ธนาคารแห่งประเทศไทย

27 กันยายน 2564

เรียน ผู้จัดการ

สถาบันการเงินทุกแห่ง

ที่ ธปท.ฝนส2.ว. 914/2564 เรื่อง นำส่งแนวนโยบายธนาคารแห่งประเทศไทย เรื่อง การกำกับดูแลข้อมูล (Data Governance)

ธนาคารแห่งประเทศไทย (ธปท.) ขอนำส่งแนวนโยบาย เรื่อง การกำกับดูแลข้อมูล (Data Governance) เพื่อให้สถาบันการเงินนำไปใช้อ้างอิงเป็นแนวทางในการกำกับดูแลข้อมูลขององค์กรให้สอดคล้องกับหลักการที่ดีที่ได้รับการยอมรับในระดับสากล โดยมีแนวทางการบริหารจัดการข้อมูลที่เหมาะสม

วัตถุประสงค์ของการออกแนวนโยบายฉบับนี้ เพื่อให้สถาบันการเงินมีการกำกับดูแลข้อมูลที่ครอบคลุมทั้งองค์กร ต่อเนื่อง และเกิดผลเป็นรูปธรรม รวมทั้งเพื่อให้ข้อมูลทั้งหมดขององค์กรมีคุณภาพ มีความมั่นคงปลอดภัย มีความเป็นส่วนบุคคล และเป็นประโยชน์ต่อการดำเนินธุรกิจ บนพื้นฐานของการคุ้มครองข้อมูลและรักษาผลประโยชน์ของลูกค้า โดยมีสาระสำคัญ คือ การกำหนดหลักการในการกำกับดูแลข้อมูล 5 ด้าน อันได้แก่ นโยบายการกำกับดูแลข้อมูล โครงสร้างการกำกับดูแลข้อมูลตามหลัก three lines of defense การบริหารจัดการตลอดวงจรชีวิตของข้อมูล การรักษาความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล และการบริหารจัดการประเด็นปัญหาด้านข้อมูล

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นายรณดล นุ่มนนท์)
รองผู้ว่าการ ด้านเสถียรภาพสถาบันการเงิน
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย แนวนโยบายธนาคารแห่งประเทศไทย เรื่อง การกำกับดูแลข้อมูล (Data Governance)

ฝ่ายนโยบายและกำกับสถาบันการเงิน 2, ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 5806, 0 2283 6559
อีเมล FIOP-RPD2@bot.or.th, ITSupervision@bot.or.th

หมายเหตุ ( ) ธนาคารจะจัดให้มีการประชุมชี้แจงในวันที่.....ณ.....
(X) ไม่มีการจัดประชุมชี้แจง

สนสว90-คส50001-25640927

คส 500	วันที่ 27 ก.ย. 2564

แนวนโยบายธนาคารแห่งประเทศไทย

เรื่อง การกำกับดูแลข้อมูล (Data Governance)

27 กันยายน 2564

ธนาคารแห่งประเทศไทย

จัดทำโดย

ฝ่ายนโยบายและกำกับสถาบันการเงิน 2

สายนโยบายสถาบันการเงิน และ

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน

ธนาคารแห่งประเทศไทย

โทรศัพท์ 0-2283-5806, 0-2283-6559

e-mail: FIOP-RPD2@bot.or.th, ITSupervision@bot.or.th

สนสว90-คส50001-25640927

คส 500	วันที่ 27 ก.ย. 2564

สารบัญ

แนวนโยบายธนาคารแห่งประเทศไทย

เรื่อง การกำกับดูแลข้อมูล (Data Governance)

---

1. เหตุผลในการออกแนวนโยบาย

ข้อมูลเป็นทรัพย์สินที่สำคัญของสถาบันการเงิน การนำเทคโนโลยีมาประยุกต์เพื่อใช้ประโยชน์จากข้อมูล ตั้งแต่ข้อมูลทั่วไปจนถึงข้อมูลทางการเงินของลูกค้าที่มีจำนวนเพิ่มมากขึ้น เป็นกลไกในการขับเคลื่อนการให้บริการทางการเงินในยุคปัจจุบัน โดยสถาบันการเงินนำเอาข้อมูลเหล่านั้นมาพัฒนาผลิตภัณฑ์และการบริการทางการเงินให้ตรงกับความต้องการของลูกค้า รวมทั้งสามารถใช้ประโยชน์จากข้อมูลในการบริหารความเสี่ยงอย่างมีประสิทธิภาพ บนพื้นฐานของการคุ้มครองข้อมูลและรักษาผลประโยชน์ของลูกค้า หากสถาบันการเงินไม่มีการกำกับดูแลและบริหารจัดการข้อมูลได้อย่างเหมาะสมเพียงพอ อาจก่อให้เกิดความเสี่ยงที่มีนัยสำคัญจนกระทบต่อความเชื่อมั่นของระบบสถาบันการเงินได้ ดังนั้น สถาบันการเงินจึงควรจัดให้มีการดูแลคุณภาพข้อมูล การรักษาความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูลอย่างเหมาะสมและสอดคล้องกับขนาด ลักษณะการดำเนินธุรกิจ ความซับซ้อนของธุรกิจ และความเสี่ยงด้านข้อมูลของสถาบันการเงิน รวมทั้งเป็นไปตามกฎเกณฑ์และกฎหมายที่เกี่ยวข้องกับการกำกับดูแลข้อมูลที่ต้องปฏิบัติตาม

ธนาคารแห่งประเทศไทย (ธปท.) สนับสนุนให้สถาบันการเงินนำข้อมูลไปใช้ประโยชน์ได้อย่างเต็มประสิทธิภาพ เพื่อพัฒนาการให้บริการทางการเงินตอบสนองความต้องการของลูกค้าได้ ในขณะเดียวกันสถาบันการเงินควรมีการบริหารจัดการความเสี่ยงจากการใช้ข้อมูลอย่างเหมาะสมควบคู่กันด้วย ดังนั้น ธปท. จึงออกแนวนโยบายเรื่องการกำกับดูแลข้อมูลฉบับนี้ เพื่อให้สถาบันการเงินนำไปใช้อ้างอิงเป็นแนวทางในการกำกับดูแลข้อมูลให้สอดคล้องกับหลักการที่ดีที่ได้รับการยอมรับในระดับสากล โดยมีแนวทางการบริหารจัดการข้อมูลที่เหมาะสม ทั้งนี้ ธปท. คาดหวังว่าสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่งจะสามารถนำแนวนโยบายฉบับนี้ไปใช้ในการกำกับดูแลข้อมูลขององค์กรเพื่อเป็นประโยชน์ต่อการดำเนินธุรกิจของสถาบันการเงิน นอกจากนี้ ผู้ประกอบธุรกิจที่มิใช่สถาบันการเงินสามารถนำแนวนโยบายฉบับนี้ไปประยุกต์ใช้เป็นแนวทางในการกำกับดูแลข้อมูลขององค์กรตนเองได้

