ธนาคารแห่งประเทศไทย
BANK OF THAILAND

Consultation Paper

แนวปฏิบัติการกำกับดูแลข้อมูล
(Data Governance Guideline)

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ธนาคารแห่งประเทศไทย
กรกฎาคม 2563

สารบัญ

แนวปฏิบัติธนาคารแห่งประเทศไทย
เรื่อง การกำกับดูแลข้อมูล (Data Governance)

1. เหตุผลในการออกแนวปฏิบัติ

ข้อมูลเป็นทรัพย์สินที่สำคัญของสถาบันการเงิน การนำเทคโนโลยีมาประยุกต์เพื่อใช้ประโยชน์จากข้อมูล ตั้งแต่ข้อมูลทั่วไปจนถึงข้อมูลทางการเงินของลูกค้าเป็นกลไกในการขับเคลื่อนการให้บริการทางการเงินในยุคปัจจุบัน โดยสถาบันการเงินนำเอาข้อมูลเหล่านั้นมาพัฒนาผลิตภัณฑ์และการบริการทางการเงินให้ตรงกับความต้องการของลูกค้า รวมทั้งสามารถใช้ประโยชน์จากข้อมูลในการบริหารความเสี่ยงอย่างมีประสิทธิภาพอีกด้วย หากสถาบันการเงินไม่มีการกำกับดูแลและบริหารจัดการข้อมูลได้อย่างเหมาะสมเพียงพอ อาจก่อให้เกิดความเสี่ยงที่มีนัยสำคัญจนกระทบต่อความเชื่อมั่นของระบบสถาบันการเงินได้ ดังนั้น สถาบันการเงินต้องจัดให้มีการดูแลคุณภาพข้อมูล การรักษาความมั่นคงปลอดภัย และการรักษาความเป็นส่วนบุคคลของข้อมูล อย่างเหมาะสมเพียงพอสอดคล้องตามระดับความเสี่ยงของสถาบันการเงิน

ธปท. สนับสนุนการนำข้อมูลไปใช้ก่อให้เกิดประโยชน์อย่างเต็มประสิทธิภาพ เพื่อพัฒนาการให้บริการทางการเงินให้ดียิ่งขึ้น ในทางกลับกัน สถาบันการเงินต้องมีการบริหารจัดการความเสี่ยงจากการใช้ข้อมูลอย่างเหมาะสมควบคู่กันด้วย ดังนั้น ธปท. จึงออกแนวปฏิบัติการกำกับดูแลข้อมูล เพื่อให้สถาบันการเงินนำไปใช้อ้างอิงเป็นมาตรฐานขั้นต่ำในการกำกับดูแลข้อมูลสอดคล้องกับหลักการที่ดีที่ได้รับการยอมรับในระดับสากล โดยมีแนวทางและการบริหารจัดการที่เหมาะสมเพียงพอ ซึ่งเป็นประโยชน์ต่อการเข้าถึงบริการทางการเงินของประชาชน การรักษาเสถียรภาพของระบบสถาบันการเงิน และความเชื่อมั่นของประชาชนต่อบริการของผู้ให้บริการทางการเงิน

