คปภ.

สำนักงานคณะกรรมการกำกับและส่งเสริม
การประกอบธุรกิจประกันภัย(คปภ.)

- ร่าง -

แนวปฏิบัติเรื่อง การกำกับดูแลข้อมูล

(Data Governance Guideline)

หลักการและเหตุผล

ปัจจุบันนอกจากเทคโนโลยีและนวัตกรรมต่างๆ ที่มาขับเคลื่อนการดำเนินธุรกิจแล้ว อีกสิ่งหนึ่งที่สำคัญ คือ ข้อมูล โดยบริษัทได้นำข้อมูลมาใช้ประโยชน์ทั้งในการพัฒนาทั้งผลิตภัณฑ์และบริการต่างๆ เพื่อเข้าถึงและตอบโจทย์ลูกค้าให้ได้มากที่สุด อย่างไรก็ตาม ข้อมูลเป็นทรัพย์สินสารสนเทศที่สำคัญประเภทหนึ่งที่สำนักงาน คปภ. มุ่งหวังให้บริษัทมีการกำกับดูแลการเข้าถึง การใช้งาน และการจัดเก็บ รวมทั้งการบริหารจัดการความเสี่ยง การรักษาความมั่นคงปลอดภัย และการรักษาความเป็นส่วนบุคคลของข้อมูล ตามประกาศ คปภ. เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต / ประกันวินาศภัย พ.ศ. ๒๕๖๓ ซึ่งกำหนดให้ทุกบริษัทต้องมีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยครอบคลุมในเรื่องบริหารจัดการทรัพย์สินสารสนเทศของบริษัท เช่น การจัดทำทะเบียนทรัพย์สินสารสนเทศ การจัดชั้นความลับของข้อมูล การกำหนดแนวทางการรักษาความมั่นคงปลอดภัยสอดคล้องตามชั้นความลับ การรักษาความมั่นคงปลอดภัยของข้อมูล การจัดเก็บข้อมูลในระบบงานหรือสื่อบันทึกข้อมูลต่างๆ และการทำลายข้อมูลที่เหมาะสมกับชั้นความลับ การควบคุมการเข้าถึงระบบ ข้อมูล และทรัพย์สินสารสนเทศ การเข้ารหัสข้อมูล (Cryptography) ที่เหมาะสมตามชั้นความลับและความสำคัญของข้อมูล เป็นต้น

ดังนั้น สำนักงาน คปภ. เล็งเห็นว่า นอกจากการรักษาความมั่นคงปลอดภัยของข้อมูล ธุรกิจประกันภัยควรมีการกำกับดูแลข้อมูลในด้านต่างๆ ที่เกี่ยวข้องอย่างเหมาะสม และมีประสิทธิภาพ เพื่อสามารถใช้ประโยชน์จากข้อมูลที่อยู่บนพื้นฐานของ ข้อมูลที่มีคุณภาพ ถูกต้อง ครบถ้วน มั่นคงปลอดภัย และมีความเป็นส่วนบุคคล สำนักงานจึงได้จัดทำแนวปฏิบัติ เรื่อง การกำกับดูแลข้อมูล (Data Governance Guideline) ที่สามารถให้แนวทางและเป็นแหล่งอ้างอิงในการนำไปปรับใช้ที่สอดคล้องตามหลักการที่ดีสอดคล้องกับมาตรฐานสากล โดยมุ่งหวังให้บริษัทนำไปดำเนินการกำกับดูแลข้อมูล จัดโครงสร้างองค์กรที่รองรับการกำกับดูแลข้อมูล กำหนดบทบาทหน้าที่ความรับผิดชอบของคณะกรรมการบริษัท และบุคลากรที่เกี่ยวข้องในการปฏิบัติหน้าที่บริหารจัดการข้อมูลอย่างชัดเจน กำหนดนโยบายการกำกับดูแลข้อมูลเป็นลายลักษณ์อักษร รวมทั้งมีกระบวนการบริหารจัดการข้อมูลที่ครอบคลุมวรจรชีวิตข้อมูล การบริหารจัดการคุณภาพของข้อมูล การบริหารจัดการความเสี่ยงด้านข้อมูล การรักษาความมั่นคงปลอดภัยของข้อมูล และการรักษาความเป็นส่วนบุคคลของข้อมูลตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เป็นต้น

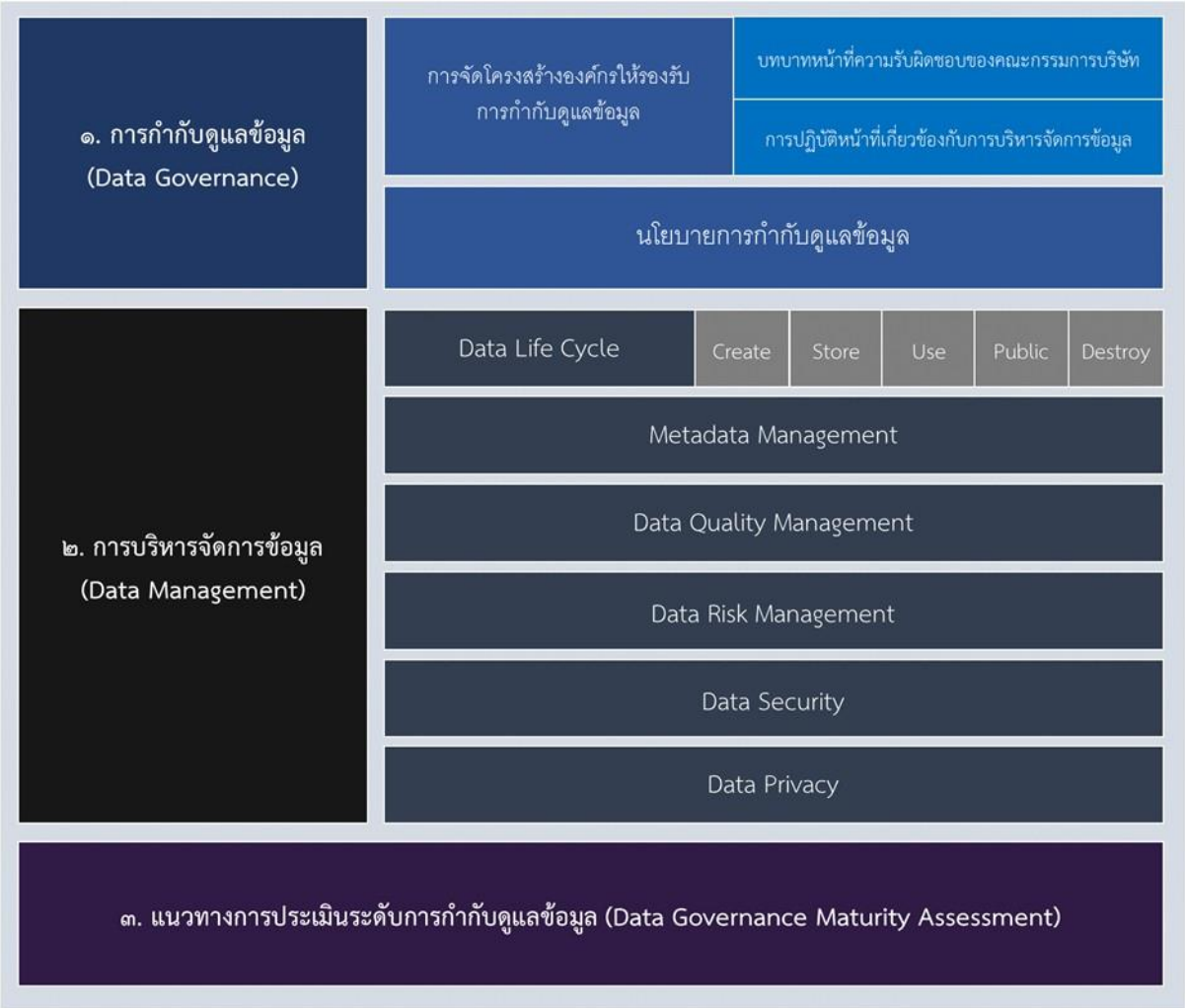
ขอบเขต

แนวปฏิบัติ เรื่อง การกำกับดูแลข้อมูล (Data Governance) ฉบับนี้ จัดทำขึ้นเพื่อเป็นประโยชน์ต่อบริษัทประกันภัย ในการนำไปประยุกต์ใช้เป็นแนวทางอ้างอิงในการกำกับดูแลและบริหารจัดการข้อมูลในองค์กรอย่างมีคุณภาพ มีความมั่นคงปลอดภัย มีความเป็นส่วนบุคคล และสามารถใช้ประโยชน์จากข้อมูลในการดำเนินธุรกิจได้อย่างเต็มประสิทธิภาพ โดยมีสาระสำคัญครอบคลุม ๓ เรื่อง ได้แก่ การกำกับดูแลข้อมูล (Data Governance) การบริหารจัดการข้อมูล (Data Management) และการประเมินประสิทธิผลของการบริหารจัดการข้อมูล (Data Governance Maturity Assessment) ทั้งนี้ สำนักงาน คปภ. คาดหวังให้บริษัทประกันภัย สามารถนำไปใช้ประโยชน์เพื่อเป็นแนวทางดำเนินการกำกับดูแล และบริหารจัดการข้อมูลขององค์กรได้อย่างหมาะสมตามขนาด ลักษณะการดำเนินธุรกิจ ความซับซ้อน และความเสี่ยงของบริษัท