2. เนื้อหา

2.1 คำจำกัดความ

ข้อมูล[1] หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ หรืออยู่ในรูปของข้อความ สถิติ หรือรูปแบบอื่นใด ทั้งที่เป็นอิเล็กทรอนิกส์ และไม่ใช่อิเล็กทรอนิกส์ เช่น ข้อมูลลูกค้า ข้อมูลพนักงาน และข้อมูลทางธุรกิจ

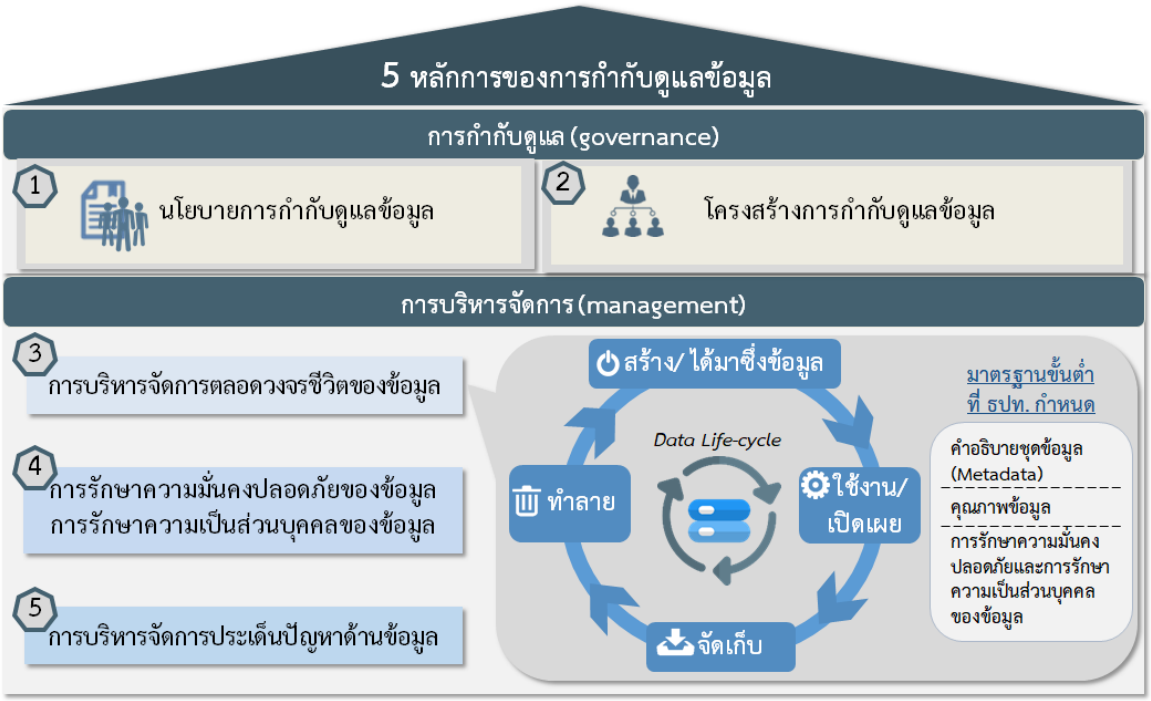
ความเสี่ยงด้านข้อมูล หมายถึง ความเสี่ยงที่อาจเกิดขึ้นจากข้อมูล หรือการใช้ข้อมูล ซึ่งจะมีผลกระทบต่อการดำเนินธุรกิจของสถาบันการเงิน เช่น ข้อมูลรั่วไหลจนนำไปสู่การถูกฟ้องร้องและเสียชื่อเสียง ข้อมูลไม่ตรงตามความต้องการของผู้ใช้งาน ข้อมูลไม่มีคุณภาพหรือมีความเบี่ยงเบน ซึ่งอาจส่งผลให้การตัดสินใจบิดเบือนไปจากความเป็นจริงหรือเกิดความผิดพลาดจนส่งผลให้การดำเนินธุรกิจไม่มีประสิทธิภาพ

2.2 หลักการ

ธปท. กำหนดหลักการเกี่ยวกับการกำกับดูแลและบริหารจัดการข้อมูลของสถาบันการเงิน เพื่อให้มั่นใจว่าข้อมูลในสถาบันการเงินมีคุณภาพ มั่นคงปลอดภัย มีความเป็นส่วนบุคคลและเป็นประโยชน์ต่อการดำเนินธุรกิจของสถาบันการเงิน บนพื้นฐานของการคุ้มครองข้อมูลและรักษาผลประโยชน์ของลูกค้า หลักการนี้กำหนดเป็น principle-based โดยสถาบันการเงินสามารถใช้ดุลพินิจในการดำเนินการให้สอดคล้องกับขนาด ลักษณะการดำเนินธุรกิจ ความซับซ้อนของธุรกิจ และความเสี่ยงด้านข้อมูลของสถาบันการเงิน รวมถึงมีความยืดหยุ่นในการทำงานภายใต้แนวทางดังกล่าว

