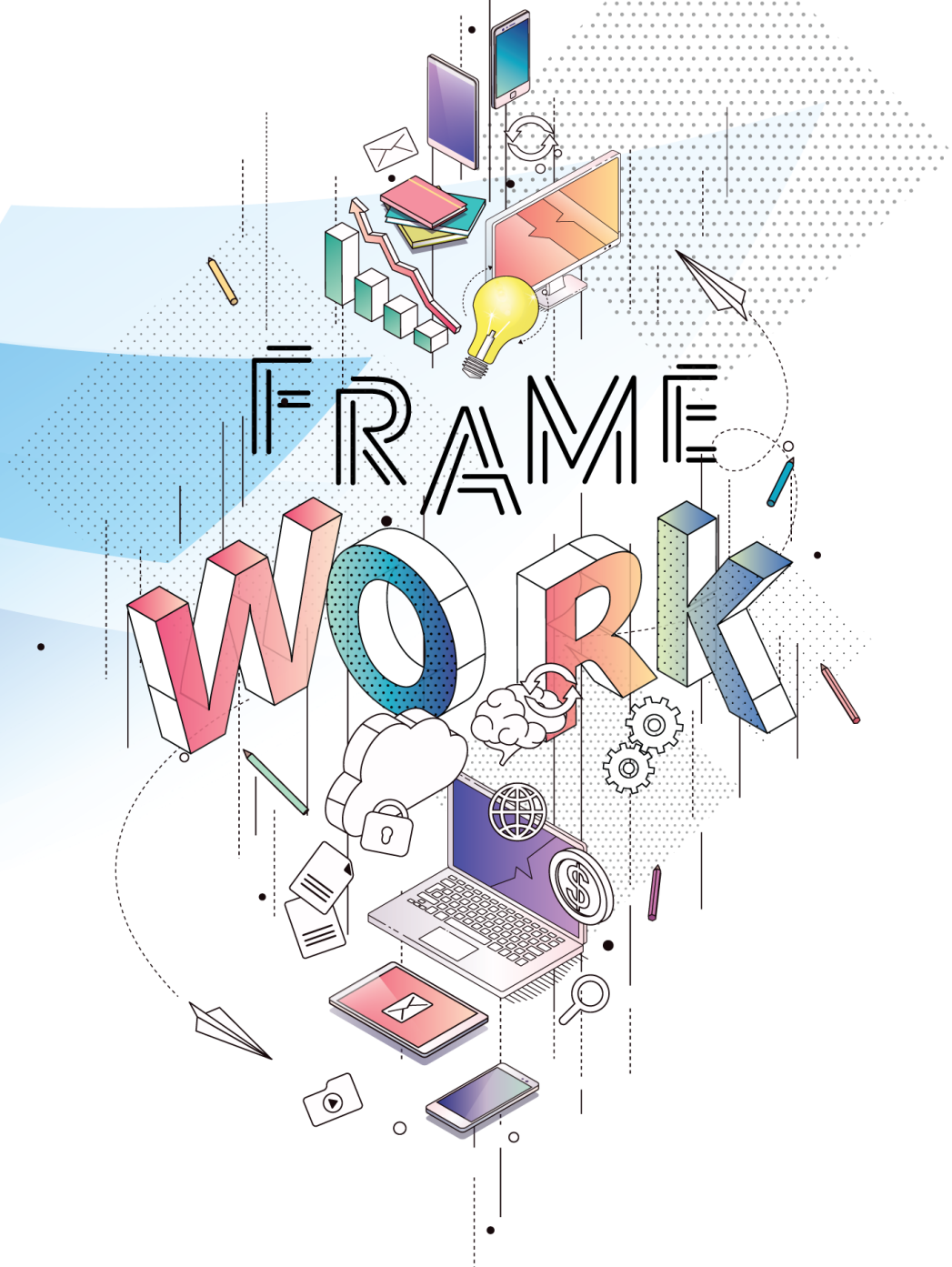
การกำกับดูแลข้อมูล

DATA GOVERNANCE FRAMEWORK



หน้าว่าง

Data Governance Framework

กรอบการกำกับดูแลข้อมูล

เวอร์ชัน ๑.๐

๑๕ มิถุนายน ๒๕๖๑

คณะกรรมการศึกษากระบวนการธรรมาภิบาลและการเปิดเผยข้อมูลดิจิทัล เพื่อการบริหารราชการแผ่นดิน