นิยามคำศัพท์	
การกำกับดูแลข้อมูล (Data Governance)	หมายถึง กระบวนการในการกำหนดทิศทาง ควบคุม และสอบทานการบริหารจัดการข้อมูล เพื่อให้องค์กรดำเนินการบริหารจัดการข้อมูลตามนโยบาย กฎ ระเบียบ หรือข้อบังคับที่กำหนดไว้ การกำกับดูแลข้อมูลที่ดีก่อให้เกิดการบริหารจัดการข้อมูลที่มีประสิทธิภาพ ส่งผลให้ข้อมูลมีความมั่นคงปลอดภัย มีคุณภาพ และมีความคุ้มทุนต่อการดำเนินงาน
การบริหารจัดการข้อมูล (Data Management)	หมายถึง แนวทางในการกำหนดนโยบาย มาตรฐาน กระบวนการที่เกี่ยวข้องกับข้อมูลทั้งหมด รวมทั้ง บุคลากรที่เกี่ยวข้อง เครื่องมือในการจัดการข้อมูลและป้องกันข้อมูล เพื่อให้องค์กรมั่นใจได้ว่าข้อมูลที่นำมาใช้มีความถูกต้อง สมบูรณ์ มั่นคงปลอดภัย เชื่อถือได้ และนำไปใช้งานได้ง่ายและมีประสิทธิภาพ
คำอธิบายชุดข้อมูล (Metadata)	หมายถึง ข้อมูลที่ใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่นๆ ที่เกี่ยวข้องทั้งกระบวนการเชิงธุรกิจและเชิงเทคโนโลยีสารสนเทศ ให้รายละเอียดถึงกฎ ข้อจำกัดของข้อมูล และโครงสร้างของข้อมูล ช่วยให้องค์กรสามารถเข้าใจข้อมูล ระบบ และขั้นตอนการทำงานได้ดียิ่งขึ้น
การบริหารจัดการคำอธิบายชุดข้อมูล (Metadata Management)	หมายถึง กระบวนการที่เกี่ยวข้องกับการบริหารจัดการหรือควบคุมคำอธิบายชุดข้อมูล เพื่อให้สามารถมั่นใจว่าคำอธิบายชุดข้อมูลสามารถมีการเข้าถึง แบ่งปัน เชื่อมโยง วิเคราะห์ และบูรณาการ ให้เกิดประสิทธิผลทั่วทั้งองค์กร
การบริหารจัดการคุณภาพข้อมูล (Data Quality Management)	หมายถึง กระบวนการที่เกี่ยวข้องกับการวางแผน การดำเนินการ และการควบคุมกิจกรรมต่างๆ รวมถึงการปรับปรุง เพื่อให้ข้อมูลมีคุณภาพ มีความน่าเชื่อถือ สามารถนำไปใช้ประกอบการวิเคราะห์และตัดสินใจทางธุรกิจได้อย่างถูกต้องเหมาะสม
คำอธิบายข้อมูลเชิงธุรกิจ (Business Metadata)	หมายถึง คำอธิบายชุดข้อมูลที่ให้รายละเอียดของชุดข้อมูลในด้านธุรกิจ เหมาะสำหรับผู้ใช้งานข้อมูลในการประกอบการดำเนินงานธุรกิจในองค์กร เช่น ชื่อข้อมูล ชื่อเจ้าของข้อมูล คำอธิบายอย่างย่อ วันที่เริ่มต้นใช้งาน วันที่ทำการเปลี่ยนแปลงข้อมูล ภาษาที่ใช้ ชื่อฟิลด์ข้อมูล (ชื่อพนักงาน นามสกุล เพศ) เป็นต้น
คำอธิบายข้อมูลเชิงเทคนิค (Technical Metadata)	หมายถึง คำอธิบายชุดข้อมูลที่ให้รายละเอียดของชุดข้อมูลในด้านเทคนิค เหมาะสำหรับผู้บริหารจัดการข้อมูลในการประกอบการดำเนินงานด้านบริหารจัดการข้อมูล เช่น ชื่อตารางข้อมูลในฐาน ข้อมูล ชื่อฟิลด์ข้อมูลในตารางข้อมูล ประเภทข้อมูล (เช่น ตัวเลข ตัวหนังสือ หรือวันที่) ความกว้างของฟิลด์ข้อมูล (เช่น ๑๐ ตัวอักษร ๕๐ ตัวอักษร หรือ ๑๐๐ ตัวอักษร) คีย์ข้อมูล รวมไปถึงข้อมูลสำหรับการสำรองข้อมูล (Backup) และกู้คืนข้อมูล (Restore) เป็นต้น
คีย์ข้อมูล (Key)	หมายถึง ฟิลด์ข้อมูลที่ใช้ในการอ้างอิง การค้นหา การแก้ไขเปลี่ยนแปลงข้อมูล หรือเพื่อสร้างความสัมพันธ์กับตารางข้อมูลอื่นๆ และข้อมูลในฐานข้อมูลมีความสอดคล้องกัน
ข้อมูลสำคัญที่จำเป็นต้องมีคุณภาพ (Critical Data Elements)	หมายถึง ข้อมูลที่มีความสำคัญต่อองค์กร และจำเป็นต้องมีการจัดการคุณภาพของข้อมูล เช่น ข้อมูลในกลุ่ม Regulatory Reporting, Financial Reporting, Business Policy และ Business Strategy เป็นต้น

ภาพรวมของประกาศและแนวปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงาน คปภ.

สรุปภาพรวมของแนวปฏิบัติเรื่อง การกำกับดูแลข้อมูล (Data Governance Guideline)



หลักการและแนวปฏิบัติ

หลักการกำกับดูแลข้อมูล ประกอบด้วย ๓ ส่วน ได้แก่

๑. การกำกับดูแลข้อมูล (Data Governance)

๒. การบริหารจัดการข้อมูล (Data Management)

๓. แนวทางการประเมินระดับการกำกับดูแลข้อมูล (Data Governance Maturity Assessment)

ส่วนที่ ๑ : การกำกับดูแลข้อมูล

๑.๑ การจัดโครงสร้างองค์กรในการกำกับดูแลข้อมูล

บริษัทควรกำหนดโครงสร้างองค์กร และบทบาทหน้าที่ความรับผิดชอบในกระบวนการกำกับดูแลข้อมูลอย่างชัดเจนเป็นลายลักษณ์อักษร โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

๑.๑.๑ หน้าที่ความรับผิดชอบของคณะกรรมการบริษัท

คณะกรรมการบริษัท มีหน้าที่ในการกำกับดูแลให้บริษัทดำเนินการด้านที่เกี่ยวข้องกับการกำกับดูแลข้อมูล ที่เหมาะสมกับขนาด ลักษณะการดำเนินธุรกิจ ความซับซ้อน และความเสี่ยงด้านข้อมูลของบริษัท รวมทั้งสอดคล้องกับกลยุทธ์ทางธุรกิจ โดยควรกำหนดหน้าที่ความรับผิดชอบในการกำกับดูแลข้อมูลอย่างชัดเจน สอดคล้องตามหลักการ 3 line of defense และให้ดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

(๑) กำกับดูแลให้บริษัทมีการกำหนดนโยบายการกำกับดูแลข้อมูล โดยได้รับการพิจารณาอนุมัติจากคณะกรรมการบริษัท หรือ คณะกรรมการชุดย่อยที่ได้รับมอบหมาย และทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(๒) กำกับดูแลให้มีการนำนโยบายการกำกับดูแลข้อมูล ที่ผ่านการอนุมัติจากคณะกรรมการบริษัท หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย มาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารจัดการข้อมูล รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม และมีการทบทวนและประเมินประสิทธิภาพของนโยบายอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(๓) กำกับดูแลให้มีผู้รับผิดชอบในการปฏิบัติหน้าที่ ครอบคลุมในเรื่องดังต่อไปนี้

- **การกำกับดูแลข้อมูล และการบริหารจัดการข้อมูล**
- **การบริหารความเสี่ยงด้านข้อมูล**
- **การกำกับการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับข้อมูล**
- **การตรวจสอบการปฏิบัติงานที่เกี่ยวข้องกับข้อมูล**

(๔) จัดให้มีโครงสร้าง และกำหนดหน้าที่ความรับผิดชอบเกี่ยวกับการบริหารจัดการข้อมูล โดยเป็นไปตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ ๓ ระดับ (Three Lines of Defense) เพื่อให้มีการกำหนดหน้าที่ความรับผิดชอบอย่างชัดเจน และมีการถ่วงดุลอำนาจในแต่ละระดับอย่างเหมาะสม

(๕) กำกับดูแลให้มีการสร้างความรู้และความตระหนักด้านการกำกับดูแลข้อมูลในองค์กรแก่ คณะกรรมการบริษัท ผู้บริหาร และบุคลากรทุกระดับขององค์กร เพื่อสื่อสารให้เกิดความเข้ารู้ ความเข้าใจถึงความสำคัญของการใช้ข้อมูลอย่างปลอดภัย

(๖) จัดสรรทรัพยากรและงบประมาณ เพื่อรองรับการดำเนินการด้านการกำกับดูแลและบริหารจัดการข้อมูลแก่หน่วยงานที่เกี่ยวข้อง ทั้งในด้านบุคลากรและเครื่องมือให้เพียงพอที่จะสนับสนุนการปฏิบัติงานที่เกี่ยวข้องกับการกำกับดูแลข้อมูล

ทั้งนี้ คณะกรรมการบริษัทสามารถมอบหมายให้คณะกรรมการชุดย่อยที่มีอยู่แล้วในปัจจุบัน หรือพิจารณาจัดตั้งคณะกรรมการกำกับดูแลข้อมูล (Data Governance Committee) ขึ้นมาเป็นการเฉพาะ เพื่อทำหน้าที่รับผิดชอบงานด้านการกำกับดูแลการบริหารจัดการข้อมูล โดยคณะกรรมการชุดย่อยหรือคณะกรรมการกำกับดูแลข้อมูล ควรประกอบด้วยผู้บริหารจากหน่วยงานที่มีความเข้าใจในข้อมูลที่สำคัญของบริษัท รวมทั้ง ผู้บริหารที่เกี่ยวข้องดังต่อไปนี้

(๑) ผู้บริหารด้านเทคโนโลยีสารสนเทศ (Chief Information Officer)

(๒) ผู้บริหารด้านบริหารจัดการข้อมูล (Chief Data Officer)

(๓) ผู้บริหารด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (Chief Information Security Officer)

(๔) ผู้บริหารระดับสูงด้านความเสี่ยง (Chief Risk Officer)

(๕) ผู้บริหารจากส่วนงานต่างๆ ที่เกี่ยวข้องซึ่งมีความรู้ความเข้าใจในข้อมูลที่เป็นข้อมูลสำคัญของบริษัท เช่น ผู้บริหารฝ่ายงานด้านการรับประกันภัย ผู้บริหารฝ่ายงานด้านการจัดการสินไหมทดแทน ผู้บริหารฝ่ายงานทรัพยากรบุคคล ผู้บริหารฝ่ายงานด้านการเงิน ผู้บริหารฝ่ายงานบริหารลูกค้า เป็นต้น

๑.๑.๒ การปฏิบัติหน้าที่เกี่ยวข้องกับการบริหารจัดการข้อมูล

๑.๑.๒.๑ การกำกับดูแลข้อมูล และการบริหารจัดการข้อมูล

บริษัทควรจัดให้มีคณะกรรมการชุดย่อย (Data Governance Committee) เพื่อปฏิบัติหน้าที่ในการกำกับดูแลข้อมูลและบริหารจัดการข้อมูล โดยควรดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

(๑) กำหนดนโยบาย และระเบียบวิธีปฏิบัติที่เกี่ยวกับการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูล รวมทั้งทบทวนหรือปรับปรุงให้เป็นปัจจุบันอยู่เสมอ โดยควรทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

(๒) จัดให้มีการสื่อสารให้ความรู้เกี่ยวกับนโยบาย และระเบียบวิธีปฏิบัติที่เกี่ยวกับการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูล ครอบคลุมทุกกระบวนการของการบริหารจัดการข้อมูล เพื่อให้บุคลากรทุกระดับเกิดความตระหนักในการใช้ข้อมูลและสามารถนำไปปฏิบัติได้อย่างถูกต้องเหมาะสม

(๓) ติดตามสถานะในเรื่องที่เกี่ยวข้องกับการกำกับดูแลข้อมูล และการบริหารจัดการข้อมูล รายงานผลประเด็นปัญหา หรือความเสี่ยงที่พบต่อคณะกรรมการบริษัท หรือคณะกรรมการชุดย่อย หรือคณะกรรมการกำกับดูแลข้อมูล ตามระยะเวลาที่เหมาะสมเพียงพอ

(๔) กำกับดูแลให้มั่นใจว่ามีการนำนโยบาย และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลไปปฏิบัติในทุกระดับขององค์กร รวมถึงกำหนดบทบาทหน้าที่ความรับผิดชอบในการอนุมัติหรือควบคุมดูแลการดำเนินการต่างๆ ที่เกี่ยวข้องกับข้อมูล เช่น การอนุมัติการเข้าถึง การใช้ และการเผยแพร่ข้อมูล เป็นต้น