แนวนโยบายฉบับนี้ ธปท. ได้กำหนดการกำกับดูแลข้อมูลไว้ 5 หลักการ ได้แก่ (1) นโยบายการกำกับดูแลข้อมูล (2) โครงสร้างการกำกับดูแลข้อมูลตามหลัก three lines of defense (3) การบริหารจัดการตลอดวงจรชีวิตข้อมูล (4) การรักษาความมั่นคงปลอดภัยของข้อมูลและการรักษาความเป็นส่วนบุคคลของข้อมูล และ (5) การบริหารจัดการประเด็นปัญหาด้านข้อมูล ทั้งนี้ สถาบันการเงินควรนำไปเป็นแนวทางในการกำกับดูแลข้อมูลในองค์กร โดยหากสถาบันการเงินใดสามารถปฏิบัติได้ตามที่กำหนดไว้ในแนวนโยบายฉบับนี้แล้ว ก็สามารถพิจารณาให้มีการกำกับดูแลข้อมูลเพิ่มเติม รวมทั้งมีการรายงานและวัดผลสำเร็จเพื่อพัฒนาการกำกับดูแลข้อมูลให้ดีอย่างต่อเนื่อง และอาจพิจารณาใช้เทคโนโลยีเพื่อยกระดับการดำเนินการด้านการกำกับดูแลข้อมูลเพิ่มขึ้นตามระดับความพร้อมของสถาบันการเงินเองได้

[1] อ้างอิงหลักการจากนิยาม “ข้อมูล” ตามที่กำหนดในประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ



2.3 การกำกับดูแลข้อมูลของสถาบันการเงิน

สถาบันการเงินควรกำกับดูแลข้อมูลตาม 5 หลักการ ดังนี้

<u>หลักการที่ 1</u> นโยบายการกำกับดูแลข้อมูล

สถาบันการเงินควรกำหนดนโยบายในการกำกับดูแลข้อมูลให้สอดคล้องกับขนาด ลักษณะการดำเนินธุรกิจ ความซับซ้อนของธุรกิจ และความเสี่ยงด้านข้อมูลของสถาบันการเงิน รวมถึงสื่อสารนโยบายดังกล่าวเพื่อสร้างความตระหนักแก่พนักงานในองค์กร รวมทั้งให้พนักงานถือปฏิบัติตาม โดย

(1) นโยบายการกำกับดูแลข้อมูลควรทำเป็นลายลักษณ์อักษรให้ครอบคลุมการดูแลข้อมูลทุกประเภทของสถาบันการเงิน รวมถึงการใช้บริการจากบุคคลภายนอกหรือพันธมิตรทางธุรกิจที่เกี่ยวข้อง[2] โดยอาจเป็นนโยบายที่จัดทำขึ้นเฉพาะหรือเพิ่มเติมจากนโยบายที่สถาบันการเงินมีอยู่แล้วได้ อย่างน้อยควรครอบคลุมในเรื่อง ดังนี้

(1.1) โครงสร้างการกำกับดูแลข้อมูล บทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องให้เป็นไปตามหลัก three lines of defense และมีการแบ่งแยกหน้าที่อย่างชัดเจน รวมถึงบริหารจัดการทรัพยากรให้มีความเพียงพอเหมาะสม ทั้งนี้รายละเอียดตามหลักการที่ 2

[2] อ้างอิงนิยาม “บุคคลภายนอก” จากประกาศธนาคารแห่งประเทศไทย ที่ สนส. 21/2562 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน และที่แก้ไขเพิ่มเติม และ
อ้างอิงนิยาม “พันธมิตรทางธุรกิจ” จากประกาศธนาคารแห่งประเทศไทย ที่ สนส. 16/2563 เรื่อง หลักเกณฑ์การใช้บริการจากพันธมิตรทางธุรกิจ (business partner) ของสถาบันการเงิน และที่แก้ไขเพิ่มเติม

(1.2) การบริหารจัดการตลอดวงจรชีวิตข้อมูล ตั้งแต่การสร้างหรือการได้มาซึ่งข้อมูล การใช้งานหรือการเปิดเผย การจัดเก็บ และการทำลายข้อมูล โดยคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นในแต่ละขั้นตอนของวงจรชีวิต ทั้งนี้รายละเอียดตามหลักการที่ 3

(1.3) การรักษาความมั่นคงปลอดภัยของข้อมูลและการรักษาความเป็นส่วนบุคคลของข้อมูลตลอดวงจรชีวิตข้อมูลให้สอดคล้องกับระดับความเสี่ยงของข้อมูล และเป็นไปตามกฎเกณฑ์และกฎหมายที่เกี่ยวข้อง ทั้งนี้รายละเอียดตามหลักการที่ 4

(1.4) การบริหารจัดการประเด็นปัญหาด้านข้อมูล เพื่อลดผลกระทบของความเสียหายที่เกิดขึ้นแล้ว ทั้งนี้รายละเอียดตามหลักการที่ 5

(2) นโยบายการกำกับดูแลข้อมูลต้องได้รับอนุมัติจากคณะกรรมการที่ได้รับมอบหมายและทบทวนตามความถี่ให้เหมาะสมซึ่งรวมถึงเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(3) มีการชี้แจงและสื่อสารนโยบายให้ผู้ที่เกี่ยวข้องทราบอย่างทั่วถึง โดยประกาศใช้อย่างเป็นทางการ และให้ทุกคนในองค์กรถือปฏิบัติ

<u>หลักการที่ 2</u> โครงสร้างการกำกับดูแลข้อมูลตามหลัก three lines of defense

โครงสร้างการกำกับดูแลข้อมูลควรเป็นไปตามหลัก three lines of defense เพื่อเอื้อต่อการทำหน้าที่ควบคุม กำกับ และตรวจสอบ และมีการแบ่งแยกหน้าที่ (segregation of duty) อย่างชัดเจน รวมถึงบริหารจัดการทรัพยากรให้มีความเพียงพอเหมาะสม โดย

(1) กำหนดบุคลากรและหน่วยงานที่มีบทบาทหน้าที่และความรับผิดชอบเกี่ยวกับการกำกับดูแลข้อมูลโดยตรงและครอบคลุมหน้าที่ดังต่อไปนี้

บทบาทหน้าที่และความรับผิดชอบที่เกี่ยวกับการกำกับดูแลข้อมูล	
1. คณะกรรมการที่ทำหน้าที่กำกับดูแลข้อมูล	Oversight committee
2. ผู้บริหารจัดการข้อมูล 2.1 ระดับผู้บริหารระดับสูง 2.2 ระดับหน่วยงานหรือทีมงาน 3. ผู้อนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวกับข้อมูล 4. ผู้ใช้ข้อมูล	1st Line
5. หน่วยงานบริหารความเสี่ยง 6. หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์และกฎหมาย	2nd Line
7. หน่วยงานตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยงที่เกี่ยวกับข้อมูล	3rd Line