ประธานกรรมการ

รองศาสตราจารย์วรากรณ์ สามโกเศศ

รองประธานกรรมการ

นายวรรณวิทย์ อาขุบุตร

คณะกรรมการ

นายสมเกียรติ ตั้งกิจวานิชย์

นางสาวกษิติธร ภูภราดัย

ผู้ช่วยศาสตราจารย์โษฑศ์รัตต ธรรมบุษดี

ผู้อำนวยการสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ผู้อำนวยการสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ

ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้จัดการใหญ่บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด

ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ผู้อำนวยการสำนักบริหารการทะเบียน กรมการปกครอง

ผู้แทนสำนักงานสภาความมั่นคงแห่งชาติ

ผู้แทนสำนักงานคณะกรรมการกฤษฎีกา

เลขานุการคณะกรรมการ

ผู้ช่วยผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล (นายวิบูลย์ ภัทรพิบูล)

ผู้อำนวยการฝ่ายนวัตกรรม

สารบัญ

สารบัญตาราง

สารบัญภาพ

บทสรุปผู้บริหาร (EXECUTIVE SUMMARY)

ข้อมูลจัดเป็นสินทรัพย์ที่สำคัญในการดำเนินงานของหน่วยงาน ภาครัฐจึงได้ให้ความสำคัญกับการนำข้อมูลมาใช้สนับสนุนการขับเคลื่อนนโยบายเศรษฐกิจและสังคมดิจิทัลให้กับทุกภาคส่วน แต่ในปัจจุบันหน่วยงานภาครัฐยังประสบกับปัญหาและอุปสรรคในการดำเนินงานในด้านต่าง ๆ ที่เกี่ยวข้องกับข้อมูล ซึ่งเป็นประเด็นปัญหาเชิงนโยบายและปฏิบัติ ทั้งในเรื่อง ความซ้ำซ้อนของข้อมูล ความมั่นคงปลอดภัยของข้อมูล (เช่น การรักษาความลับ การเข้าถึงข้อมูล การรักษาความเป็นส่วนบุคคล) คุณภาพของข้อมูล (เช่น ความถูกต้อง ความครบถ้วน ความเป็นปัจจุบัน) การเปิดเผยข้อมูล (เช่น หน่วยงานเจ้าของข้อมูลไม่อนุญาตให้เข้าถึงข้อมูล กระบวนการขอใช้ข้อมูลซับซ้อนและใช้เวลานาน ข้อมูลไม่อยู่ในรูปแบบที่ใช้งานต่อได้ง่าย) และยังไม่มีการนำข้อมูลไปใช้ประโยชน์อย่างเป็นรูปธรรม ประเด็นปัญหาและอุปสรรคเหล่านี้อาจเป็นผลมาจากการบริหารจัดการข้อมูลที่ไม่ครอบคลุมและไม่ชัดเจนของหน่วยงาน ดังนั้นจึงจำเป็นต้องให้หน่วยงานมีมาตรการและแนวปฏิบัติในการบริหารจัดการและกำกับดูแลข้อมูลที่มีประสิทธิภาพและประสิทธิผล