2. ขอบเขตการถือปฏิบัติ

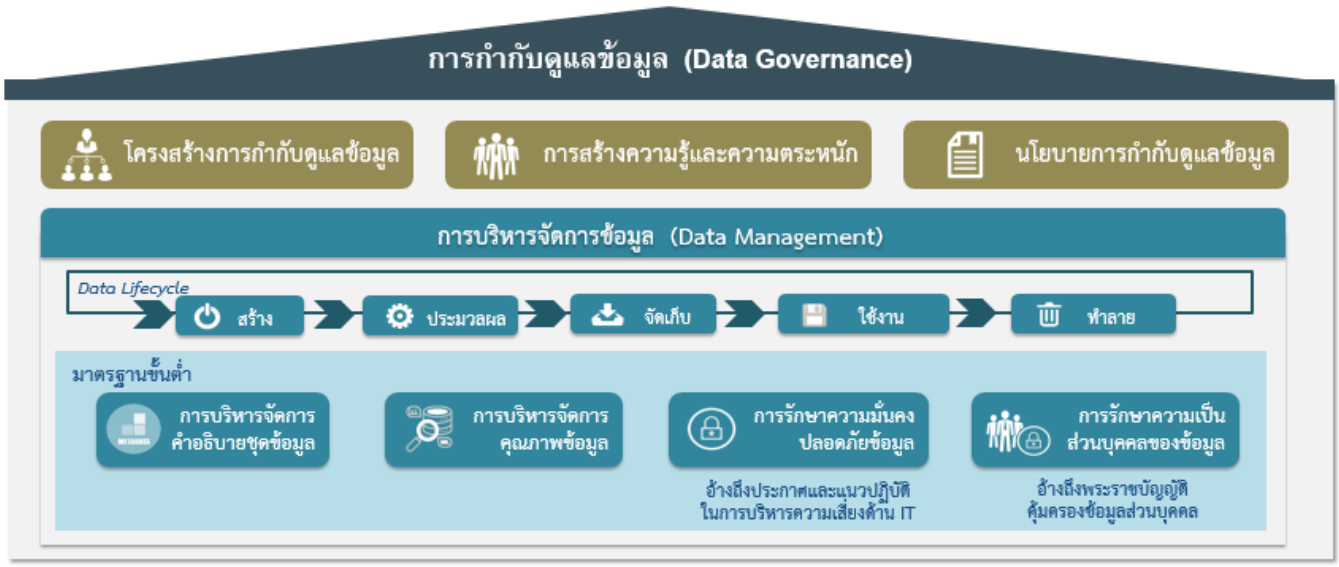
แนวปฏิบัติฉบับนี้ ใช้กับสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

3. หลักการของแนวปฏิบัติ

แนวปฏิบัติฉบับนี้ ได้กำหนดมาตรฐานขั้นต่ำที่เกี่ยวกับการกำกับดูแลข้อมูล โดยเป็นส่วนเพิ่มเติมจากประกาศและแนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) เพื่อให้มั่นใจว่าข้อมูลในองค์กรมีความครบถ้วน ถูกต้อง ทันสมัย ปลอดภัย เชื่อมโยงกับข้อมูลจากแหล่งอื่นได้ และเป็นประโยชน์ต่อการดำเนินธุรกิจของสถาบันการเงิน

สถาบันการเงินที่สามารถปฏิบัติตามมาตรฐานขั้นต่ำที่กำหนดไว้ตามแนวปฏิบัตินี้แล้ว อาจพิจารณาให้มีการกำกับดูแลครอบคลุมทุกชุดข้อมูลในองค์กร รวมทั้ง มีการรายงานและวัดผลสำเร็จเพื่อพัฒนาการกำกับดูแลข้อมูลให้ดีขึ้นอย่างต่อเนื่อง รวมทั้งอาจพิจารณาใช้เทคโนโลยีเพื่อยกระดับการดำเนินการด้านการกำกับดูแลข้อมูลได้ตามระดับความพร้อมของสถาบันการเงินเอง

4. ภาพรวมของแนวปฏิบัติ



การกำกับดูแลข้อมูล เพื่อให้มีการดูแลคุณภาพข้อมูล การรักษาความมั่นคงปลอดภัยของข้อมูล และการรักษาความเป็นส่วนบุคคลของข้อมูล ประกอบไปด้วย 2 ส่วน ได้แก่

1. การกำกับดูแลข้อมูล (data governance) ครอบคลุม การจัดโครงสร้างองค์กรและการกำหนดบทบาทหน้าที่ของผู้ที่เกี่ยวข้องให้รองรับการกำกับดูแลข้อมูล สอดคล้องตามหลัก 3 lines of defense การสร้างความรู้และความตระหนักแก่บุคลากรในองค์กร และการกำหนดนโยบายด้านการกำกับดูแลข้อมูล

2. การบริการจัดการข้อมูล (data management) ตลอดวงจรชีวิตของข้อมูล (data life cycle) ได้แก่ การสร้างหรือการได้มาซึ่งข้อมูล การประมวลผล การจัดเก็บ การใช้งาน และการทำลายข้อมูล ซึ่งครอบคลุมการบริหารจัดการข้อมูลขั้นต่ำ ได้แก่ การบริหารจัดการคำอธิบายชุดข้อมูล (meta data management) การบริหารจัดการคุณภาพของข้อมูล (data quality management) การรักษาความมั่นคงปลอดภัยของข้อมูล (data security) และการรักษาความเป็นส่วนบุคคลของข้อมูล (data privacy)