สถาบันการเงินควรระบุบทบาทหน้าที่ของคณะกรรมการ หน่วยงาน หรือพนักงานที่เกี่ยวข้องกับการกำกับดูแลข้อมูลให้ชัดเจนเป็นลายลักษณ์อักษร เพื่อให้ผู้ที่เกี่ยวข้องทราบถึงบทบาทหน้าที่และความรับผิดชอบของตนเอง (รายละเอียดตามเอกสารแนบ 1) อย่างไรก็ตาม สถาบันการเงินสามารถพิจารณาการจัดรูปแบบโครงสร้างการกำกับดูแลด้านข้อมูลให้เหมาะสมกับขนาด ลักษณะการดำเนินธุรกิจ ความซับซ้อนของธุรกิจ และความเสี่ยงด้านข้อมูลของสถาบันการเงินได้ เท่าที่มีบุคลากรและหน่วยงานที่ทำหน้าที่ข้างต้นครบถ้วนและไม่ขัดกับหลักการตรวจสอบและถ่วงดุลที่เหมาะสม เช่น อาจมอบหมายให้คณะกรรมการด้านเทคโนโลยีทำหน้าที่กำกับดูแลข้อมูลเพิ่มเติมได้ โดยที่ไม่ต้องจัดตั้งคณะกรรมการกำกับดูแลข้อมูลขึ้นมาเป็นการเฉพาะ

(2) จัดให้มีทรัพยากรทั้งด้านบุคลากรและเครื่องมือให้เพียงพอที่จะสนับสนุนการปฏิบัติงานที่เกี่ยวข้องกับการกำกับดูแลข้อมูล รวมถึงมีบุคลากรที่มีความรู้ ความเชี่ยวชาญหรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ นอกจากนี้ ควรจัดให้มีการอบรมและพัฒนาความรู้ความเชี่ยวชาญด้านการกำกับดูแลข้อมูลให้แก่บุคลากรที่เกี่ยวข้อง โดยมีการวัดประสิทธิผลของหลักสูตรฝึกอบรมที่จัดขึ้นด้วย

(3) กำหนดแผนงานการเสริมสร้างความตระหนักด้านการกำกับดูแลข้อมูลแก่บุคลากรทุกระดับ รวมถึงบุคคลภายนอกที่เกี่ยวข้องอย่างต่อเนื่อง โดยมีแผนงานที่ชัดเจนต่อเนื่องและวัดผลได้ รวมถึงมีการทบทวนและปรับปรุงเนื้อหาอย่างเหมาะสม

<u>หลักการที่ 3</u> การบริหารจัดการตลอดวงจรชีวิตของข้อมูล

สถาบันการเงินควรบริหารจัดการข้อมูลตลอดวงจรชีวิตของข้อมูล ตั้งแต่การสร้างหรือการได้มาซึ่งข้อมูล การใช้งานหรือการเปิดเผย การจัดเก็บ และการทำลายข้อมูล โดยคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นในแต่ละขั้นตอนของวงจรชีวิตและมีการควบคุมดูแลที่เหมาะสมเพื่อให้มั่นใจว่าข้อมูลในทุกขั้นตอนของวงจรชีวิตมีคุณภาพ มั่นคงปลอดภัย มีความเป็นส่วนบุคคล โดย

(1) ควรจัดทำแผนภาพหรือการบันทึกในรูปแบบอื่นใดที่สามารถแสดงให้เห็นถึงความเชื่อมโยงของข้อมูลทั้งองค์กร ซึ่งครอบคลุมตั้งแต่การสร้างหรือการได้มาซึ่งข้อมูล การรับส่งข้อมูลระหว่างระบบงาน การใช้งานหรือเปิดเผย การจัดเก็บข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง ๆ เพื่อให้สถาบันการเงินสามารถบริหารจัดการข้อมูลตลอดวงจรชีวิตให้สอดคล้องกับความเสี่ยงและความซับซ้อนของข้อมูลภายในองค์กร

(2) มีการบริหารจัดการคำอธิบายชุดข้อมูล เพื่อให้สามารถนำข้อมูลไปใช้วิเคราะห์เชื่อมโยงความสัมพันธ์ของระบบที่เกี่ยวข้องได้อย่างครบถ้วนถูกต้อง (รายละเอียดตามเอกสารแนบ 2)

(3) มีการบริหารจัดการคุณภาพข้อมูล เพื่อให้ข้อมูลมีคุณภาพ น่าเชื่อถือ สามารถนำไปใช้ประกอบการวิเคราะห์และตัดสินใจทางธุรกิจได้อย่างถูกต้องเหมาะสม รวมทั้งสร้างความเชื่อมั่นให้กับผู้ใช้บริการ (รายละเอียดตามเอกสารแนบ 3)

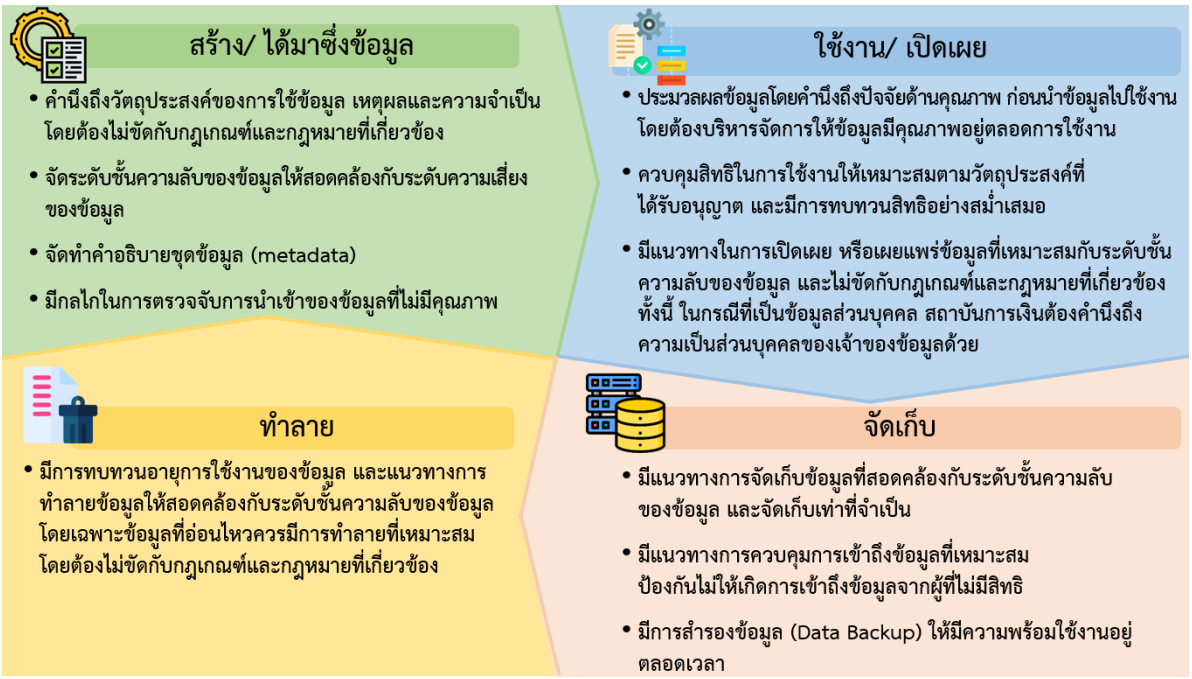
ตัวอย่างของข้อมูลที่ขาดคุณภาพและผลกระทบต่อสถาบันการเงิน

