริษัทในการให้บริการ ทั้งที่เป็นพันธมิตรทางธุรกิจที่ดำเนินการแทนบริษัท หรือพันธมิตรทางธุรกิจในรูปแบบอื่นที่มีการทำธุรกิจร่วมกับบริษัทเพื่อเอื้อให้เกิดประโยชน์ทางธุรกิจ โดยมีการเชื่อมต่อระบบงานด้านเทคโนโลยีสารสนเทศกับบริษัท ไม่ว่าจะเป็นการเชื่อมต่อโดยตรง (direct link) หรือผ่าน API

หัวข้อ	คำอธิบาย
	๑๑. Payment Gateway คือ ผู้ให้บริการภายนอกที่ให้บริการชำระเงินทางอิเล็กทรอนิกส์ผ่านอุปกรณ์อย่างหนึ่งอย่างใดหรือผ่านทางเครือข่ายเทคโนโลยีสารสนเทศให้แก่บริษัท ๑๒. ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider: ISP) คือ ผู้ให้บริการเครือข่ายอินเทอร์เน็ต (internet service provider) ที่ให้บริการเชื่อมต่อระบบเครือข่ายภายนอก เช่น เครือข่าย Internet ๑๓. ผู้ให้บริการเครือข่าย (Media Provider) คือ ผู้ให้บริการเครือข่าย (media provider) ที่ให้บริการเชื่อมต่อระบบเครือข่ายระหว่างภายในกลุ่มบริษัทที่ไม่ได้ตั้งอยู่บริเวณเดียวกัน และ/หรือ ระหว่างบริษัทภายนอก เช่น การเช่าสายสื่อสารประเภทสายใยแก้วนำแสง (fiber optic)
๒. ประเภทของการเชื่อมต่อ	เป็นการเชื่อมต่อระบบงานระหว่างองค์กร โดยแบ่งประเภทของการเชื่อมต่อเป็นดังนี้ ๑. การเชื่อมต่อตรง (Direct Connect) เป็นการเชื่อมต่อระบบงานกันโดยตรงระหว่างบริษัทหรือองค์กร (direct link) กับผู้ให้บริการภายนอก ๒. API (application programming interface) เป็นบริการช่องทางการเชื่อมต่อเพื่อแลกเปลี่ยนข้อมูลจากระบบหนึ่งไปสู่ระบบอื่นๆ ในลักษณะการใช้ชุดคำสั่งโปรแกรม (code) ที่อนุญาตให้ software program สามารถสื่อสารระหว่างกันได้ กับผู้ให้บริการภายนอก ๓. อื่นๆ (Others) ใช้ช่องทางอื่นๆ ทำการเชื่อมต่อสื่อสารระบบงานกับผู้ให้บริการภายนอก ๔. ไม่ได้มีการเชื่อมต่อถึงกัน คือ ไม่มีการเชื่อมต่อระบบงานของบริษัทกับผู้ให้บริการภายนอก
๓. รายละเอียดขอบเขตของการทำงาน	ขอบเขต ลักษณะงานและกระบวนการทำงาน สำหรับงานที่ต้องการใช้บริการจากบุคคลภายนอกที่มีความชัดเจนซึ่งเป็นงานที่ไม่ซ้ำซ้อนกับขอบเขตที่มีผู้ดำเนินการอยู่แล้ว และสอดคล้องกับหลักเกณฑ์การกำกับดูแลฉบับนี้
๔. การเข้าถึงข้อมูลสำคัญของบริษัท และข้อมูลตาม PDPA, GDPR	ในการให้บริการด้านเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอกมีการเข้าถึงข้อมูลในระดับชั้นสำคัญของบริษัทในระดับชั้นที่ไม่เปิดเผย รวมถึงข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA และ/หรือ GDPR)
๕. ระดับความเสี่ยงของการให้บริการ	ระดับของโอกาสหรือระดับเหตุการณ์ที่ไม่พึงประสงค์ที่จะเกิดจากผู้ให้บริการภายนอก โดยอาจจะเกิดขึ้นในอนาคต และมีผลกระทบต่อการให้บริการ แบ่งได้ดังนี้ ๑. ความเสี่ยงน้อย โอกาสที่จะมีเหตุการณ์ที่ไม่พึงประสงค์และส่งผลต่อบริการของบริษัทน้อย ๒. ความเสี่ยงปานกลาง มีโอกาสที่จะมีเหตุการณ์ที่ไม่พึงประสงค์บ้างและส่งผลต่อบริการของบริษัทเป็นบางส่วน