จากการศึกษาเกี่ยวกับการบริหารจัดการและกำกับดูแลข้อมูล (Data Governance) พบว่าการกำกับดูแลข้อมูลถือเป็นหัวใจสำคัญในการบริหารจัดการข้อมูล (Data Management) กล่าวคือ การกำกับดูแลข้อมูลเป็นกลไกในการกำหนดทิศทาง ควบคุม และทวนสอบการบริหารจัดการข้อมูล เพื่อให้หน่วยงานได้ดำเนินการบริหารจัดการข้อมูลตามนโยบาย กฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ การกำกับดูแลข้อมูลที่ดีก่อให้เกิดการบริหารจัดการข้อมูลที่ดี ส่งผลให้ข้อมูลมีความมั่นคงปลอดภัย มีคุณภาพ มีคุณค่าทางเศรษฐกิจและสังคม และมีความคุ้มทุนต่อการดำเนินงาน

เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัยได้จริง กรอบการกำกับดูแลข้อมูล (Data Governance Framework) ในเอกสารฉบับนี้จึงถูกจัดทำขึ้น เพื่อกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูล โดยประกอบด้วย สภาพแวดล้อมของการกำกับดูแลข้อมูล กฎเกณฑ์หรือนโยบายที่เกี่ยวข้องกับการดำเนินงานกับข้อมูล บทบาทและความรับผิดชอบในการกำกับดูแลข้อมูล กระบวนการกำกับดูแลข้อมูล และการวัดการดำเนินการและความสำเร็จของการกำกับดูแล กล่าวคือ บุคคลที่ได้รับบทบาทในการกำกับดูแลจะมีหน้าที่ในการกำหนดขอบเขต กฎเกณฑ์ และนโยบายข้อมูลที่ใช้ในกระบวนการกำกับดูแล เพื่อควบคุมและตรวจสอบการดำเนินงานที่เกี่ยวข้องกับข้อมูล ตั้งแต่การสร้าง การจัดเก็บ การประมวลผล การใช้ การเผยแพร่ จนถึงการทำลาย โดยกฎเกณฑ์และนโยบายข้อมูลต้องสอดคล้องกับสภาพแวดล้อมและวัฒนธรรมองค์กรของแต่ละหน่วยงาน การวัดผลการดำเนินการช่วยให้เห็นระดับการดำเนินการของการกำกับดูแลข้อมูล ซึ่งส่งผลต่อความสำเร็จของการดำเนินการหรือคุณภาพของข้อมูล

กรอบการกำกับดูแลข้อมูลจะเป็นแนวทางให้หน่วยงานภาครัฐ ทั้งส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานของรัฐรูปแบบใหม่ นำไปปรับใช้ให้เข้ากับลักษณะเฉพาะของแต่ละหน่วยงานเพื่อให้สามารถปรับตัวตามบริบทที่เปลี่ยนแปลงอย่างต่อเนื่อง

บทที่ ๑ บทนำ (INTRODUCTION)

๑.๑ ความเป็นมา

ข้อมูลจัดเป็นหนึ่งในสินทรัพย์ที่สำคัญ และเป็นกลไกในการขับเคลื่อนการดำเนินงานของหน่วยงาน เพื่อนำไปสู่เป้าหมายที่ได้กำหนดไว้ อย่างไรก็ตามสถานการณ์ด้านการบริหารจัดการข้อมูลและการใช้ประโยชน์จากข้อมูลของหน่วยงานภาครัฐในปัจจุบันนั้นยังมีอุปสรรคในด้านต่าง ๆ ทั้งในด้านการจัดเก็บข้อมูล (เช่น ข้อมูลเดียวกันแต่จัดเก็บกระจายไปในหลายระบบ หลายส่วนงาน หลายรูปแบบ) ด้านการเปิดเผยข้อมูล (เช่น หน่วยงานเจ้าของข้อมูลไม่อนุญาตให้เข้าถึงข้อมูล กระบวนการขอใช้ข้อมูลซับซ้อนและใช้เวลานาน ข้อมูลไม่อยู่ในรูปแบบที่ใช้งานต่อได้ง่าย) ด้านความมั่นคงปลอดภัยของข้อมูล (เช่น การรักษาความลับ การเข้าถึง ความเป็นส่วนบุคคล) และด้านคุณภาพของข้อมูล (เช่น ความถูกต้อง ความสมบูรณ์ ความต้องกัน ความเป็นปัจจุบัน ตรงตามความต้องการใช้งาน ความพร้อมใช้)