- ❖ ข้อมูลขาดความเป็นปัจจุบัน ส่งผลต่อการวิเคราะห์ที่ไม่ถูกต้อง
- ❖ ข้อมูลขาดความพร้อมใช้งาน ส่งผลให้การดำเนินธุรกิจหยุดชะงัก

(4) ติดตามและบริหารจัดการความเสี่ยงด้านข้อมูลตลอดวงจรชีวิตให้เหมาะสมและเป็นไปตามแนวทางการบริหารจัดการความเสี่ยงของสถาบันการเงิน เพื่อหลีกเลี่ยงโอกาสเกิดความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงานของสถาบันการเงิน

นอกจากนี้ เพื่อให้การบริหารจัดการตลอดวงจรชีวิตข้อมูลมีประสิทธิภาพ สถาบันการเงินควรกำหนดกระบวนการบริหารจัดการในแต่ละขั้นตอนของวงจรชีวิตข้อมูลให้ชัดเจน เพื่อให้ผู้ที่เกี่ยวข้องสามารถนำไปถือปฏิบัติตามได้ โดยมีตัวอย่างประเด็นที่ควรคำนึงถึงในการกำหนดกระบวนการบริหารจัดการในแต่ละขั้นตอนของวงจรชีวิตข้อมูล ดังนี้

ประเด็นที่ควรคำนึงถึงในแต่ละขั้นตอนของวงจรชีวิตข้อมูล



<u>หลักการที่ 4</u> การรักษาความมั่นคงปลอดภัยของข้อมูลและการรักษาความเป็นส่วนบุคคลของข้อมูล

สถาบันการเงินควรรักษาความมั่นคงปลอดภัยของข้อมูลและการรักษาความเป็นส่วนบุคคลของข้อมูลตลอดวงจรชีวิตให้สอดคล้องกับระดับความเสี่ยงของข้อมูล ให้เป็นไปตามกฎเกณฑ์และกฎหมายที่เกี่ยวข้อง โดย

(1) มีการรักษาความมั่นคงปลอดภัยของข้อมูลที่ครอบคลุมการรับส่งข้อมูลผ่านเครือข่ายการสื่อสาร การจัดเก็บหรือใช้ข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง ๆ การเก็บรักษาและการทำลายข้อมูล รวมถึงกรณีที่สถาบันการเงินมีการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ให้สอดคล้องกับระดับความเสี่ยงของข้อมูล ทั้งนี้ สถาบันการเงินสามารถอ้างอิงแนวทางการรักษาความมั่นคงปลอดภัยจากประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน[3] รวมถึงแนวปฏิบัติอื่นที่เกี่ยวข้อง

(2) มีการรักษาความเป็นส่วนบุคคลของข้อมูล ให้สอดคล้องกับกฎเกณฑ์และกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยต้องมีการเก็บรวบรวมใช้งาน หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น ภายใต้วัตถุประสงค์ที่กำหนดไว้ และคำนึงถึงสิทธิของเจ้าของข้อมูล

(3) มีการดูแลข้อมูลของลูกค้าให้เป็นไปตามมาตรฐานขั้นต่ำสำหรับการดูแลข้อมูลของลูกค้าตามที่ธนาคารแห่งประเทศไทยกำหนดในประกาศธนาคารแห่งประเทศไทยว่าด้วยการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market conduct)[4]

<u>หลักการที่ 5</u> การบริหารจัดการประเด็นปัญหาด้านข้อมูล

สถาบันการเงินควรเตรียมความพร้อมในการบริหารจัดการประเด็นปัญหาด้านข้อมูลเพื่อป้องกันไม่ให้เกิดเหตุการณ์ที่อาจนำไปสู่ความเสียหาย หรือเพื่อลดผลกระทบกรณีมีความเสียหายเกิดขึ้นแล้ว

(1) มีกระบวนการติดตามและบริหารจัดการประเด็นปัญหาด้านข้อมูล ทั้งการตรวจจับ การระบุ การยับยั้งปัญหา การวิเคราะห์หาสาเหตุ การรวบรวมหลักฐานหรือเอกสาร การแก้ไขปัญหาการบริหารจัดการให้สามารถกลับมาดำเนินธุรกิจได้ตามปกติ รวมถึงการปรับปรุงกระบวนการควบคุมเพื่อลดโอกาสที่จะเกิดปัญหาที่คล้ายกันในอนาคต ในกรณีที่ประเด็นปัญหาที่เกิดขึ้นส่งผลกระทบต่อ

[3] ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 21/2562 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน และที่แก้ไขเพิ่มเติม

[4] ประกาศธนาคารแห่งประเทศไทย ที่ สกส2. 4/2563 เรื่อง การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market conduct) และที่แก้ไขเพิ่มเติม

ความต่อเนื่องในการดำเนินธุรกิจ สถาบันการเงินสามารถปฏิบัติตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) ของสถาบันการเงิน

(2) มีการเตรียมความพร้อมรองรับกรณีเกิดเหตุการละเมิดข้อมูล เช่น ข้อมูลรั่วไหล โดยเฉพาะกรณีที่เป็นข้อมูลส่วนบุคคล สถาบันการเงินต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลตามที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งรวมถึงกรณีที่การละเมิดดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า