5. หลักการที่พึงปฏิบัติ

5.1 การกำกับดูแลข้อมูล (data governance)

5.1.1 โครงสร้างการกำกับดูแลข้อมูล

วัตถุประสงค์ *เพื่อให้มีโครงสร้างและบทบาทหน้าที่ในการกำกับดูแลข้อมูลที่เหมาะสมสอดคล้องตามหลัก 3 lines of defenses*

<u>คณะกรรมการที่ทำหน้าที่กำกับดูแลข้อมูล</u>

(1) ควรจัดตั้งคณะกรรมการที่ทำหน้าที่กำกับดูแลข้อมูล โดยประกอบด้วยผู้บริหารที่เกี่ยวข้อง เช่น ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer) ผู้บริหารระดับสูงด้านบริหารจัดการข้อมูล (Chief Data Officer) ผู้บริหารระดับสูงด้านการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Chief Information Security Officer) ผู้บริหารระดับสูงด้านความเสี่ยง (Chief Risk Officer) และผู้บริหารจากส่วนงานอื่นที่เกี่ยวข้อง

(2) บทบาทหน้าที่ของคณะกรรมการที่ทำหน้าที่กำกับดูแลข้อมูล ครอบคลุมอย่างน้อย

- กำหนดเป้าหมายในการกำกับดูแลข้อมูล ให้สอดรับกับแผนกลยุทธ์ของ สง.
- ดูแลให้มีการจัดทำ ทบทวน ปรับปรุงนโยบายการกำกับดูแลข้อมูล
- กำกับดูแลและติดตามการดำเนินงานที่เกี่ยวข้องกับข้อมูล รวมถึงให้คำปรึกษาและตัดสินประเด็นสำคัญที่เกี่ยวข้องกับข้อมูล
- สนับสนุน ส่งเสริม และผลักดันการกำกับดูแลข้อมูลอย่างทั่วถึงและต่อเนื่อง
- ดูแลและสนับสนุนให้มีการสื่อสารกับบุคลากรในองค์กรให้ตระหนักถึงความสำคัญของข้อมูล การใช้ข้อมูลอย่างปลอดภัย เพื่อลดความเสี่ยงด้านข้อมูล

<u>การจัดโครงสร้างองค์กรให้รองรับการกำกับดูแลข้อมูล</u>

(3) จัดให้มีโครงสร้างองค์กรและบทบาทหน้าที่ความรับผิดชอบในกระบวนการกำกับดูแลข้อมูลอย่างชัดเจนเป็นลายลักษณ์อักษร โดยสอดคล้องตามหลักการถ่วงดุล (check and balance) และการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจน (segregation of duties)

(4) ควรดูแลให้มีทรัพยากรทั้งด้านบุคคลากรและเครื่องมือให้เพียงพอที่จะสนับสนุนการปฏิบัติงานที่เกี่ยวข้องกับการกำกับดูแลข้อมูล รวมถึง จัดให้มีบุคลากรที่มีความรู้ความเชี่ยวชาญหรือประสบการณ์ที่เพียงพอในการปฏิบัติหน้าที่ที่ได้รับมอบหมาย

(5) ควรพิจารณาจัดให้มีผู้บริหารระดับสูงทำหน้าที่บริหารจัดการข้อมูล โดยผู้บริหารระดับสูงดังกล่าว ควรมีบทบาทหน้าที่ครอบคลุม

- กำกับดูแลการบริหารจัดการข้อมูล ให้เป็นไปตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องในการกำกับดูแลข้อมูล
- ส่งเสริมการให้ความรู้ ความตระหนัก แก่บุคลากรทั่วทั้งองค์กร

(6) จัดให้มีหน่วยงานหรือทีมงานที่ทำหน้าที่บริหารจัดการข้อมูล ทำหน้าที่ครอบคลุมอย่างน้อย

- จัดทำ ทบทวน ปรับปรุงนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องในการกำกับดูแลข้อมูลให้เป็นปัจจุบันอย่างสม่ำเสมอ
- สื่อสาร ให้ความรู้ และให้คำแนะนำเกี่ยวกับนโยบาย มาตรฐานและระเบียบวิธีปฏิบัติเกี่ยวกับการกำกับดูแลข้อมูล รวมทั้ง การสร้างความตระหนักในการใช้ข้อมูลอย่างเหมาะสมและปลอดภัย เพื่อให้เกิดการกำกับดูแลข้อมูลที่ดีภายใน สง.
- ติดตามสถานะของบริหารจัดการข้อมูล รายงานผลและประเด็นปัญหาหรือความเสี่ยงที่พบต่อคณะกรรมการที่ทำหน้าที่กำกับดูแลข้อมูลเป็นประจำ