สาเหตุของปัญหานั้นมาจากการขาดการวางแผนในการบริหารจัดการข้อมูลทั้งวงจรชีวิตของข้อมูล (สร้าง จัดเก็บ ประมวลผล นำไปใช้ เปิดเผย และทำลาย) ขาดการบูรณาการข้อมูล อุปสรรคทางด้านกฎระเบียบ รวมถึงการบริหารจัดการที่ไม่ครอบคลุมประเภทของข้อมูล นั่นคือ ข้อมูลที่มีโครงสร้าง (เช่น ฐานข้อมูล) กึ่งโครงสร้าง (เช่น Extensible Markup Language - XML) ไม่มีโครงสร้าง (เช่น เสียง ภาพ ภาพเคลื่อนไหว)

ดังนั้นเพื่อให้การนำข้อมูลไปใช้ก่อให้เกิดประโยชน์อย่างเต็มที่และมีประสิทธิภาพ จะต้องอาศัยกรอบการกำกับดูแลข้อมูล (Data Governance Framework) ที่เอื้อให้หน่วยงานภาครัฐต่าง ๆ สามารถนำไปใช้กำกับดูแล และบริหารจัดการข้อมูลของหน่วยงานภาครัฐทุกขั้นตอนอย่างเป็นระบบและมีความชัดเจนมากยิ่งขึ้น

๑.๒ วัตถุประสงค์

การจัดทำกรอบการกำกับดูแลข้อมูล เพื่อให้หน่วยงานภาครัฐสามารถนำไปผลักดัน และดำเนินการในการกำกับดูแลข้อมูล รวมถึงติดตามการบริหารจัดการข้อมูลให้มีความโปร่งใส ตรวจสอบได้ ส่งผลต่อคุณภาพ ความมั่นคงปลอดภัย และบูรณาการข้อมูลได้อย่างครบถ้วน ถูกต้อง และข้อมูลเป็นปัจจุบัน

๑.๓ หน่วยงานภาครัฐที่นำไปใช้

กรอบการกำกับดูแลข้อมูลนี้ครอบคลุมถึงการกำกับดูแลและการบริหารจัดการข้อมูลภายในหน่วยงานภาครัฐทั้ง ๔ ประเภท คือ ส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานของรัฐรูปแบบใหม่ ดังนี้

๑) ส่วนราชการ หมายถึง หน่วยงานที่รับผิดชอบการให้บริการสาธารณะทางปกครอง ซึ่งเป็นภารกิจหลักของรัฐ ให้บริการเป็นการทั่วไปและไม่มุ่งกำไร และมีความสัมพันธ์กับรัฐ

๒) รัฐวิสาหกิจ หมายถึง หน่วยงานที่รับผิดชอบบริการสาธารณะทางอุตสาหกรรมและพาณิชยกรรม มีวัตถุประสงค์เพื่อการแสวงหารายได้ ต้องสามารถเลี้ยงตัวเองจากการดำเนินงานเชิงพาณิชย์ แต่สามารถรับเงินงบประมาณสนับสนุนเป็นครั้งคราวหรือบางส่วนในบางกรณี

๓) องค์การมหาชน หมายถึง หน่วยงานที่รับผิดชอบบริการสาธารณะทางสังคมและวัฒนธรรม ไม่มีวัตถุประสงค์ในการแสวงหากำไร เป็นนิติบุคคลและมีความสัมพันธ์กับรัฐ ซึ่งประกอบด้วย รัฐจัดตั้ง ได้รับเงินอุดหนุนจากรัฐ หรือสามารถเลี้ยงตัวเองได้ และรัฐมีอำนาจบริหารจัดการ