(๕) กำกับดูแลให้มีหน่วยงานหรือผู้รับผิดชอบบริหารจัดการคำอธิบายชุดข้อมูล (Metadata) เพื่อทำหน้าที่ในการจัดทำ ปรับปรุงแก้ไข และสอบทานคำอธิบายชุดข้อมูลให้เป็นปัจจุบัน

ทั้งนี้ เพื่อให้การดำเนินการด้านการกำกับดูแลข้อมูล และการบริหารจัดการข้อมูลมีประสิทธิภาพ บริษัทสามารถพิจารณากำหนดให้มีคณะทำงานหรือบุคลากรเพื่อดำเนินการในเรื่องดังต่อไปนี้

❖ **คณะทำงานที่ปฏิบัติหน้าที่ด้านการบริกรข้อมูล (Data Steward) เพื่อดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้**

(๑) สนับสนุนให้เกิดการกำกับดูแลข้อมูล และบริหารจัดการข้อมูลภายในองค์กร โดยรับคำสั่งโดยตรงจากคณะกรรมการชุดย่อยที่ปฏิบัติหน้าที่ในการกำกับดูแลข้อมูลและบริหารจัดการข้อมูล เพื่อสร้างความมั่นใจว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย และระเบียบวิธีปฏิบัติขององค์กร

(๒) กำหนดให้มีหัวหน้าบริกรข้อมูล (Lead Data Steward) โดยควรเป็นหนึ่งในคณะกรรมการชุดย่อย ที่ปฏิบัติหน้าที่ในการกำกับดูแลข้อมูลและบริหารจัดการข้อมูล

(๓) กำหนดให้มีบุคลากรที่บริกรข้อมูลด้านธุรกิจ (Business Data Steward) ปฏิบัติหน้าที่รับผิดชอบในการนิยามคุณลักษณะข้อมูลที่มีคุณภาพ รวมถึงนิยามของคำอธิบายชุดข้อมูล (Metadata) ที่สำคัญภายในองค์กร ทั้งนี้ บริกรข้อมูลด้านธุรกิจควรประกอบด้วยบุคลากรจากหลายหน่วยงานที่มีชุดข้อมูลที่สำคัญของบริษัท เพื่อสามารถนิยามข้อมูลที่มีคุณภาพ และคำอธิบายชุดข้อมูลได้อย่างชัดเจนที่สุด

(๔) กำหนดให้มีบุคลากรที่บริกรข้อมูลด้านเทคนิค (Technical Data Steward) ปฏิบัติหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศ รวมถึงข้อเสนอแนะเชิงเทคนิคแก่บริกรข้อมูลด้านธุรกิจ เช่น การนิยามคำอธิบายชุดข้อมูลเชิงเทคนิค (Technical Metadata) ทั้งนี้ บริกรข้อมูลด้านเทคนิคควรมาจากฝ่ายเทคโนโลยีสารสนเทศขององค์กร

❖ **บริษัทควรกำหนดบุคลากรหรือหน่วยงานที่เป็นเจ้าของข้อมูล (Data Owners) เพื่อดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้**

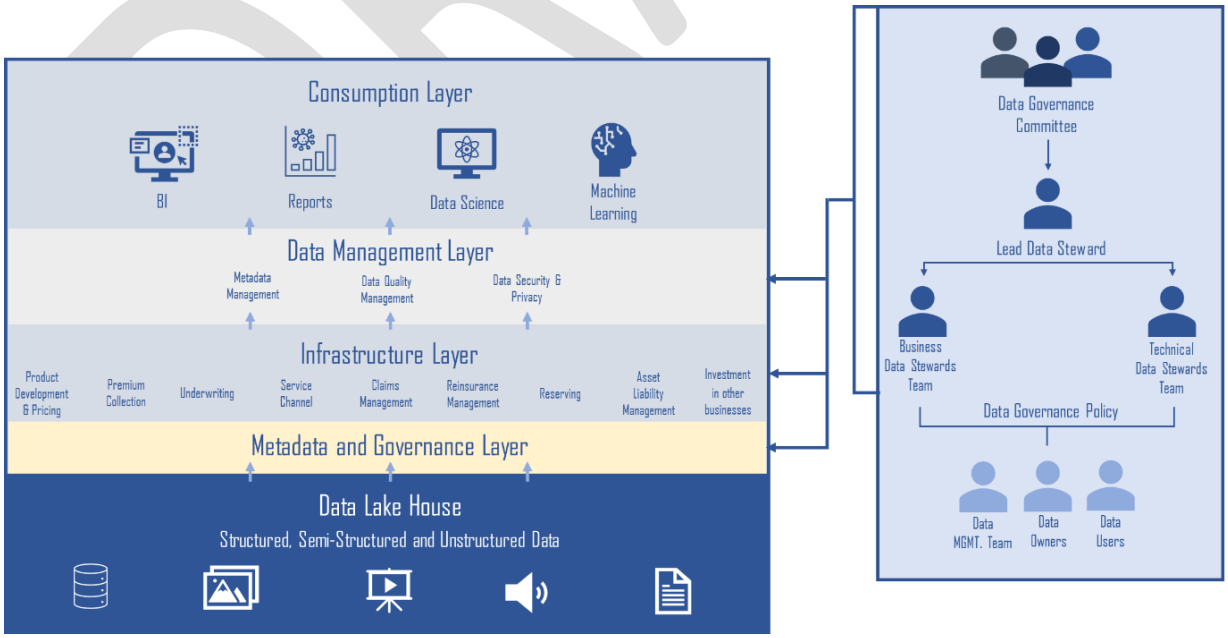
(๑) กำหนดให้มีบุคลากรหรือหน่วยงานที่เป็นเจ้าของข้อมูลซึ่งปฏิบัติหน้าที่รับผิดชอบดูแลชุดข้อมูลโดยตรงในแต่ละชุดข้อมูลที่สำคัญ โดยทั่วไปควรเป็นผู้บริหารจากหน่วยงานที่รับผิดชอบชุดข้อมูลที่สำคัญภายในองค์กร

(๒) ปฏิบัติหน้าที่ทบทวนและอนุมัติการดำเนินการต่างๆ ที่เกี่ยวข้องกับข้อมูลที่รับผิดชอบดูแลอยู่ รวมถึงให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

❖ **บริษัทควรจัดให้มีคณะทำงานที่ปฏิบัติหน้าที่บริหารจัดการข้อมูล (Data Management Team) เพื่อดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้**

(๑) ปฏิบัติหน้าที่สนับสนุนการดำเนินการบริหารจัดการข้อมูลในด้านเทคโนโลยีสารสนเทศ เช่น การจัดทำสถาปัตยกรรมข้อมูล การจัดการฐานข้อมูล การวิเคราะห์ข้อมูล การตรวจสอบคุณภาพข้อมูล รวมถึงการดำเนินการอื่นที่สนับสนุนให้กิจกรรมที่ใช้ข้อมูลภายในองค์กรมีประสิทธิภาพมากยิ่งขึ้น

<u>ตัวอย่าง แผนผังระบบงานเพื่อประกอบการพิจารณาจัดทำ data management diagram</u>



๑.๑.๒.๒ การบริหารความเสี่ยงด้านข้อมูล

หน่วยงานที่ปฏิบัติหน้าที่ในการบริหารความเสี่ยง ควรดำเนินการอย่างน้อย ในเรื่องดังต่อไปนี้

(๑) จัดทำกรอบและนโยบายการบริหารจัดการความเสี่ยงแบบองค์รวมของบริษัทให้ครอบคลุมการบริหารจัดการความเสี่ยงด้านข้อมูล รวมทั้งกำหนดให้**หน่วยงานที่เกี่ยวข้อง**ทำการประเมินความเสี่ยงด้านข้อมูลตามกรอบและกระบวนการบริหารความเสี่ยงของบริษัท

(๒) ให้คำแนะนำ ติดตาม และทบทวนความเสี่ยงด้านข้อมูลให้อยู่ในระดับที่ยอมรับได้ (Risk Appetite) ให้สอดคล้องกับนโยบายการบริหารจัดการความเสี่ยงแบบองค์รวมของบริษัท รวมถึงนำเสนอผลการบริหารความเสี่ยงด้านข้อมูลต่อคณะกรรมการที่เกี่ยวข้อง

ทั้งนี้ หน่วยงานที่ปฏิบัติหน้าที่ในการบริหารความเสี่ยง บริษัทสามารถจัดให้มีบุคลากรหรือหน่วยงานที่ทำหน้าที่บริหารจัดการความเสี่ยงด้านข้อมูลโดยเฉพาะสำหรับดำเนินการตามที่กล่าวข้างต้น

๑.๑.๒.๓ การกำกับการปฏิบัติตามกฎหมายและหลักเกณฑ์เกี่ยวข้องกับข้อมูล

หน่วยงานที่ปฏิบัติหน้าที่กำกับการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับข้อมูล โดยควรมีหน้าที่ในการติดตามดูแล ให้คำแนะนำ สอบทาน และรายงานการปฏิบัติงานที่เกี่ยวข้องกับข้อมูล เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และ ประกาศสำนักงาน คปภ. เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต / ประกันวินาศภัย พ.ศ. ๒๕๖๔ เป็นต้น

๑.๑.๒.๔ การตรวจสอบการปฏิบัติงานที่เกี่ยวข้องกับข้อมูล

หน่วยงานที่ปฏิบัติหน้าที่ในการตรวจสอบการปฏิบัติงานที่เกี่ยวข้องกับข้อมูล โดยควรมีหน้าที่ในการตรวจสอบการปฏิบัติงานและการบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับข้อมูล เพื่อติดตามและสอบทานให้มั่นใจว่ามีการดำเนินการเป็นไปตามที่นโยบายและระเบียบวิธีปฏิบัติที่กำหนด

๑.๒ นโยบายการกำกับดูแลข้อมูล

บริษัทควรกำหนดและจัดทำนโยบายการกำกับดูแลข้อมูลเป็นลายลักษณ์อักษร ที่เหมาะสมสอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ ความเสี่ยงที่เกี่ยวข้องและการใช้บริการจากผู้ให้บริการภายนอก โดยครอบคลุมอย่างน้อย ดังนี้

(๑) นโยบายการกำกับดูแลข้อมูล ควรครอบคลุมการกำกับดูแลข้อมูลทุกประเภทของบริษัท รวมถึงการใช้บริการจากบุคคลภายนอก โดยสามารถพิจารณาจัดทำนโยบายขึ้นเป็นการเฉพาะ หรือเพิ่มเติมให้ครอบคลุมจากนโยบายที่มีอยู่แล้วของบริษัทได้

(๒) โครงสร้างการกำกับดูแลข้อมูล บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการบริษัท คณะกรรมการชุดย่อยที่ได้รับมอบหมาย ผู้บริหารระดับสูง หน่วยงาน และบุคลากรที่เกี่ยวข้อง

(๓) การบริหารจัดการข้อมูล (Data Management) โดยอย่างน้อยควรครอบคลุมในเรื่องดังต่อไปนี้