(7) จัดให้มีการกำหนดบทบาทหน้าที่ผู้รับผิดชอบในการอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น อนุญาตการเข้าถึงข้อมูล การใช้และเผยแพร่ข้อมูล เป็นต้น รวมถึง การควบคุมดูแลข้อมูลให้มั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐานและระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล เช่น ดูแลให้จัดทำทะเบียนข้อมูลและทบทวนให้เป็นปัจจุบัน ดูแลให้มีการกำหนดชั้นความลับข้อมูลและกำหนดเกณฑ์คุณภาพข้อมูล เป็นต้น

(8) จัดให้มีการกำหนดบทบาทหน้าที่ของผู้ที่นำข้อมูลไปใช้งานตามบทบาทหน้าที่ความผิดชอบให้ชัดเจน โดยมีบทบาทหน้าที่ครอบคลุม

- ปฏิบัติตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องในการกำกับดูแลข้อมูล

- สนับสนุนการกำกับดูแลข้อมูลโดยการให้ความต้องการในการใช้ข้อมูล และรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูลไปยังหน่วยงานหรือทีมงานในการบริหารจัดการข้อมูล

<u>บทบาทหน้าที่ของหน่วยงานที่ทำหน้าที่ด้านการบริหารความเสี่ยง การกำกับการปฏิบัติตามกฎหมายและหลักเกณฑ์ และการตรวจสอบ</u>

(9) จัดให้มีหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านข้อมูล (data risk) ทำหน้าที่ครอบคลุม
- สนับสนุนให้มีการประเมินความเสี่ยงด้านข้อมูลให้เป็นไปตามกรอบและกระบวนการบริหารความเสี่ยงของ สง.
- ให้คำปรึกษา ติดตาม และทบทวนความเสี่ยงด้านข้อมูลให้อยู่ในระดับที่ยอมรับได้ รวมทั้งรวบรวมและเชื่อมโยงความเสี่ยงด้านข้อมูลกับความเสี่ยงด้านอื่นของ สง. และนำเสนอผลการบริหารความเสี่ยงต่อคณะกรรมการที่เกี่ยวข้อง

(10) จัดให้มีหน่วยงานที่ทำหน้าที่กำกับการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับข้อมูล ทำหน้าที่ติดตาม ดูแล ให้คำปรึกษา สอบทานและรายงานการปฏิบัติงานที่เกี่ยวข้องกับข้อมูล เช่น พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น เพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแล

(11) จัดให้มีหน่วยงานที่ทำหน้าที่ตรวจสอบ ทำหน้าที่ตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูล เพื่อสอบทานให้มั่นใจว่าเป็นไปตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล

5.1.2 การสร้างความรู้และความตระหนักด้านการกำกับดูแลข้อมูลในองค์กร

วัตถุประสงค์ *เพื่อให้บุคลากรมีความรู้และความเชี่ยวชาญเพียงพอในการปฏิบัติงาน รวมถึงให้บุคลากรทุกระดับและบุคคลภายนอกที่เกี่ยวข้องมีความตระหนักด้านการกำกับดูแลข้อมูล*

(1) จัดให้มีกระบวนการดูแลให้บุคลากรขององค์กรและบุคคลภายนอกที่ว่าจ้าง เข้าใจ รับทราบและลงนามยอมรับเงื่อนไขการว่าจ้างที่ครอบคลุมการรักษาความมั่นคงปลอดภัยด้านข้อมูล และข้อตกลงการไม่เปิดเผยข้อมูล (non-disclosure agreement) ก่อนเริ่มปฏิบัติงาน

(2) กำหนดโปรแกรมการอบรมและพัฒนาความรู้ความเชี่ยวชาญด้านการกำกับดูแลข้อมูล (training program) ให้แก่บุคลากรที่เกี่ยวข้อง โดยมีการวัดประสิทธิผลของหลักสูตรฝึกอบรมที่จัดขึ้น