๔) หน่วยงานของรัฐรูปแบบใหม่ หมายถึง

- องค์การของรัฐที่เป็นอิสระ (Independent Administrative Organization) ซึ่งเป็นหน่วยงานรูปแบบใหม่ที่จัดตั้งขึ้น เพื่อทำหน้าที่ในการควบคุมกำกับดูแลกิจกรรมของรัฐ ตามนโยบายสำคัญที่ต้องการความเป็นกลางอย่างเคร่งครัด
- กองทุนที่เป็นนิติบุคคล ซึ่งเป็นเครื่องมือทางเศรษฐกิจของรัฐ หมายถึง นิติบุคคลที่จัดตั้งขึ้นโดยตราเป็นพระราชบัญญัติ เนื่องจากต้องการอำนาจรัฐในการบังคับฝ่ายเดียวต่อภาคเอกชนหรือประชาชน ในการสมทบเงินเข้ากองทุน

๑.๔ ขอบเขตของเนื้อหาภายในกรอบการกำกับดูแลข้อมูล

ขอบเขตของกรอบการกำกับดูแลข้อมูลในเอกสารฉบับนี้ ประกอบด้วย บทที่ ๒ อธิบายถึงแนวคิดการกำกับดูแลข้อมูล ประกอบด้วย นิยามของการกำกับดูแลข้อมูล ความหมายและประเภทข้อมูล การบริหารจัดการข้อมูล ความสัมพันธ์ระหว่างการบริหารจัดการข้อมูลกับการกำกับดูแลข้อมูล แนวคิดในการกำกับดูแลข้อมูลจากต่างประเทศ และกรณีศึกษาในการกำกับดูแลข้อมูลจากต่างประเทศ บทที่ ๓ กล่าวถึงกรอบการกำกับดูแลข้อมูล ประกอบด้วย สภาพแวดล้อมของการกำกับดูแลข้อมูล การนิยามข้อมูล กฎเกณฑ์ข้อมูล โครงสร้างของการกำกับดูแลข้อมูล กระบวนการกำกับดูแลข้อมูล และการวัดการดำเนินการและความสำเร็จของการกำกับดูแลข้อมูล

บทที่ ๒ แนวคิดการกำกับดูแลข้อมูล (DATA GOVERNANCE CONCEPT)

๒.๑ นิยามของการกำกับดูแลข้อมูล (Data Governance Definition)

การกำกับดูแลข้อมูล (Data Governance) ได้มีผู้เชี่ยวชาญจากหน่วยงานต่าง ๆ ให้คำนิยามไว้ดังต่อไปนี้

“กิจกรรมที่ประกอบด้วยการกำหนดอำนาจ การควบคุม และการตัดสินใจในการบริหารจัดการข้อมูล โดยที่ข้อมูลถูกจัดให้เป็นหนึ่งในสินทรัพย์ของหน่วยงาน” (Askham, N., 2016)

“ระบบที่กำหนดถึงอำนาจการตัดสินใจ และหน้าที่ความรับผิดชอบต่อกระบวนการที่เกี่ยวข้องกับข้อมูล โดยที่มีแบบแผนที่ชัดเจนและได้รับการยอมรับ ซึ่งแบบแผนดังกล่าวต้องสามารถอธิบายได้ว่า ใครมีบทบาทในการทำอะไรกับข้อมูลชุดไหน เมื่อไร ใช้หลักการและวิธีการอย่างไรในการใช้ข้อมูล ” (Thomas, 2009)

“การกำหนดสิทธิ์และการควบคุม (การวางแผน การตรวจสอบ และการบังคับ) ในการบริหารจัดการข้อมูล” (Henderson et al., 2017)