- การบริหารจัดการวงจรชีวิตของข้อมูล (Data Life Cycle)
- การบริหารจัดการคำอธิบายชุดข้อมูล (Metadata Management)
- การบริหารจัดการคุณภาพของข้อมูล (Data Quality Management)
- การบริหารจัดการความเสี่ยงด้านข้อมูล (Data Risk Management)
- การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)
- การรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy)

(๔) จัดให้มีการสื่อสารนโยบายและระเบียบวิธีปฏิบัติเกี่ยวกับการบริหารจัดการข้อมูลให้กับผู้ที่เกี่ยวข้องทราบอย่างทั่วถึง รวมทั้งบุคลากรทุกระดับในองค์กรเพื่อรับทราบและถือปฏิบัติ

ส่วนที่ ๒ : การบริหารจัดการข้อมูล (Data Management)

๒.๑ วงจรชีวิตของข้อมูล (Data Life Cycle)

บริษัทควรมีการบริหารจัดการข้อมูลตลอดทั้งวงจรชีวิตของข้อมูล โดยครอบคลุมในเรื่อง การบริหารจัดการคำอธิบายชุดข้อมูล (Metadata Management) การบริหารจัดการคุณภาพข้อมูล (Data Quality Management) การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) และการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy)

ทั้งนี้ **วงจรชีวิตของข้อมูล** หมายถึง ลำดับขั้นตอนของข้อมูลตั้งแต่การเริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ประกอบด้วย ๕ ขั้นตอน ดังนี้

๑) การสร้างข้อมูล (Create) คือ การสร้างข้อมูลขึ้นมาใหม่ โดยวิธีการบันทึกด้วยบุคคลหรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ ทั้งนี้ กระบวนการสร้างข้อมูลให้รวมถึงการซื้อ หรือการรับข้อมูลจากภายนอกด้วย

๒) การจัดเก็บข้อมูล (Store) คือ การจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้างหรือจัดเก็บข้อมูลให้มีระเบียบง่ายต่อการใช้งาน ไม่สูญหายหรือถูกทำลาย และให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่างๆ ตามความต้องการได้อย่างรวดเร็ว โดยสามารถดำเนินการได้ทั้งในรูปแบบการลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS)

๓) การใช้ข้อมูล (Use) คือ การกระทำใดๆ ที่นำข้อมูลที่ได้จากกระบวนการจัดเก็บมาประมวลผล หรือดำเนินการให้เกิดประโยชน์ตามวัตถุประสงค์การนำข้อมูลมา เช่น การโอนข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน การเปลี่ยนรูปแบบการจัดเก็บข้อมูล เป็นต้น ทั้งนี้ กระบวนการใช้ข้อมูล ให้รวมถึงการสำรอง (Back up) หรือสำเนาข้อมูลด้วย

๔) การเผยแพร่ข้อมูล (Publish) คือ การแบ่งปัน การกระจาย และการแลกเปลี่ยนข้อมูลทั้งภายในและภายนอกองค์กร ทั้งนี้ ให้รวมถึงการดำเนินการกำหนดเงื่อนไขของการนำข้อมูลไปใช้ และการควบคุมการเข้าถึงข้อมูล (Access Control) ก่อนดำเนินการเผยแพร่ข้อมูล

๕) การทำลายข้อมูล (Destroy) คือ การดำเนินการทำลายข้อมูลที่เกินกว่าระยะเวลาจัดเก็บที่กำหนด

ทั้งนี้ เพื่อให้เห็นภาพความเชื่อมโยงของข้อมูลทั่วทั้งองค์กรที่ครอบคลุมตามวงจรชีวิตของข้อมูล รวมทั้งการจัดเก็บข้อมูลสำคัญ และการเข้าถึงหรือใช้งานข้อมูลต่างๆ ภายในองค์กร โดยบริษัทสามารถพิจารณาจัดทำแผนผังการไหลของข้อมูล (Data Flow Diagram) ภายในบริษัท เพื่อประโยชน์ในการบริหารจัดการข้อมูลให้เหมาะสมกับความเสี่ยงและลำดับชั้นความสำคัญของข้อมูล

๒.๒ การบริหารจัดการคำอธิบายชุดข้อมูล (Metadata Management)

บริษัทควรจัดทำคำอธิบายชุดข้อมูล โดยควรดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

(๑) กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการคำอธิบายชุดข้อมูล โดยให้ครอบคลุมถึงบทบาทหน้าที่ของบุคลากรหรือหน่วยงานที่รับผิดชอบ กระบวนการจัดทำคำอธิบายชุดข้อมูล การควบคุมดูแลและสอบทานคำอธิบายชุดข้อมูล

(๒) จัดทำคำอธิบายชุดข้อมูลที่สำคัญของบริษัท โดยการจัดทำคำอธิบายชุดข้อมูล ควรประกอบด้วยคำอธิบายชุดข้อมูล ๒ ประเภทอย่างน้อยดังต่อไปนี้

- คำอธิบายข้อมูลเชิงธุรกิจ (Business Metadata) ครอบคลุมอย่างน้อย ชื่อชุดข้อมูล คำอธิบายอย่างย่อ ผู้ทำหน้าที่อนุมัติ และควบคุมดูแลข้อมูล วันที่เริ่มต้นใช้งาน วันที่ทำการเปลี่ยนแปลงข้อมูลล่าสุด แหล่งที่มาของข้อมูล
- คำอธิบายข้อมูลเชิงเทคนิค (Technical Metadata) ครอบคลุมอย่างน้อย ชื่อตารางข้อมูลในฐานข้อมูล ชื่อฟิลด์ข้อมูลในตารางข้อมูล ประเภทข้อมูล ความกว้างของฟิลด์ข้อมูล คีย์ข้อมูล รวมถึงการสำรองข้อมูล และกู้คืนข้อมูล

ทั้งนี้ การจัดทำคำอธิบายชุดข้อมูลที่สำคัญของบริษัท ควรพิจารณาให้ครอบคลุมชุดข้อมูลที่สำคัญที่จำเป็นต้องมีคุณภาพ (Critical Data Element) ในการดำเนินธุรกิจ **โดยอย่างน้อยควรพิจารณาข้อมูลที่เกี่ยวข้องกับการดำเนินงานด้านการรับประกันภัย (Underwriting) และงานด้านการบริหารจัดการค่าสินไหมทดแทน (Claims Management)** เนื่องจากข้อมูลดังกล่าวมีความสำคัญในการให้บริการผู้เอาประกันภัย การพิจารณารับประกันภัย รวมถึงการปฏิบัติตามภาระผูกพันที่มีต่อผู้เอาประกันภัย

(๓) กำหนดให้มีกระบวนการควบคุมการเข้าถึง การกำหนดสิทธิ์ และการปรับปรุงแก้ไขคำอธิบายชุดข้อมูล

(๔) กำหนดให้มีการปรับปรุงรายการคำอธิบายชุดข้อมูลให้เป็นปัจจุบัน และควรทำการทบทวนและตรวจสอบคำอธิบายชุดข้อมูลอย่างน้อยปีละ ๑ ครั้ง

โดยบริษัทสามารถพิจารณาให้คณะทำงานที่ปฏิบัติหน้าที่ด้านการบริกรข้อมูล (Data Steward) เป็นผู้รับผิดชอบหลักในการดำเนินการบริหารจัดการคำอธิบายชุดข้อมูล ร่วมกับหน่วยงานอื่นๆ ที่เกี่ยวข้อง

<u>ตัวอย่าง แบบฟอร์มคำอธิบายข้อมูลเชิงธุรกิจ (Business Metadata)</u>

		ตัวอย่าง 1	**ตัวอย่าง 2**	**ตัวอย่าง 3**
เลขที่เมทาดาตา(Metadata_ID)	เลขที่ (ห้ามซ้ำ)	M001	M002	M003
1. ประเภทข้อมูล (data_type)	ชุดข้อมูลนี้เป็นข้อมูลประเภทใด	ข้อมูลทะเบียน	อื่นๆ	ข้อมูลทะเบียน
2. ชื่อชุดข้อมูล (title)	ชื่อของชุดข้อมูลที่กำหนดโดยหน่วยงานที่รับผิดชอบหรือเป็นเจ้าของข้อมูล	ข้อมูลประวัติบุคลากร	ข้อมูลการรักษาพยาบาลของบุคลากร	ข้อมูลกรมธรรม์
3. หน่วยงานที่รับผิดชอบหรือเป็นเจ้าของข้อมูล(data_owner)	ชื่อหน่วยงานที่รับผิดชอบหรือเป็นเจ้าของข้อมูล	ฝ่ายทรัพยากรบุคคล	ฝ่ายทรัพยากรบุคคล	ฝ่ายรับประกันภัย
4. ชื่อผู้ติดต่อ (contact_person)	ชื่อนามสกุลบุคลากร หรือกลุ่มที่ได้รับการมอบหมายให้เป็นผู้ประสานงานหลักของชุดข้อมูล	นาย สงบ สันติ	นางสาว ดี เด่น	นาย อิง ฟ้า
5. อีเมลผู้ติดต่อ (contact_email)	อีเมลบุคลากร หรือกลุ่มที่ได้รับการมอบหมายให้เป็นผู้ประสานงานหลักของชุดข้อมูล	sagobs@ins.co.th	deed@ins.co.th	underwrite@ins.co.th
6. คำสำคัญ (tag_string)	หัวข้อหรือแท็ก (tag) ที่ใช้ระบุคำสำคัญในชุดข้อมูล	บุคลากร พนักงาน ลูกจ้าง ประวัติ	สวัสดิการรักษาพยาบาล บุคลากร	กรมธรรม์ความคุ้มครอง การรับประกันภัย เบี้ยกรมธรรม์
7.รายละเอียด (notes)	คำอธิบายรายละเอียดที่สำคัญของชุดข้อมูลอย่างสั้น	เป็นข้อมูลประวัติส่วนตัวที่พนักงานให้ไว้เมื่อบรรจุเป็นพนักงาน	เป็นข้อมูลในการรักษาพยาบาลและการเบิกจ่ายค่ารักษาพยาบาลของบุคลากร	เป็นข้อมูลกรมธรรม์ของผู้เอาประกันภัยที่ได้จากการรับประกันภัย
8.วัตถุประสงค์ (objective)	อธิบายที่มาและวัตถุประสงค์ของการจัดทำชุดข้อมูล	ภายในองค์กร	ภายในขอบเขตความร่วมมือ	ภายในองค์กร

		ตัวอย่าง 1	ตัวอย่าง 2	ตัวอย่าง 3
9.1. หน่วยความถี่ของการปรับปรุงข้อมูล (update_frequency_unit)	ความถี่ที่ข้อมูลในระบบคลังข้อมูลถูกปรับปรุง/เพิ่มหรือเปลี่ยนแปลงข้อมูลสถิติ : ความถี่ในการเผยแพร่ข้อมูลสู่ผู้ใช้ข้อมูล	Real Time	ทุกวัน	Real Time
9.2. ค่าความถี่ของการปรับปรุงข้อมูลในรอบช่วงเวลา (update_frequency_interval)	ความถี่ในการปรับปรุงข้อมูล	-	1 ปี	-
10. แหล่งที่มา (data_source)	แหล่งที่มาของข้อมูลที่นำมาจัดทำชุดข้อมูล พร้อมหน่วยงานที่จัดทำ	ระบบ Enterprise Resource Planning	ระบบ Enterprise Resource Planning	ระบบ Underwriting
11. รูปแบบการเก็บข้อมูล (data_format)	รูปแบบของการจัดเก็บข้อมูล	Database	Database	Database
12. หมวดหมู่ข้อมูล (data_category)	หมวดหมู่ข้อมูลแบ่งตามการเปิดเผยข้อมูล	ข้อมูลความลับของบริษัท	ข้อมูลส่วนบุคคล	ข้อมูลความลับของบริษัท/ข้อมูลส่วนบุคคล
13. ระดับชั้นความลับ (data_classification)	ระดับชั้นความลับของข้อมูลตามนโยบายขององค์กร	ลับที่สุด	ลับ	ลับที่สุด
14. ข้อมูลส่วนบุคคล (personal_data)	ความเป็นข้อมูลส่วนบุคคล	เป็น	เป็น	เป็น