(3) กำหนดโปรแกรมในการเสริมสร้างความตระหนัก (awareness program) ด้านการกำกับดูแลข้อมูลแก่บุคลากรทุกระดับและบุคคลภายนอกที่เกี่ยวข้อง โดยมีแผนงานที่ชัดเจน ต่อเนื่องและวัดผลได้ รวมถึงมีการทบทวนและปรับปรุงเนื้อหาอย่างเหมาะสมอย่างสม่ำเสมอ

5.1.3 นโยบายการกำกับดูแลข้อมูล

วัตถุประสงค์ *เพื่อให้มีแนวทางการกำกับดูแลและบริหารจัดการข้อมูลอย่างเหมาะสมเพียงพอสอดคล้องต่อระดับความเสี่ยงของสถาบันการเงิน*

(1) กำหนดให้มีนโยบายการกำกับดูแลข้อมูลเป็นลายลักษณ์อักษร โดยครอบคลุมการกำกับดูแลข้อมูลทั้งองค์กร (enterprise wide) อาจเป็นนโยบายที่จัดทำขึ้นเฉพาะหรือเพิ่มเติมให้ครอบคลุมจากนโยบายที่สถาบันการเงินมีได้ โดยควรครอบคลุม

- ขอบเขตการกำกับดูแลข้อมูลที่ครอบคลุมข้อมูลสำคัญของสถาบันการเงิน รวมถึงการใช้บริการจากบุคคลภายนอก
- โครงสร้างการกำกับดูแลข้อมูล บทบาทและหน้าที่ความรับผิดชอบของคณะกรรมการ ผู้บริหารระดับสูง ฝ่ายงานและบุคลากรที่เกี่ยวข้อง
- การบริการจัดการข้อมูล (data management) ตลอดวงจรชีวิตของข้อมูล (data life cycle) ได้แก่ การสร้างหรือการได้มาซึ่งข้อมูล การประมวลผล การจัดเก็บ การใช้งาน และการทำลายข้อมูล ซึ่งครอบคลุมการบริหารจัดการข้อมูลขั้นต่ำ ได้แก่ การบริหารจัดการคำอธิบายชุดข้อมูล (meta data management) การบริหารจัดการคุณภาพของข้อมูล (data quality management) การรักษาความมั่นคงปลอดภัยของข้อมูล (data security) และการรักษาความเป็นส่วนบุคคลของข้อมูล (data privacy)

(2) นโยบายดังกล่าวต้องได้รับอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย และได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(3) จัดให้มีการชี้แจงและสื่อสารนโยบายให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึง โดยประกาศใช้อย่างเป็นทางการ และมีผลให้ทุกคนในองค์กรถือปฏิบัติ

5.2 การบริหารจัดการข้อมูล (data management)

5.2.1 การบริหารจัดการคำอธิบายชุดข้อมูล (metadata management)

วัตถุประสงค์ *เพื่อให้มีคำอธิบายชุดข้อมูล สามารถนำข้อมูลไปใช้วิเคราะห์เชื่อมโยงความสัมพันธ์ของระบบที่เกี่ยวข้องได้อย่างครบถ้วนถูกต้อง*

(1) กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการคำอธิบายชุดข้อมูล ครอบคลุม บทบาทหน้าที่ของผู้ที่รับผิดชอบ กระบวนการจัดทำคำอธิบายชุดข้อมูล การควบคุมดูแลและสอบทานคำอธิบายชุดข้อมูล

(2) จัดให้มีหน่วยงานหรือผู้รับผิดชอบในการจัดทำ ปรับปรุงแก้ไข และสอบทานคำอธิบายชุดข้อมูลให้เป็นปัจจุบัน

(3) การจัดทำคำอธิบายชุดข้อมูลทั้งในเชิงธุรกิจและเชิงเทคนิคกับทุกชุดข้อมูลสำคัญอย่างครบถ้วน รวมถึงกำหนดให้เป็นส่วนหนึ่งในกระบวนการพัฒนาระบบเทคโนโลยีสารสนเทศ