เอกสารแนบ 1

บทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลข้อมูลตามหลัก three lines of defense

1. คณะกรรมการที่ทำหน้าที่กำกับดูแลข้อมูล[5] มีหน้าที่

- กำหนดเป้าหมายในการกำกับดูแลข้อมูลให้สอดรับกับแผนกลยุทธ์ของสถาบันการเงิน
- ดูแลให้มีการจัดทำ ทบทวน และปรับปรุงนโยบาย การกำกับดูแลข้อมูล
- กำกับดูแลและติดตามการดำเนินงานที่เกี่ยวข้องกับข้อมูล รวมถึงให้คำปรึกษาและตัดสินประเด็นสำคัญที่เกี่ยวข้องกับข้อมูล
- สนับสนุน ส่งเสริม และผลักดันการกำกับดูแลข้อมูล อย่างทั่วถึงและต่อเนื่อง
- ดูแลและสนับสนุนให้มีการสื่อสารกับบุคลากรในองค์กรให้ตระหนักถึงความสำคัญของข้อมูล การใช้ข้อมูลอย่างปลอดภัย เพื่อให้เกิดการกำกับดูแลข้อมูลที่ดีภายในสถาบันการเงิน

2. ผู้บริหารจัดการข้อมูล ทั้งระดับผู้บริหารระดับสูง และระดับหน่วยงานหรือทีมงาน

2.1 ระดับผู้บริหารระดับสูง มีหน้าที่

- บริหารจัดการข้อมูล ให้เป็นไปตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล
- ส่งเสริมการให้ความรู้ และสร้างความตระหนักแก่บุคลากรทั่วทั้งองค์กร

2.2 ระดับหน่วยงานหรือทีมงาน มีหน้าที่

- จัดทำ ทบทวน ปรับปรุงนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูลให้เป็นปัจจุบัน
- สื่อสาร ให้ความรู้ และให้คำแนะนำเกี่ยวกับนโยบาย มาตรฐานและระเบียบวิธีปฏิบัติเกี่ยวข้องกับการกำกับดูแลข้อมูล รวมทั้ง การสร้างความตระหนักถึงความสำคัญของข้อมูล การใช้ข้อมูลอย่างปลอดภัย เพื่อให้เกิดการกำกับดูแลข้อมูลที่ดีภายในองค์กร
- ติดตามสถานะของการบริหารจัดการข้อมูล รายงาน ผลและประเด็นปัญหาหรือความเสี่ยงที่พบต่อคณะกรรมการที่ทำหน้าที่กำกับดูแลข้อมูลเป็นประจำ

3. ผู้อนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวกับข้อมูล มีหน้าที่

- อนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น อนุญาตการเข้าถึงข้อมูล การใช้และเผยแพร่ข้อมูล

[5] คณะกรรมการที่ทำหน้าที่กำกับดูแลข้อมูล สามารถประกอบด้วยผู้บริหารที่เกี่ยวข้อง เช่น ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer) ผู้บริหารระดับสูงด้านบริหารจัดการข้อมูล (Chief Data Officer) ผู้บริหารระดับสูงด้านการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Chief Information Security Officer) ผู้บริหารระดับสูงด้านความเสี่ยง (Chief Risk Officer) หรือผู้บริหารจากส่วนงานอื่นที่เกี่ยวข้อง

- ควบคุมดูแลข้อมูลให้มั่นใจว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐานและระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล เช่น ดูแลให้จัดทำทะเบียนข้อมูลและทบทวนให้เป็นปัจจุบัน ดูแลให้มีการกำหนดชั้นความลับข้อมูลและกำหนดเกณฑ์คุณภาพข้อมูล

4. ผู้ใช้ข้อมูล มีหน้าที่

- ปฏิบัติตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล
- สนับสนุนการกำกับดูแลข้อมูลให้ตรงความต้องการในการใช้ข้อมูล และรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูลไปยังหน่วยงานหรือทีมงานที่ทำหน้าที่บริหารจัดการข้อมูล

5. หน่วยงานบริหารความเสี่ยง มีหน้าที่

- จัดทำกรอบและกระบวนการบริหารความเสี่ยงของสถาบันการเงินให้ครอบคลุมความเสี่ยงด้านข้อมูล รวมทั้งสนับสนุนให้หน่วยงานต่าง ๆ มีการประเมินความเสี่ยงด้านข้อมูล
- ให้คำปรึกษา ติดตาม และทบทวนความเสี่ยงด้านข้อมูลให้อยู่ในระดับที่ยอมรับได้ รวมทั้งรวบรวมและเชื่อมโยงความเสี่ยงด้านข้อมูลกับความเสี่ยงด้านอื่นของสถาบันการเงิน และนำเสนอผลการบริหารจัดการความเสี่ยงต่อคณะกรรมการที่เกี่ยวข้อง

6. หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์และกฎหมาย มีหน้าที่

- ติดตาม ให้คำปรึกษา และกำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับข้อมูล เพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎเกณฑ์และกฎหมายที่เกี่ยวข้องกับข้อมูลของหน่วยงานกำกับดูแล