ตัวอย่าง การจัดทำคำอธิบายชุดข้อมูลเชิงเทคนิค (Technical Metadata)

ชื่อตารางข้อมูลในฐานข้อมูล	ชื่อฟิลด์ข้อมูลในตารางข้อมูล	ประเภทข้อมูล (Data Types)	ความกว้างของฟิลด์ข้อมูล	คีย์ข้อมูล	ตัวอย่าง
พนักงาน	รหัสพนักงาน	int	0-99999	Primary key	5505
พนักงาน	ชื่อ	nvarchar	50	-	สงบ
พนักงาน	นามสกุล	nvarchar	100	-	สันติ
กรมธรรม์	รหัสกรมธรรม์	nvarchar	100	Primary key	P00001
ผลิตภัณฑ์	ชื่อผลิตภัณฑ์	nvarchar	100	-	ประกันชีวิตแบบสะสมทรัพย์
ผลิตภัณฑ์	รหัสหมวดหมู่ผลิตภัณฑ์	int	0-9999	Foreign key (หมวดหมู่ผลิตภัณฑ์)	012

ตัวอย่าง การจัดทำคำอธิบายชุดข้อมูล (Metadata)

Metadata

client_no.	first_name	last_name	policy_no.	nin	policy_start_date	policy_end_date	...	data_source
0023	Simon	Mars	10230	HD 45 65 77 A	11082558	10082567	...	Underwriting/ClientSetup
0024	Anderson	Park	10965	EE 66 78 91 D	12092561	Null	...	Underwriting/ClientSetup
0025	Aran	Dusit	11500	770 6659 6666 000	25122562	24122581	...	Underwriting/ClientSetup

Data

Column	Description	Data Types
client_no.	Primary key of a table	int
first_name	Client first name	nvarchar(50)
last_name	Client last name	nvarchar(50)
policy_no.	Client's policy number	nvarchar(50)
nin	National Identification number	nvarchar(50)
policy_start_date	Start date of policy.	date
policy_end_date	Policy end date. Null if policy still active.	date
...	...	...

Business Metadata

Technical Metadata

หมายเหตุ ตัวอย่างข้างต้นเป็นการให้ตัวอย่างและแนวคิด เพื่อให้บริษัททำความเข้าใจและสามารถนำไปปรับใช้ให้เหมาะสมกับประเภทข้อมูล และระบบเทคโนโลยีสารสนเทศที่ดำเนินการอยู่ในปัจจุบัน ทั้งนี้ ควรพิจารณาให้เหมาะสมกับลักษณะของข้อมูล ขนาด ลักษณะ และความซับซ้อนในการดำเนินธุรกิจ

๒.๓ การบริหารจัดการคุณภาพข้อมูล (Data Quality Management)

บริษัทควรมีกระบวนการบริหารจัดการคุณภาพของข้อมูล และกำหนดให้มีผู้ทำหน้าที่รับผิดชอบในการบริหารจัดการคุณภาพข้อมูล บริษัทอาจพิจารณาให้เจ้าของข้อมูล (Data Owners) เป็นผู้รับผิดชอบหลักในการดำเนินการดังกล่าว โดยมีคณะทำงานที่ปฏิบัติหน้าที่ด้านการบริกรข้อมูล (Data Steward) เป็นผู้ให้คำปรึกษาและแนะนำ เพื่อให้สามารถดำเนินการดังกล่าวได้อย่างมีประสิทธิภาพ รวมทั้งกำหนดคุณลักษณะข้อมูลที่มีคุณภาพที่ชัดเจน ครอบคลุมทั้งในด้านความถูกต้อง (Accuracy) ครบถ้วน (Completeness) สอดคล้องกัน (Consistency) เป็นปัจจุบัน (Timeliness) ตรงกับความต้องการของผู้ใช้ (Relevancy) และพร้อมใช้งาน (Availability) โดยควรพิจารณาดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

๒.๓.๑ การกำหนดหลักเกณฑ์คุณภาพของข้อมูล โดยควรครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(๑) กำหนดข้อมูลสำคัญที่จำเป็นต้องมีคุณภาพ (Critical Data Element) ในแต่ละชุดข้อมูล รวมทั้งกำหนดระดับคุณภาพข้อมูล ในแต่ละชุดข้อมูล เพื่อใช้ในการประเมิน โดยอาจพิจารณาจากคุณลักษณะข้อมูลตามที่บริษัทกำหนดไว้

(๒) กำหนดให้มีกระบวนการควบคุมการเปลี่ยนแปลงหลักเกณฑ์คุณภาพข้อมูล รวมถึงกำหนดบุคลากรหรือหน่วยงานที่รับผิดชอบในเรื่องดังกล่าว

๒.๓.๒ การประเมินคุณภาพของข้อมูล (Data Quality Assessment) โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(๑) **กำหนดแนวทางในการประเมินคุณภาพข้อมูล** เพื่อติดตามคุณภาพข้อมูลอย่างต่อเนื่อง เช่น ข้อมูลที่บันทึกหรือจัดเก็บมีความคลาดเคลื่อนจากรูปแบบที่กำหนด ข้อมูลเป็นค่าว่าง ข้อมูลไม่สอดคล้องกัน ข้อมูลไม่เป็นปัจจุบัน และข้อมูลไม่พร้อมใช้งาน เป็นต้น ทั้งนี้ ในการวิเคราะห์คุณภาพข้อมูล ควรพิจารณาจากคำอธิบายชุดข้อมูล (Metadata) และ ข้อมูลสำคัญที่จำเป็นต้องมีคุณภาพ (Critical Data Element) โดยสามารถเปรียบเทียบกับระดับคุณภาพข้อมูลที่กำหนดไว้ รวมถึงควรกำหนดบุคลากรหรือหน่วยงานที่รับผิดชอบในเรื่องดังกล่าว

องค์ประกอบในการประเมินคุณภาพข้อมูล
ที่มา :ตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ

(๒) **จัดทำผลการประเมินคุณภาพข้อมูล** เพื่อใช้ติดตามคุณภาพข้อมูลอย่างต่อเนื่อง และรวบรวมชุดข้อมูลที่ไม่เป็นไปตามเกณฑ์คุณภาพที่กำหนด โดยควรรายงานไปยังบุคคลากรหรือหน่วยงานที่เกี่ยวข้อง เพื่อดำเนินการแก้ไขให้ถูกต้องตามเกณฑ์คุณภาพที่กำหนด

๒.๓.๓ การปรับปรุงคุณภาพข้อมูล (Data Quality Improvement) โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(๑) มีกระบวนการปรับปรุงข้อมูล สำหรับชุดข้อมูลที่ไม่ผ่านเกณฑ์การประเมินคุณภาพตามที่กำหนด

(๒) วิเคราะห์สาเหตุ (Root Cause Analysis) เพื่อป้องกันไม่ให้เกิดชุดข้อมูลที่ไม่มีคุณภาพในลักษณะเดียวกันอีกในอนาคต

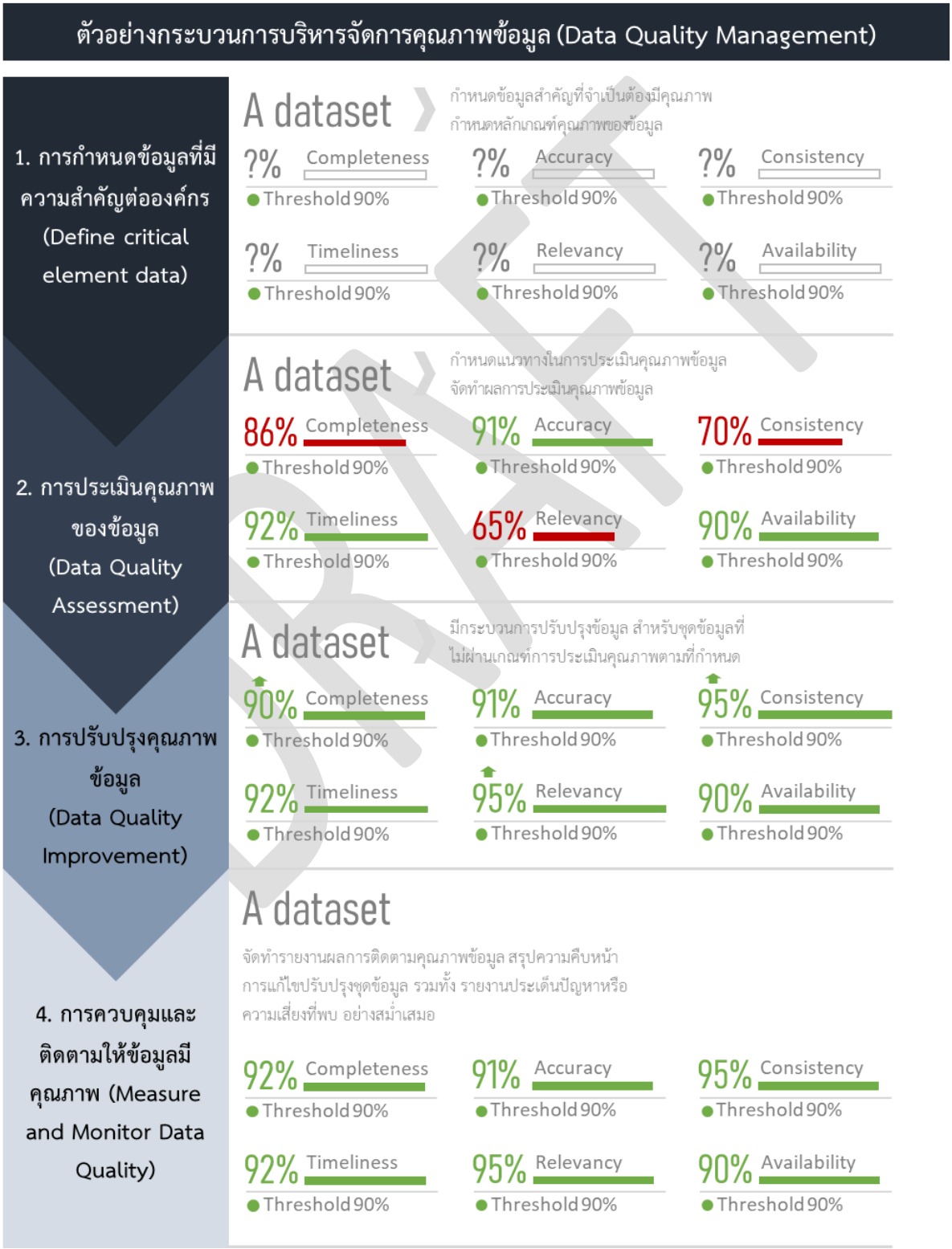
(๓) มีกระบวนการควบคุมการปรับปรุงคุณภาพข้อมูลที่รัดกุม เช่น กระบวนการบริหารจัดการการเปลี่ยนแปลง การจัดเก็บหลักฐานสำหรับก่อนและหลังการแก้ไขข้อมูล เป็นต้น รวมถึงกำหนดบุคลากรหรือหน่วยงานที่รับผิดชอบในเรื่องดังกล่าว