- คำอธิบายข้อมูลเชิงธุรกิจ (business metadata) ครอบคลุม ชื่อชุดข้อมูล คำอธิบายอย่างย่อ ผู้ทำหน้าที่อนุมัติและควบคุมดูแลข้อมูล วันที่เริ่มต้นใช้งาน วันที่ทำการเปลี่ยนแปลงข้อมูลล่าสุด แหล่งที่มาของข้อมูล
- คำอธิบายข้อมูลเชิงเทคนิค (technical metadata) ครอบคลุม ชื่อตารางข้อมูลในฐานข้อมูล ชื่อฟิลด์ข้อมูลในตารางข้อมูล ประเภทข้อมูล ความกว้างของฟิลด์ข้อมูล คีย์ข้อมูล (primary key หรือ foreign key) รวมถึงการสำรองข้อมูล (backup) และกู้คืนข้อมูล (restore)

(4) กำหนดให้มีกระบวนการควบคุม การเข้าถึง การกำหนดสิทธิ์ การปรับปรุงแก้ไขคำอธิบายชุดข้อมูล เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

(5) มีการปรับปรุงทะเบียนรายการคำอธิบายชุดข้อมูล ให้เป็นปัจจุบันอย่างต่อเนื่อง โดยมีการสอบทานอย่างสม่ำเสมออย่างน้องปีละ 1 ครั้ง

5.2.2 การบริหารจัดการคุณภาพข้อมูล (data quality management)

วัตถุประสงค์ *เพื่อให้ข้อมูลคุณภาพ น่าเชื่อถือ สามารถนำไปใช้ประกอบการวิเคราะห์และตัดสินใจทางธุรกิจได้อย่างถูกต้องเหมาะสม รวมทั้งสร้างความเชื่อมั่นให้กับผู้ใช้บริการ*

(1) กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการคุณภาพข้อมูล ครอบคลุม บทบาทหน้าที่ผู้รับผิดชอบ คุณลักษณะข้อมูลที่มีคุณภาพ กระบวนการบริหารจัดการคุณภาพข้อมูล ได้แก่

- การกำหนดหลักเกณฑ์คุณภาพข้อมูล (data quality requirement)
- การประเมินคุณภาพข้อมูล (data quality assessment)
- การปรับปรุงคุณภาพข้อมูล (resolved data quality issues)
- การควบคุมและติดตามให้ข้อมูลมีคุณภาพ (monitoring and control)

(2) จัดให้มีหน่วยงานหรือผู้รับผิดชอบในการบริหารจัดการคุณภาพข้อมูล

(3) จัดให้มีการกำหนดคุณลักษณะข้อมูลที่มีคุณภาพที่ชัดเจน เช่น ด้านความถูกต้อง (accuracy) ความครบถ้วน (completeness) ความสอดคล้องกัน (consistency) ความเป็นปัจจุบัน (timeliness) ความพร้อมใช้ (availability) ความไม่ซ้ำซ้อน (uniqueness) เป็นต้น

(4) การกำหนดหลักเกณฑ์คุณภาพข้อมูล (data quality requirement) อย่างน้อยครอบคลุม

- กำหนด critical data elements (CDE) ในแต่ละชุดข้อมูล โดยประเมินตามคุณลักษณะข้อมูลที่มีคุณภาพของสถาบันการเงิน
- กำหนดระดับคุณภาพข้อมูล (data quality threshold) ในแต่ละชุดข้อมูล เพื่อใช้ในการประเมินคุณภาพของชุดข้อมูล
- กำหนดให้มีกระบวนการควบคุมการเปลี่ยนแปลงหลักเกณฑ์คุณภาพข้อมูล การกำหนดคุณลักษณะข้อมูลที่มีคุณภาพ การกำหนด CDE และการกำหนดระดับคุณภาพข้อมูล เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

(5) การประเมินคุณภาพข้อมูล (data quality assessment) อย่างน้อยครอบคลุม

- ประเมินคุณภาพข้อมูลตามหลักเกณฑ์คุณภาพข้อมูล โดยจัดทำ data profiling กับชุดข้อมูลที่เป็น CDE และเปรียบเทียบกับระดับคุณภาพข้อมูล
- จัดทำผลการประเมินคุณภาพข้อมูล (data quality scorecard) เพื่อใช้ติดตามคุณภาพข้อมูลอย่างต่อเนื่อง
- ระบุชุดข้อมูลที่ไม่เป็นไปตามระดับคุณภาพข้อมูล รวมทั้งแจ้งผู้ทำหน้าที่อนุมัติและควบคุมดูแลข้อมูล เพื่อหาแนวทางดำเนินการแก้ไขให้ข้อมูลมีคุณภาพต่อไป