หัวข้อ	คำอธิบาย
	๓. ความเสี่ยงสูง มีโอกาสที่จะมีเหตุการณ์ที่ไม่พึงประสงค์สูงและส่งผลต่อบริการของบริษัททำให้เกิดความเสียหายต่อธุรกิจมาก ๔. ในกรณีที่ไม่สามารถระบุ service risk level ได้ ให้ระบุ service risk level เป็น “ไม่มีกรณีดังกล่าว”
๖. SLA ของบริการ	ผลการประเมินมาตรฐานการให้บริการด้านเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอก (service level agreement : SLA) โดยแบ่งได้ดังนี้ ๑. ผ่าน หมายถึง ผู้ให้บริการภายนอกสามารถให้บริการได้ตามมาตรฐานที่บริษัทกำหนด ๒. ไม่ผ่าน หมายถึง ผู้ให้บริการภายนอกไม่สามารถให้บริการได้ตามมาตรฐานที่บริษัทกำหนด ๓. บริษัทไม่มีการควบคุมมาตรฐานการให้บริการผู้ให้บริการภายนอกด้วย SLA
๗. ประเภทของบริการ Cloud	ประเภทบริการคลาวด์ที่บริษัทมีการใช้บริการจากผู้ให้บริการคลาวด์ภายนอก ดังนี้ ๑. มีการใช้บริการคลาวด์ ประเภท IaaS (Infrastructure as a Service) เป็นการให้บริการเฉพาะโครงสร้างพื้นฐานของระบบ เช่น หน่วยประมวลผล (processing unit) เครือข่ายข้อมูล (network) ระบบเก็บข้อมูล (storage) หรือพื้นที่เซิร์ฟเวอร์ (hosting) โดยมีการใช้บริการจากผู้ให้บริการภายนอกเพียงบริการเดียว ๒. มีการใช้บริการคลาวด์ ประเภท PaaS (Platform as a Service) เป็นบริการแพลทฟอร์มที่ให้บริการสำหรับนักพัฒนาในการพัฒนาโปรแกรม โดยผู้รับบริการสามารถพัฒนาโปรแกรมระบบ อาทิเช่น บริการ Google app engine ซึ่งผู้รับบริการสามารถสร้างโปรแกรมประยุกต์ประเภท web application บนเว็บที่มีอัตราการเข้าชมสูง โดยไม่ต้องจัดการโครงสร้างพื้นฐานสำหรับอัตราการเข้าชมที่สูง โดยมีการใช้บริการจากผู้ให้บริการภายนอกเพียงบริการเดียว ๓. มีการใช้บริการคลาวด์ ประเภท SaaS (Software as a Service) เป็นรูปแบบการให้บริการใช้ซอฟต์แวร์หรือแอฟพลิเคชันบนระบบคลาวด์ อำนวยความสะดวกให้ผู้ใช้สามารถเรียกใช้บริการซอฟต์แวร์เหล่านี้ได้ผ่านเครือข่ายอินเตอร์เน็ตโดยไม่จำเป็นต้องติดตั้งซอฟต์แวร์ไว้ที่บริษัท หรือคอมพิวเตอร์ของผู้ใช้งาน โดยมีการใช้บริการจากผู้ให้บริการภายนอกเพียงบริการเดียว ๔. มีการใช้บริการคลาวด์ ประเภท IaaS และ PaaS จากผู้ให้บริการภายนอก ๕. มีการใช้บริการคลาวด์ ประเภท IaaS และ SaaS จากผู้ให้บริการภายนอก ๖. มีการใช้บริการคลาวด์ ประเภท PaaS และ SaaS จากผู้ให้บริการภายนอก ๗. มีการใช้บริการคลาวด์ ทั้ง IaaS PaaS และ SaaS จากผู้ให้บริการภายนอก ๘. ไม่มีการใช้บริการคลาวด์จากผู้ให้บริการภายนอก

หัวข้อ	คำอธิบาย
๘. ประเทศที่ตั้งศูนย์คอมพิวเตอร์	ประเทศ (สถานที่ตั้งทางภูมิศาสตร์) ของศูนย์คอมพิวเตอร์เพื่อใช้ให้บริการในการประมวลผล และ/หรือศูนย์เก็บข้อมูลที่ผู้ให้บริการภายนอกนำมาให้บริการต่อบริษัท

สำนักงานคณะกรรมการกำกับและส่งเสริม
การประกอบธุรกิจประกันภัย(คปภ.)
Office of Insurance Commission