๒.๓.๔ การควบคุมและติดตามให้ข้อมูลมีคุณภาพ (Measure and Monitor Data Quality) โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(๑) มีกระบวนการควบคุมและติดตามผลการประเมินคุณภาพข้อมูลอย่างต่อเนื่อง รวมถึงควรมีการสอบทานคุณภาพข้อมูลให้เป็นไปตามหลักเกณฑ์ที่กำหนดอย่างสม่ำเสมอ

(๒) กำหนดให้มีขั้นตอนในการรายงานไปยังบุคลากรหรือหน่วยงานที่เกี่ยวข้อง เมื่อตรวจพบชุดข้อมูลที่มีคุณภาพต่ำกว่าที่เกณฑ์กำหนดไว้

(๓) จัดทำรายงานผลการติดตามคุณภาพข้อมูล สรุปความคืบหน้าการแก้ไขปรับปรุงชุดข้อมูล รวมทั้งรายงานประเด็นปัญหาหรือความเสี่ยงที่พบ ภาพรวมปัญหาและสาเหตุที่ทำให้ชุดข้อมูลไม่มีคุณภาพ นำเสนอต่อคณะกรรมการที่ทำหน้าที่กำกับดูแลข้อมูล หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมายอย่างสม่ำเสมอ



๒.๔ การบริหารจัดการความเสี่ยงด้านข้อมูล (Data Risk Management)

บริษัทควรมีกระบวนการบริหารจัดการความเสี่ยงด้านข้อมูล โดยควรครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(๑) กำหนดเกณฑ์ในการประเมินความเสี่ยงจากปัจจัยหรือเหตุการณ์ซึ่งอาจส่งผลกระทบต่อคุณภาพข้อมูล ได้แก่ ความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความสอดคล้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงกับความต้องการของผู้ใช้ (Relevancy) และความพร้อมใช้งาน (Availability) ที่อาจเกิดขึ้นในการดำเนินงานที่เกี่ยวข้องกับการกำกับดูแลข้อมูล และการบริหารจัดการข้อมูล

(๒) แนวทางและมาตรการในการควบคุมความเสี่ยงที่อาจเกิดขึ้น และส่งผลต่อคุณภาพของข้อมูล

(๓) การติดตามและรายงานผลการบริหารความเสี่ยงข้อมูลให้คณะกรรมการที่ทำหน้าที่กำกับดูแลข้อมูล หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสม

ทั้งนี้ บริษัทอาจพิจารณาให้เจ้าของข้อมูล (Data Owners) เป็นผู้รับผิดชอบหลักในการดำเนินการดังกล่าว โดยมีหน่วยงานที่ปฏิบัติหน้าที่ในการบริหารความเสี่ยงเป็นผู้ให้คำปรึกษาและแนะนำ เพื่อให้สามารถดำเนินการดังกล่าวได้อย่างมีประสิทธิภาพ

<u>ตัวอย่าง ประเด็นความเสี่ยงจากปัจจัยหรือเหตุการณ์ที่ส่งผลกระทบต่อข้อมูล</u>

สถานการณ์ความเสี่ยง	ประเด็นที่เกี่ยวข้องกับความเสี่ยง
การบริหารจัดการที่ขาดประสิทธิภาพ	การกำกับดูแลข้อมูล รวมทั้งการจัดโครงสร้างองค์กรให้รองรับ / นโยบายการกำกับดูแลข้อมูล
การถูกล่วงละเมิดการรักษาความมั่นคงปลอดภัยของข้อมูล / การรักษาความเป็นส่วนบุคคลของข้อมูล	การรักษาความมั่นคงปลอดภัยของข้อมูล (Data security) / การรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy)
คุณภาพของข้อมูลลดลงตามระยะเวลาการใช้งาน	การบริหารจัดการวงจรชีวิตของข้อมูล (Data Life Cycle Management)
ข้อผิดพลาดของความเชื่อมโยงของข้อมูล	การบริหารจัดการคำอธิบายชุดข้อมูล (Metadata Management)
ไม่สามารถส่งรายงานได้ตามระยะเวลาที่หน่วยงานกำกับดูแลกำหนด	การบริหารจัดการคุณภาพข้อมูลในเรื่องความเป็นปัจจุบันของข้อมูล (Timeliness)
ข้อมูลไม่มีคุณภาพตามเกณฑ์ที่กำหนด	การประเมินคุณภาพของข้อมูล (Data Quality Assessment) / การปรับปรุงคุณภาพข้อมูล (Data Quality Improvement)
ผู้ให้บริการจากภายนอกสามารถเข้าถึงข้อมูลสำคัญ หรือนำข้อมูลออกจากระบบคอมพิวเตอร์ของบริษัท โดยไม่ได้รับอนุญาต	การบริหารจัดการผู้ให้บริการจากภายนอก (Third Party Management)

๒.๕ การรักษาความมั่นคงปลอดภัยของข้อมูล (Data security)

การรักษาความมั่นคงปลอดภัยของข้อมูล ให้บริษัทดำเนินการตามที่ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต / ประกันวินาศภัย พ.ศ. ๒๕๖๓ และแนวปฏิบัติ เรื่อง การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต/ประกันวินาศภัย พ.ศ. ๒๕๖๔ กำหนด โดยควร

พิจารณาให้ครอบคลุมตามหลักการ CIA ซึ่งประกอบด้วย การรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability)

ทั้งนี้ แนวทางเพิ่มเติมสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูล มีดังนี้

(๑) จัดให้มีนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security Policy) ที่เป็นลายลักษณ์อักษร อาจเป็นนโยบายที่จัดทำขึ้นเฉพาะหรือเพิ่มเติมให้ครอบคลุมจากนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) ของบริษัท

(๒) กำหนดมาตรฐาน หรือระเบียบวิธีด้านการรักษาความมั่นคงปลอดภัยของข้อมูล โดยครอบคลุมอย่างน้อย ในเรื่องดังต่อไปนี้

- การจัดชั้นความลับของข้อมูลที่เหมาะสมตามระดับความสำคัญของข้อมูล
- การกำหนดสิทธิ์ในการเข้าถึงข้อมูลอย่างชัดเจน
- การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล โดยประเมินความเสี่ยงจากการระบุแหล่งที่จัดเก็บข้อมูลที่สำคัญและอ่อนไหว และแนวทางการป้องกันที่ใช้อยู่ในปัจจุบันว่ามีความสอดคล้องและเหมาะสมเพียงพอกับความเสี่ยง
- จัดให้มีแนวทางบริหารจัดการความมั่นคงปลอดภัยของข้อมูล โดยกำหนดกระบวนการควบคุมดูแล การติดตาม และตรวจสอบการเข้าถึงของข้อมูล รวมถึงกำหนดบุคลากรหรือหน่วยงานที่รับผิดชอบในเรื่องดังกล่าว

<u>ตัวอย่างของแนวทางการบริหารจัดการความมั่นคงปลอดภัยของข้อมูล</u>

ตัวอย่างแนวทาง	คำอธิบาย
การใช้ระบบเฝ้าระวังความปลอดภัย (Monitoring System)	เพื่อช่วยตรวจจับภัยคุกคามที่อาจเกิดขึ้น รวมถึงกิจกรรมที่ผิดปกติที่เกิดขึ้นภายในระบบงาน และแจ้งเตือนไปยังผู้ดูแลข้อมูล หรือผู้ดูแลระบบความมั่นคงปลอดภัย
การเข้ารหัสข้อมูล (Encryption)	เพื่อป้องกันข้อมูลจากผู้ที่ไม่มีสิทธิ์ในการเข้าถึง เปลี่ยนแปลงแก้ไข และทำให้ไม่สามารถอ่านข้อมูลได้หากไม่มีคีย์ถอดรหัส
การปิดทับข้อมูล (Data Masking)	เพื่อช่วยปกป้องหรือปกปิดข้อมูลจริงที่มีความสำคัญในการนำข้อมูลไปใช้ โดยทำการปกปิดหรือปิดบังข้อมูลเพื่อทำให้ข้อมูลนั้นแสดงเป็นข้อมูลหลอกหรือนามแฝง

๒.๖ การรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy)

การรักษาความเป็นส่วนบุคคลข้อมูล ให้บริษัทปฏิบัติตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือ ประกาศสำนักงาน คปภ. เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประชีวิต/วินาศภัย พ.ศ. ๒๕๖๔ เป็นต้น โดยการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลควรพิจารณาเท่าที่จำเป็น ภายใต้วัตถุประสงค์ที่กำหนดไว้เมื่อได้รับข้อมูลส่วนบุคคล รวมทั้งมีการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลทั้งที่อยู่ในรูปแบบกระดาษ และอิเล็กทรอนิกส์

นอกจากนี้ ควรมีแนวทางดำเนินการเพื่อรองรับสถานการณ์ในกรณีที่เกิดเหตุการณ์ละเมิด เช่น ข้อมูลผู้เอาประกันภัยหรือข้อมูลลูกค้ามีการรั่วไหล โดยเฉพาะอย่างยิ่งกรณีข้อมูลส่วนบุคคลมีการรั่วไหล บริษัทต้องพิจารณาดำเนินการตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดไว้ ทั้งการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล รวมทั้งแนวทางหรือมาตรการในการเยียวยาของบริษัท

ส่วนที่ ๓ : แนวทางการประเมินระดับการกำกับดูแลข้อมูล (Data Governance Maturity Assessment)

บริษัทควรมีการประเมินระดับการกำกับดูแลข้อมูล เพื่อวัดประสิทธิภาพ และทราบถึงสถานะของระดับการกำกับดูแลข้อมูลของบริษัทที่ดำเนินการอยู่ในปัจจุบัน เพื่อนำผลการประเมินมาเป็นข้อมูลประกอบการพิจารณาพัฒนาแนวทางการบริหารจัดการข้อมูลให้มีประสิทธิภาพยิ่งขึ้น

ทั้งนี้ การกำหนดเกณฑ์ในการประเมินระดับการกำกับดูแลข้อมูลของบริษัท ควรพิจารณากำหนดให้สอดคล้องกับขนาด ลักษณะ ความเสี่ยง และความซับซ้อนในการดำเนินธุรกิจของบริษัท