(6) การปรับปรุงคุณภาพข้อมูล (resolved data quality issues) อย่างน้อยครอบคลุม

- มีกระบวนการนำชุดข้อมูลที่ไม่ผ่านเกณฑ์การประเมินคุณภาพมาปรับปรุง

- วิเคราะห์หาสาเหตุที่แท้จริง (root cause analysis) เพื่อป้องกันไม่ให้เกิดชุดข้อมูลที่ไม่มีคุณภาพขึ้นอีกในอนาคต
- กำหนดให้มีกระบวนการควบคุมการปรับปรุงคุณภาพข้อมูลที่รัดกุม เช่น กระบวนการบริหารจัดการการเปลี่ยนแปลง กระบวนการขออนุมัติจากผู้ทำหน้าที่อนุมัติและควบคุมดูแลข้อมูล เป็นต้น รวมทั้งจัดเก็บหลักฐานแสดงข้อมูลก่อน หลังการแก้ไขข้อมูล เพื่อป้องกันการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

(7) การควบคุมและติดตามให้ข้อมูลมีคุณภาพ (monitor and control) อย่างน้อยครอบคลุม

- ติดตามและปรับปรุงผลการประเมินคุณภาพข้อมูล อย่างต่อเนื่อง เพื่อให้สามารถติดตามคุณภาพของชุดข้อมูลได้อย่างทันการณ์
- มีกระบวนการหรือเครื่องมือแจ้งเตือนไปยังผู้ทำหน้าที่อนุมัติและควบคุมดูแลข้อมูล เมื่อพบว่าชุดข้อมูลมีคุณภาพต่ำกว่าระดับคุณภาพข้อมูลที่กำหนด
- สอบทานคุณภาพข้อมูลให้เป็นไปตามหลักเกณฑ์ที่กำหนดอย่างสม่ำเสมอ
- จัดทำรายงานผลการติดตามคุณภาพข้อมูล สรุปความคืบหน้าการแก้ไขปรับปรุงชุดข้อมูลที่ไม่ผ่านเกณฑ์การประเมินคุณภาพ รวมทั้ง รายงานประเด็นปัญหาหรือความเสี่ยงที่พบ ภาพรวมปัญหาและสาเหตุที่ทำให้ชุดข้อมูลไม่มีคุณภาพ นำเสนอคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายเป็นประจำ

5.2.3 การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

วัตถุประสงค์ *เพื่อให้มีการรักษาความมั่นคงปลอดภัยของข้อมูล ครอบคลุมการรับส่งข้อมูลผ่านเครือข่ายสื่อสาร การจัดเก็บหรือใช้ข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง ๆ การเก็บรักษาและการทำลายข้อมูล*

(1) การรักษาความมั่นคงปลอดภัยของข้อมูลให้ สง. อ้างอิงประกาศและแนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เรื่อง การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

5.2.4 การรักษาความเป็นส่วนบุคคลของข้อมูล (data privacy)

วัตถุประสงค์ *เพื่อให้สถาบันการเงินมีการรักษาความเป็นส่วนตัวของข้อมูลตามที่กฎหมายกำหนด*

(1) การรักษาความเป็นส่วนบุคคลข้อมูล ให้ สง. ปฏิบัติตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง โดยสถาบันการเงินต้องมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น ภายใต้วัตถุประสงค์ที่กำหนดไว้เมื่อได้รับข้อมูลส่วนบุคคล รวมทั้งมีการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลทั้งข้อมูลส่วนบุคคลที่อยู่ในรูปแบบกระดาษและอิเล็กทรอนิกส์

6. กำหนดการรับฟังความคิดเห็น

ธนาคารแห่งประเทศไทยเปิดรับฟังความคิดเห็นและข้อเสนอแนะต่อแนวปฏิบัติการกำกับดูแลข้อมูล (Data Governance Guideline) ผ่านทางเว็บไซต์ของธนาคารแห่งประเทศไทย (www.bot.or.th) ตั้งแต่ วันที่ 24 กรกฎาคม 2563 จนถึง วันที่ 14 สิงหาคม 2563

ประสานงาน :
ทีมเกณฑ์การกำกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
Email: ITSupervision@bot.or.th

ธนาคารแห่งประเทศไทย