7. หน่วยงานตรวจสอบ มีหน้าที่

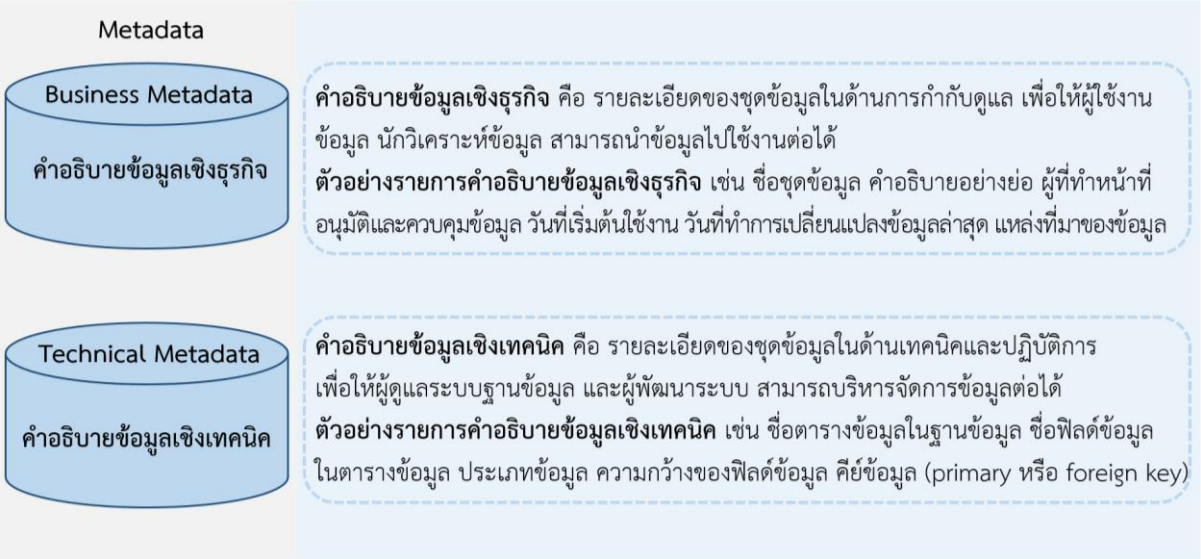
- ตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูล เพื่อสอบทานให้มั่นใจว่าเป็นไปตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล

เอกสารแนบ 2

การบริหารจัดการคำอธิบายชุดข้อมูล (Metadata Management)

1. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการคำอธิบายชุดข้อมูลให้ครอบคลุมบทบาทหน้าที่ของผู้ที่รับผิดชอบ กระบวนการจัดทำคำอธิบายชุดข้อมูล การควบคุมดูแล และสอบทานคำอธิบายชุดข้อมูล
2. จัดให้มีหน่วยงานหรือผู้รับผิดชอบในการจัดทำ ปรับปรุงแก้ไข และสอบทานคำอธิบายชุดข้อมูล รวมถึงปรับปรุงทะเบียนรายการคำอธิบายชุดข้อมูลให้เป็นปัจจุบัน
3. จัดทำคำอธิบายชุดข้อมูลทั้งในเชิงธุรกิจและเชิงเทคนิคกับทุกชุดข้อมูลสำคัญอย่างครบถ้วน รวมถึงกำหนดให้เป็นส่วนหนึ่งในกระบวนการพัฒนาระบบเทคโนโลยีสารสนเทศ

คำอธิบายชุดข้อมูล (Metadata) ประกอบด้วย



4. กำหนดให้มีกระบวนการควบคุมการเข้าถึง การกำหนดสิทธิ การปรับปรุงแก้ไขคำอธิบายชุดข้อมูล เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน
5. มีการปรับปรุงทะเบียนรายการคำอธิบายชุดข้อมูลให้เป็นปัจจุบัน

เอกสารแนบ 3

การบริหารจัดการคุณภาพข้อมูล

สถาบันการเงินควรมีการบริหารจัดการคุณภาพข้อมูล โดยกำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการคุณภาพข้อมูล จัดให้มีหน่วยงานหรือผู้รับผิดชอบในการบริหารจัดการคุณภาพข้อมูล และจัดให้มีการกำหนดคุณลักษณะข้อมูลที่มีคุณภาพที่ชัดเจน รวมทั้งมีกระบวนการบริหารจัดการคุณภาพข้อมูล ตามแนวทางดังนี้

1. <u>การกำหนดหลักเกณฑ์คุณภาพข้อมูล</u>

- มีการกำหนดข้อมูลหลักที่จำเป็นต้องมีคุณภาพ (critical data element) ในแต่ละชุดข้อมูล
- มีการกำหนดระดับคุณภาพข้อมูล ในแต่ละชุดข้อมูล เพื่อใช้ในการประเมินคุณภาพของชุดข้อมูล
- มีการกำหนดให้มีกระบวนการควบคุมการเปลี่ยนแปลงหลักเกณฑ์คุณภาพข้อมูล กำหนดคุณลักษณะข้อมูลที่มีคุณภาพ เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

ตัวอย่างลักษณะข้อมูลที่มีคุณภาพ

ตัวอย่างคำอธิบายตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ

2. <u>การประเมินคุณภาพข้อมูล</u>

- มีการประเมินคุณภาพข้อมูลตามหลักเกณฑ์คุณภาพข้อมูล เช่น การตรวจสอบและวิเคราะห์คุณภาพข้อมูลในเชิงเทคนิค (data profiling) กับข้อมูลหลักที่จำเป็นต้องมีคุณภาพในแต่ละชุดข้อมูล รวมถึงการเปรียบเทียบกับระดับคุณภาพข้อมูลที่สถาบันการเงินกำหนด
- มีการจัดทำผลการประเมินคุณภาพข้อมูล เพื่อใช้ติดตามคุณภาพข้อมูลอย่างต่อเนื่อง
- มีการระบุชุดข้อมูลที่ไม่เป็นไปตามระดับคุณภาพข้อมูล รวมทั้งแจ้งผู้ทำหน้าที่อนุมัติและควบคุมดูแลข้อมูล เพื่อหาแนวทางดำเนินการแก้ไขให้ข้อมูลมีคุณภาพต่อไป