ตัวอย่าง การกำหนดแนวทางการประเมินระดับการกำกับดูแลข้อมูล

เกณฑ์ในการประเมินระดับการกำกับดูแลข้อมูล สามารถแบ่งได้ ๖ ระดับ ดังนี้	
ระดับ ๐	องค์กรยังไม่มีการริเริ่มการบริหารจัดการข้อมูล หรือกระบวนการที่เกี่ยวข้องการบริหารจัดการข้อมูลอย่างเป็นทางการ
ระดับ ๑	องค์กรอยู่ในระดับเริ่มต้นดำเนินการบริหารจัดการข้อมูล โดยมีการกำกับดูแลข้อมูลเพียงเล็กน้อย หรือไม่มีเลย มีเครื่องมือและทรัพยากรในการบริหารจัดการข้อมูลที่จำกัด แต่ยังขาดบุคลากรที่สามารถปฏิบัติหน้าที่ในด้านดังกล่าวได้ รวมถึงการกำหนดหน้าที่ความรับผิดชอบด้านการบริหารจัดการข้อมูลยังคงจำกัดอยู่ที่บุคลากรบางกลุ่มเท่านั้น
ระดับ ๒	องค์กรมีการจัดสรรทรัพยากรที่สอดคล้องกับการบริหารจัดการข้อมูลขององค์กร และมีเครื่องมือที่ช่วยสนับสนุนหรืออำนวยความสะดวกให้แก่บุคลากรในการดำเนินการ รวมทั้งมีการกำหนดบทบาทหน้าที่ความรับผิดชอบอย่างชัดเจนให้แก่ผู้ที่มีส่วนเกี่ยวข้อง และสามารถบริหารจัดการข้อมูลที่มีอยู่แล้วภายในองค์กรได้ในระดับหนึ่ง แต่ยังไม่ครอบคลุมหรือไม่มีประสิทธิภาพเพียงพอในทุกวงจรชีวิตของข้อมูล
ระดับ ๓	องค์กรมีความสามารถในการบริหารจัดการข้อมูลในทุกวงจรชีวิตของข้อมูล รวมถึงมีการกำหนดกระบวนการ และระเบียบวิธีปฏิบัติที่เป็นทางการมากขึ้น ควบคู่ไปกับการมีหน่วยงานที่เป็นศูนย์กลางเพื่อทำหน้าหน้าที่ในการกำกับดูแลข้อมูล รวมทั้งมีการกำหนดนโยบายและแนวทางในการควบคุมการบริหารจัดการข้อมูลสำหรับหน่วยงานต่างๆ ภายในองค์กร
ระดับที่ ๔	องค์กรมีการบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับข้อมูล และมีแผนการรองรับความเสี่ยง รวมถึงจัดทำตัวชี้วัดประสิทธิภาพของการดำเนินงานดังกล่าว โดยมีเครื่องมือที่ได้มาตรฐานสำหรับการบริหารจัดการข้อมูลตั้งแต่ระดับส่วนบุคคล จนถึงระดับโครงสร้างพื้นฐานขององค์กร ควบคู่ไปกับการกำกับดูแลข้อมูลที่มีประสิทธิภาพทั่วทั้งองค์กร
ระดับที่ ๕	องค์กรมีความสามารถในการคาดการผลลัพธ์ที่ได้จากการใช้ข้อมูลในระดับสูง มีกลไกในการสอบทาน ประเมินผล และปรับปรุงคุณภาพของข้อมูลอย่างต่อเนื่อง รวมถึงมีการควบคุมดูแล การจัดเก็บ การใช้ การส่งข้อมูลในทุกระดับ ทำให้ไม่เกิดความซ้ำซ้อนในการประมวลผลข้อมูล

ที่มา : Data Management Body of Knowledge Second Edition

ทั้งนี้ ปัจจัยที่สามารถนำมาใช้เป็นเกณฑ์ในการวัดระดับการดำเนินการกำกับดูแลข้อมูล บริษัทสามารถพิจารณาจากปัจจัย ๔ ด้านดังต่อไปนี้

(๑) การดำเนินงาน โดยประเมินจากสถานะปัจจุบันของการดำเนินงานด้านการกำกับดูแลและบริหารจัดการ รวมถึงความมีประสิทธิภาพ และประสิทธิผลของการดำเนินงานโดยมุ่งหวังให้เป็นไปตามที่องค์กรตั้งเป้าไว้

(๒) เครื่องมือ การดำเนินงานด้านการกำกับดูแลและบริหารจัดการข้อมูลได้รับการจัดสรรทรัพยากรที่เพียงพอ มีการกำหนดการเข้าถึงและการใช้งานเครื่องมือที่เหมาะสม เพื่อให้ได้ผลลัพธ์ที่มีประสิทธิภาพ รวมถึงมีการวางแผนการนำเครื่องมือและเทคโนโลยีมาใช้เพื่อรองรับความสามารถในด้านการกำกับดูแลและบริหารจัดจากข้อมูลในอนาคต

(๓) มาตรฐาน และระเบียบวิธีปฏิบัติ การดำเนินงานที่เกี่ยวข้องในด้านการกำกับดูแลและบริหารจัดการข้อมูลมีมาตรฐาน และระเบียบวิธีปฏิบัติ เพื่อเป็นแนวทางแก่ให้บุคลากรที่เกี่ยวข้อง รวมทั้งการนำปฏิบัติจริงได้อย่างมีประสิทธิผล

(๔) บุคลากร องค์กรมีบุคลากรเพื่อดำเนินงานด้านการกำกับดูแลและบริหารจัดการข้อมูล รวมทั้งมีความรู้และความเข้าใจที่สามารถดำเนินงานดังกล่าวได้อย่างมีประสิทธิภาพ และได้รับการฝึกอบรมให้ความรู้ที่เกี่ยวข้องกับการดำเนินดังกล่าวอย่างเพียงพอเหมาะสม

ภาคผนวก

ตัวอย่าง ข้อมูลสำคัญที่จำเป็นต้องมีคุณภาพ (Critical Data Elements) ในธุรกิจประกันภัย

ประเภทข้อมูล	ตัวอย่าง	ความเป็นส่วนบุคคล	การใช้งาน	แหล่งข้อมูล
	ข้อมูลที่เกี่ยวข้องกับการประกันภัยแบบดั้งเดิม (Traditional Data)			
ข้อมูลทางประชากร (Demographic data)	เพศ, อายุ, สถานภาพสมรส, อาชีพ , ที่อยู่	ข้อมูลส่วนบุคคล	เกณฑ์คัดเลือกภัย (Risk selection)	เจ้าของกรมธรรม์ (Policy holders)
ข้อมูลทางการแพทย์ (Medical data)	ประวัติการรักษา, โรคประจำตัว, ประวัติการเจ็บป่วยในครอบครัว, การตรวจยีน	ข้อมูลส่วนบุคคล	เกณฑ์คัดเลือกภัย (Risk selection)	เจ้าของกรมธรรม์ (Policy holders)
ข้อมูลทรัพย์สินที่เสี่ยงภัย (Exposure data)	ประเภทรถยนต์, มูลค่าที่อยู่อาศัย, ประเภทอาคารที่อยู่อาศัย	ข้อมูลส่วนบุคคล / ข้อมูลที่ไม่เป็นส่วนบุคคล	เกณฑ์คัดเลือกภัย (Risk selection)	เจ้าของกรมธรรม์ (Policy holders)
ข้อมูลพฤติกรรม (Behavioural data)	การสูบบุหรี่, พฤติกรรมการดื่มเครื่องดื่มแอลกอฮอล์, ระยะทางขับขี่ต่อปี, อัตราการขาดผลบังคับของกรมธรรม์ประกันชีวิต, ความรับผิดส่วนแรก	ข้อมูลส่วนบุคคล / ข้อมูลที่ไม่เป็นส่วนบุคคล	เกณฑ์คัดเลือกภัย (Risk selection), การตลาด (Marketing)	เจ้าของกรมธรรม์ (Policy holders), ค่าสถิติภายในภาคธุรกิจ (Industry statistics)
ข้อมูลความเสียหายที่เกิดขึ้น (Loss data)	รายงานค่าสินไหมทดแทนจากอุบัติเหตุรถยนต์, รายงานค่าสินไหมทดแทนจากประกันภัยความรับผิดต่อบุคคลภายนอก	ข้อมูลส่วนบุคคล / ข้อมูลที่ไม่เป็นส่วนบุคคล	การบริหารจัดการค่าสินไหมทดแทน (Claims management)	เจ้าของกรมธรรม์ (Policy holders), ข้อมูลภายในภาคธุรกิจ (Information exchange within industry)
ข้อมูลทางสถิติของประชากร (Population data)	อัตรามรณะ, อัตราการป่วย	ข้อมูลนิรนาม และข้อมูลรวมของประชากร	เกณฑ์คัดเลือกภัย (Risk selection)	หน่วยงานรัฐ (Government), ค่าสถิติภายในภาคธุรกิจ (Industry statistics), สถาบันการศึกษา (Academia)

ประเภทข้อมูล	ตัวอย่าง	ความเป็นส่วนบุคคล	การใช้งาน	แหล่งข้อมูล
ข้อมูลความเสี่ยงภัย (Hazard data)	ความถี่และความรุนแรงของภัยธรรมชาติ	ข้อมูลที่ไม่เป็นส่วนบุคคล	เกณฑ์คัดเลือกภัย (Risk selection)	หน่วยงานรัฐ (Government), ค่าสถิติภายในภาคธุรกิจ (Industry statistics), สถาบันการศึกษา (Academia)
ข้อมูลอื่นๆ (Other traditional data)	การอ้างอิงข้อมูลเครดิต, รายงานการปรับค่าสินไหมทดแทน (Claim adjustment reports)	ข้อมูลส่วนบุคคล / ข้อมูลที่ไม่เป็นส่วนบุคคล	เกณฑ์คัดเลือกภัย (Risk selection), การตลาด (Marketing), การบริหารจัดการค่าสินไหมทดแทน (Claims management)	เจ้าของกรมธรรม์ (Policy holders), สำนักงานเครดิต (Credit agents), หน่วยงานที่มีความเกี่ยวข้องกับงานสินไหมทดแทน (Agencies involved in the claim)
	ข้อมูลที่เกี่ยวข้องกับการประกันภัยสมัยใหม่ (New Data in the era of digitization)			
ข้อมูล Internet of Things (IoT data)	พฤติกรรมการขับขี่ (Telematics), ข้อมูลกิจกรรมที่หรือสุขภาพที่วัดค่าได้จากอุปกรณ์สวมใส่ (Wearables)	ข้อมูลส่วนบุคคล	เกณฑ์คัดเลือกภัย (Risk selection), การบริหารจัดการค่าสินไหมทดแทน (Claims management)	อุปกรณ์เก็บข้อมูล (Data collection devices)
ข้อมูลสื่อออนไลน์ (Online media data)	การค้นหาเว็บไซต์, พฤติกรรมการซื้อของออนไลน์, กิจกรรมบนสื่อโซเชียลมีเดีย	ข้อมูลส่วนบุคคล	เกณฑ์คัดเลือกภัย (Risk selection), การตลาด (Marketing),	ผู้ให้บริการอินเทอร์เน็ต (Internet providers) ผู้ให้บริการโปรแกรมค้นหาข้อมูล (Search engine providers), แพล็ตฟอร์มสื่อโซเชียลมีเดีย (Social media platform), ผู้ให้บริการพาณิชย์อิเล็กทรอนิกส์ (E-Commerce providers)