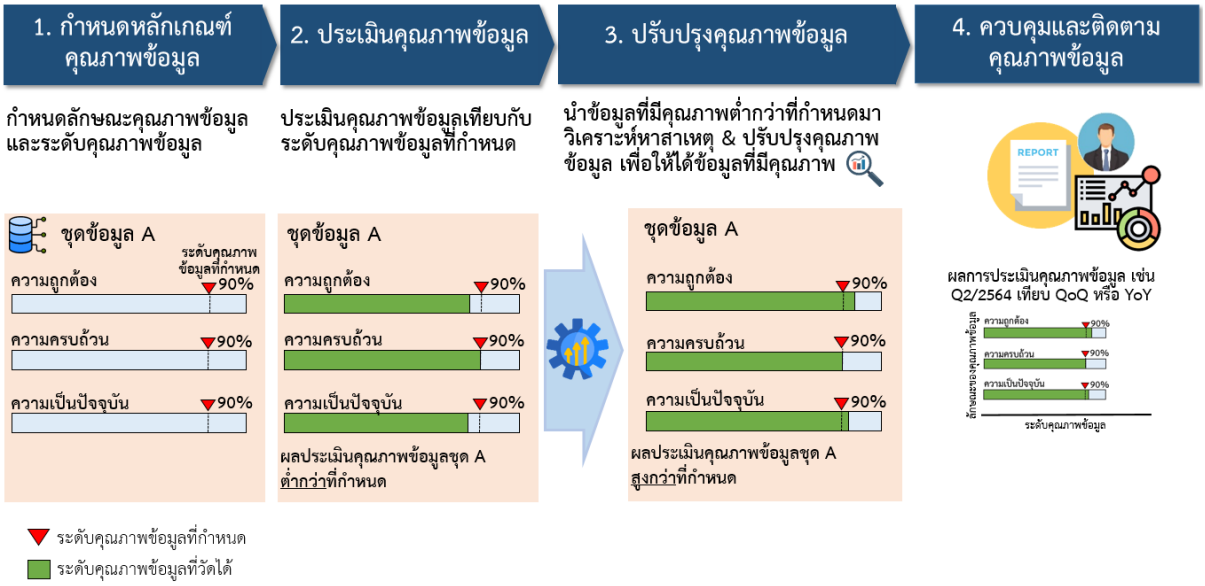
3. <u>การปรับปรุงคุณภาพข้อมูล</u>

- มีกระบวนการนำชุดข้อมูลที่ไม่ผ่านเกณฑ์การประเมินคุณภาพมาปรับปรุง
- มีการวิเคราะห์หาสาเหตุที่แท้จริง เพื่อป้องกันไม่ให้เกิดชุดข้อมูลที่ไม่มีคุณภาพขึ้นอีกในอนาคต
- มีการกำหนดให้มีกระบวนการควบคุมการปรับปรุงคุณภาพข้อมูลที่รัดกุม เช่น กระบวนการบริหารจัดการการเปลี่ยนแปลง กระบวนการขออนุมัติจากผู้ทำหน้าที่อนุมัติ และควบคุมดูแลข้อมูล รวมทั้งจัดเก็บหลักฐานแสดงข้อมูลก่อนและหลังการแก้ไขข้อมูล เพื่อป้องกันการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

4. <u>การควบคุมและติดตามให้ข้อมูลมีคุณภาพ</u>

- มีการติดตามและปรับปรุงผลการประเมินคุณภาพข้อมูลอย่างต่อเนื่อง เพื่อให้สามารถติดตามคุณภาพของชุดข้อมูลได้อย่างทันกาล
- มีกระบวนการหรือเครื่องมือในการติดตามระดับคุณภาพข้อมูล เมื่อพบว่าชุดข้อมูลมีคุณภาพต่ำกว่าระดับคุณภาพข้อมูลที่กำหนด
- มีการสอบทานคุณภาพข้อมูลให้เป็นไปตามหลักเกณฑ์ที่กำหนดอย่างสม่ำเสมอ
- มีการจัดทำรายงานผลการติดตามคุณภาพข้อมูล สรุปความคืบหน้าการแก้ไขปรับปรุงชุดข้อมูลที่ไม่ผ่านเกณฑ์การประเมินคุณภาพ รวมทั้ง รายงานประเด็นปัญหาหรือความเสี่ยงที่พบ ภาพรวมปัญหาและสาเหตุที่ทำให้ชุดข้อมูลไม่มีคุณภาพ นำเสนอคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายเป็นประจำ

ตัวอย่างกระบวนการบริหารจัดการคุณภาพข้อมูล



คำถาม-คำตอบท้ายแนวนโยบายธนาคารแห่งประเทศไทย

เรื่อง การกำกับดูแลข้อมูล (Data Governance)

ลงวันที่ 27 กันยายน 2564

ข้อ	คำถาม	คำตอบ
ขอบเขตการบังคับใช้		
1	แนวนโยบายเรื่องกำกับดูแลข้อมูลของสถาบันการเงินต้องครอบคลุมข้อมูลของบริษัทในกลุ่มธุรกิจทางการเงินและบริษัทที่เกี่ยวข้องกับสถาบันการเงินด้วยหรือไม่	แนวนโยบายฉบับนี้มุ่งเน้นให้สถาบันการเงินนำไปใช้เป็นแนวทางในการกำกับดูแลข้อมูลทุกประเภทของสถาบันการเงิน ดังนั้น หากข้อมูลใดมีความเกี่ยวข้องกับสถาบันการเงิน ก็ควรได้รับการดูแลภายใต้นโยบายการกำกับดูแลข้อมูลนี้ด้วย อย่างไรก็ดี แนวนโยบายฉบับนี้เปิดกว้างให้ผู้ประกอบธุรกิจที่มิใช่สถาบันการเงินสามารถนำไปประยุกต์ใช้เป็นแนวทางในการกำกับดูแลข้อมูลขององค์กรตนเองได้
หลักการที่ 1 นโยบายการกำกับดูแลข้อมูล		
2	สาขาของธนาคารพาณิชย์ต่างประเทศสามารถนำนโยบายการกำกับดูแลข้อมูลของธนาคารพาณิชย์แม่ที่ต่างประเทศ มาใช้โดยไม่ต้องจัดทำนโยบายการกำกับดูแลข้อมูลขึ้นมาใหม่ได้หรือไม่	สามารถทำได้ หากนโยบายการกำกับดูแลข้อมูลดังกล่าวมีเนื้อหาสอดคล้องและครอบคลุมหลักการตามที่ธนาคารแห่งประเทศไทยกำหนด โดยนำมาปรับใช้ให้เหมาะสมและสอดคล้องกับความเสี่ยงของสาขาของธนาคารพาณิชย์ต่างประเทศ
หลักการที่ 2 โครงสร้างการกำกับดูแลข้อมูลตามหลัก three lines of defense		
3	สาขาของธนาคารพาณิชย์ต่างประเทศสามารถใช้โครงสร้างการกำกับดูแลข้อมูลของธนาคารพาณิชย์แม่ที่ต่างประเทศ ได้หรือไม่	สามารถทำได้ หากธนาคารพาณิชย์แม่ที่ต่างประเทศมีบุคลากรและหน่วยงานที่ทำหน้าที่ครบถ้วนตามที่กำหนดในเอกสารแนบ 1 และไม่ขัดกับหลักการการตรวจสอบและถ่วงดุลที่เหมาะสม