ประเภทข้อมูล	ตัวอย่าง	ความเป็นส่วนบุคคล	การใช้งาน	แหล่งข้อมูล
ข้อมูลดิจิตอลของบริษัทประกันภัย (Insurer's own digital data)	ข้อมูลบทสนทนา หรือข้อมูลการติดต่อสื่อสารระหว่างผู้เอาประกันภัย และบริษัทประกันภัย	ข้อมูลส่วนบุคคล	การตลาด (Marketing), การบริหารจัดการค่าสินไหมทดแทน (Claims management)	ศูนย์ให้บริการลูกค้า เว็ปไซต์และแอปพลิเคชันของบริษัทประกันภัย
ข้อมูลอื่นๆ (Other digital data)	ภาพถ่ายเซลฟีเพื่อประมาณการอายุปัจจุบันของผู้เอาประกันชีวิต	ข้อมูลส่วนบุคคล / ข้อมูลที่ไม่เป็นส่วนบุคคล	เกณฑ์คัดเลือกภัย (Risk selection), การตลาด (Marketing), การบริหารจัดการค่าสินไหมทดแทน (Claims management)	เจ้าของกรมธรรม์ (Policy holders), ทุกแหล่งข้อมูลที่มีความเกี่ยวข้องกับการประกันภัย

ตัวอย่างเกณฑ์ในการประเมินระดับของการกำกับดูแลข้อมูลในปัจจุบันกับเป้าหมายที่องค์กรกำหนดไว้

มิติ	องค์ประกอบ	Current Level ๐ - ๕	Desired Level ๑ - ๕	นิยามระดับต่ำสุด	มีความตระหนักรู้ วิสัยทัศน์ในการกำกับดูแลข้อมูล การลงทุน และการนำไปปฏิบัติ	มียุทธวิธี ความคิดริเริ่มในการสร้างแนวทางการกำกับดูแลข้อมูล	มีเป้าหมาย การมุ่งเป้าที่ชัดเจนขึ้นและมีความมุ่งมั่นในธรรมาภิบาลข้อมูลขับเคลื่อนการเริ่มต้นที่สำคัญ	มียุทธศาสตร์ มีการระบุกลยุทธ์ทางธรรมาภิบาลข้อมูลอย่างชัดเจนและมีการสนับสนุนจากผู้บริหาร	มีการใช้งานแพร่หลาย ธรรมาภิบาลข้อมูลมีการใช้งานอย่างแพร่หลายและเป็นวัฒนธรรมด้านข้อมูล	นิยามระดับสูงสุด
					Level ๑	Level ๒	Level ๓	Level ๔	Level ๕	
คน (People)	โครงสร้างองค์กร			ไม่เป็นทางการ	ตระหนักรู้ในวัตถุประสงค์ และความสำคัญของธรรมาภิบาลข้อมูล	มีข้อจำกัดในการแยกมีหน่วยงานย่อยภายใน	จัดตั้งโครงสร้างทีมและต้นแบบธรรมาภิบาลข้อมูล	มีการสนับสนุนจากผู้บริหารระดับสูง	มีการแต่งตั้ง Chief Data Officer หรือตำแหน่งเทียบเท่า	เป็นทางการและมีการบูรณาการ
	หน้าที่และความรับผิดชอบ			ไม่สัมพันธ์กัน/ไม่ร่วมมือกัน	ทรัพยากรด้านธรรมาภิบาลข้อมูลไม่มีการจำกัดความอย่างชัดเจนในระดับองค์กร	หน้าที่ความรับผิดชอบในธรรมาภิบาลข้อมูลเป็นแบบไซโล	ศูนย์รวมผู้เชี่ยวชาญเฉพาะด้านเพื่อสนับสนุนความต้องการและความคิดริเริ่มขององค์กร	มีการระบุบริกรข้อมูล เจ้าของข้อมูลและผู้ใช้ข้อมูล	มีการวางความรับผิดชอบและการเชื่อมโยงกันในบทบาทหน้าที่ ทั้งในระบบฝ่ายและองค์กร	เป็นทางการและมีการตรวจสอบในระดับองค์กร
	วัฒนธรรมและการสื่อสาร			ไม่เปิดเผย/ปิดบัง	หน้าที่ความรับผิดชอบของแต่ละคนในการรักษาไว้ซึ่งความมุ่งมั่นในวิสัยทัศน์ด้านธรรมาภิบาลข้อมูล	ไม่มีการเชื่อมโยงกันในการปฏิบัติงานข้ามหน่วยงาน	ก่อตั้งการบริการกลุ่มลูกค้าภายใน	มีกระบวนการ การกำกับดูแล และทรัพยากรที่เปิดเผยโปร่งใส และเข้าถึงได้	มีการเปลี่ยนแปลงวัฒนธรรมที่นำไปสู่การพัฒนาปรับปรุงด้านธรรมาภิบาลข้อมูลอย่างต่อเนื่อง	เปิดเผย/โปร่งใส
กระบวนการ (Process)	การจัดการสินทรัพย์ข้อมูล			ไม่เป็นหมวดหมู่/กระจัดกระจาย	ขาดความเข้าใจด้านสินทรัพย์ข้อมูลและความเป็นเจ้าของข้อมูล	ในแต่ละหน่วยธุรกิจมีการครอบครองข้อมูลที่แยกออกจากหมวดหมู่ในสินทรัพย์ข้อมูล	มีการวางมาตรฐานในการจัดการสินทรัพย์ข้อมูลในแต่ละหน่วยงาน	มีการบริหารจัดการบัญชีข้อมูลระดับองค์กรที่เป็นมาตรฐาน	มีแผนการรักษาไว้ให้คงอยู่เพื่อรองรับการเติบโตทั้งด้านปริมาณและความซับซ้อนของข้อมูล	มีการจัดทำบัญชีข้อมูลทั้งองค์กร
	มาตรฐานกระบวนการ			ความสมบูรณ์แค่ภายนอก/ไม่เป็นมาตรฐาน	การจัดการกระบวนการที่ไม่มีประสิทธิภาพ	ระบุเวลาในการตอบสนองต่อการขอใช้ข้อมูล	มีการวางเส้นทางสำหรับสินทรัพย์ข้อมูลใหม่ๆ ด้วยกระบวนการที่ชัดเจนและได้รับการอนุมัติแล้ว	มีการเข้าถึงคำจำกัดความของข้อมูลหลายระดับภายใต้การจัดการ	มีต้นแบบของการบริการด้านธรรมาภิบาลข้อมูลภายในองค์กร	เป็นมาตรฐานทั้งภายนอกและภายใน

มิติ	องค์ประกอบ	Current Level ๐ - ๕	Desired Level ๑ - ๕	นิยามระดับต่ำสุด	มีความตระหนักรู้ วิสัยทัศน์ในการกำกับดูแลข้อมูล การลงทุน และการนำไปปฏิบัติ	มียุทธวิธี ความคิดริเริ่มในการสร้างแนวทางการกำกับดูแลข้อมูล	มีเป้าหมาย การมุ่งเป้าที่ชัดเจนขึ้นและมีความมุ่งมั่นในธรรมาภิบาลข้อมูลขับเคลื่อนการเริ่มต้นที่สำคัญ	มียุทธศาสตร์ มีการระบุกลยุทธ์ทางธรรมาภิบาลข้อมูลอย่างชัดเจนและมีการสนับสนุนจากผู้บริหาร	มีการใช้งานแพร่หลาย ธรรมาภิบาลข้อมูลมีการใช้งานอย่างแพร่หลายและเป็นวัฒนธรรมด้านข้อมูล	นิยามระดับสูงสุด
					Level ๑	Level ๒	Level ๓	Level ๔	Level ๕	
	นิยามและมาตรฐานข้อมูล			หลากหลาย/เข้าใจยาก	ไม่มีการติดตามอย่างต่อเนื่องในมาตรฐานสากล	กระตุ้นให้เกิดการใช้มาตรฐานสากลมากที่สุดเท่าที่เป็นไปได้	มีแนวทางการใช้งานที่เหมาะสมสำหรับแหล่งข้อมูลที่เป็นมาตรฐาน	มีการเข้าถึงเมตาดาตา ทรัพยากร มาตรฐานข้อมูล และนโยบายได้อย่างเปิดเผย	มีกระบวนการทำงานร่วมกันในการจัดการสินทรัพย์ข้อมูล	เป็นมาตรฐานและเข้าถึงได้
เทคโนโลยี (Technology)	การจัดการคุณภาพของข้อมูล			ไม่ถูกต้อง / ไม่น่าเชื่อถือ	ไม่มีกระบวนการจัดการที่เข้มงวดหรือเชื่อถือได้ในการรักษาคุณภาพของข้อมูล	หน่วยงานมีการระบุหน้าที่ความรับผิดชอบในด้านคุณภาพข้อมูล	มีการวางการวัดคุณภาพของข้อมูล และของเขตของการใช้งาน	มีความสามารถในการสร้างการเปลี่ยนแปลงต่อระบบเพื่อรักษาคุณภาพของข้อมูล	ธรรมาภิบาลข้อมูลสามารถตอบสนองความเปลี่ยนแปลงได้	เชื่อถือได้
	การตรวจสอบและวัดผล			ไม่มี / เฉพาะหน้าเป็นครั้งๆ	การระบุตัวตนที่ไม่สอดคล้องกันในการวัดคุณภาพในแต่ละหน่วยงาน	ตรวจสอบและติดตามตัวชี้วัดที่สำคัญในระบบของหน่วยงาน	รองรับการเติบโตของระบบแบบเรียลไทม์และสนับสนุนการตัดสินใจที่สำคัญ	มีการรายงานที่เป็นมาตรฐานและ dashboard แบบเรียลไทม์ในการวัดคุณภาพข้อมูล	มีการติดตาม/ตรวจสอบคุณภาพของข้อมูลและการตรวจจับความสามารถแบบอัตโนมัติ	การตรวจสอบและมีวงรอบอย่างเป็นทางการ
	เครื่องมือ			ต่างคนต่างใช้เครื่องมือไม่เหมือนกัน	มีการใช้เครื่องมือที่แตกต่างกันในแต่ละหน่วยงานโดยไม่คำนึงถึงผลกระทบต่อธรรมาภิบาลข้อมูล	แต่ละหน่วยงานมีการประเมินชุดเครื่องมือใหม่ๆเพื่อประโยชน์ในการปรับปรุงธรรมาภิบาลข้อมูล	มีสถาปัตยกรรมและโครงสร้างในกระบวนการต่างๆ มีความสอดคล้องในด้านคุณภาพข้อมูลและมีการควบคุมการเข้าถึง	มีระบบที่เข้าถึงง่ายในการบันทึกการละเมิดและข้อเสนอแนะในการปรับปรุง	มีการวางกรอบและนโยบายบนคลาวด์หรือการบริการด้านการจัดการ	บูรณาการกันระดับองค์กร

<u>เอกสารอ้างอิง</u>

มาตรฐานและแนวปฏิบัติอ้างอิง (Reference Standards and Best Practices)
๑. DAMA-DMBOK: Data Management Body of Knowledge: 2nd Edition ๒. Data Governance for Government: ธรรมาภิบาลข้อมูลภาครัฐ เวอร์ชัน ๑.๐ ๓. แนวปฏิบัติการกำกับดูแลข้อมูล (Data Governance Guideline) ธนาคารแห่งประเทศไทย ๔. Issues Paper on the Use of Big Data Analytics in Insurance by International Association of Insurance Supervisors (IAIS)

คปภ.

สำนักงานคณะกรรมการกำกับและส่งเสริม
การประกอบธุรกิจประกันภัย(คปภ.)