“การจัดการข้อมูล จากมุมมองที่เกี่ยวข้องกับข้อมูล ทำให้หน่วยงานตระหนักถึงการจัดทำมาตรฐานข้อมูลที่เป็นระบบและการบูรณาการข้อมูล ทั้งข้อมูลที่อยู่ในระบบ ข้อมูลที่สัมพันธ์กับการดำเนินงานของหน่วยงาน นโยบาย และกระบวนการปฏิบัติงานต่าง ๆ” (Kim, H. Y., & Cho, J. S., 2017)

จากนิยามต่าง ๆ ข้างต้น จึงได้ข้อสรุปว่า การกำกับดูแลข้อมูล (Data Governance) คือ “การกำหนดสิทธิในการตัดสินใจและความรับผิดชอบ ในการส่งเสริมให้เกิดกระบวนการจัดทำ การใช้งาน และการบริหารจัดการข้อมูล รวมถึงกระบวนการที่กำหนดบทบาท นโยบาย และมาตรฐาน ที่ช่วยสนับสนุนให้การดำเนินงานเกี่ยวกับข้อมูลมีประสิทธิภาพมากยิ่งขึ้น ซึ่งส่งผลให้หน่วยงานสามารถบรรลุเป้าหมายได้”

ในมุมมองของภาครัฐ การกำกับดูแลข้อมูล (Data Governance) หมายถึง “การกำหนดสิทธิ หน้าที่และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย โดยใช้ข้อมูลเป็นหลักในการขับเคลื่อนประเทศ เช่น การใช้ข้อมูลในการวิเคราะห์การตัดสินใจเชิงนโยบายและการบริหารราชการแผ่นดิน การเพิ่มประสิทธิภาพในการบริการประชาชน การเสริมสร้างและผลักดันธุรกิจที่เกิดจากการใช้นวัตกรรมข้อมูล ” ทั้งนี้ Intra-governmental Group on Geographic Information (IGGI, 2005) ให้องค์ประกอบหลักของการกำกับดูแลข้อมูลที่ดี ประกอบไปด้วย

๑) มีความมั่นคงปลอดภัยและรักษาความเป็นส่วนบุคคล โดยมีมาตรการในการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคล ซึ่งช่วยป้องกันความเสียหายที่จะเกิดขึ้นกับข้อมูลและการละเมิดสิทธิส่วนบุคคล

๒) มีมาตรการควบคุมและจัดการวงจรชีวิตของข้อมูล ซึ่งประกอบด้วย การประเมินธุรกิจ การกำหนดประเภทและแนวทางการแบ่งประเภทของชุดข้อมูล มีการตรวจสอบอย่างต่อเนื่อง ทั้งการเก็บข้อมูลและการทำลายข้อมูล

๓) มีนโยบายการใช้ข้อมูลที่ชัดเจน โดยกำหนดนโยบายและกฎเกณฑ์ของข้อมูลเป็นกรอบสำหรับการบริหารจัดการและกำกับดูแลข้อมูล

๔) มีการกำหนดบทบาทหน้าที่ของเจ้าของข้อมูล โดยกำหนดวิธีการที่ผู้ดูแลข้อมูลหรือเจ้าของข้อมูลสามารถจัดการ เปลี่ยนแปลง หรือส่งผ่านข้อมูลให้ชัดเจน เพื่อไม่ให้เกิดปัญหาในกรณีที่ชุดข้อมูลหรือฐานข้อมูลบางแหล่งอาจจะมีผู้ดูแล ผู้ใช้งาน หรือเจ้าของข้อมูลหลายคนหรือหลายหน่วยงาน

๕) ข้อมูลมีเมทาดาตา โดยเมทาดาตาจะช่วยให้ผู้ใช้งานเข้าใจว่าข้อมูลชุดนี้คือข้อมูลที่เกี่ยวข้องกับอะไร สามารถนำไปใช้งานอย่างไร และมีข้อจำกัดอะไร โดยมีมาตรฐานของเมทาดาตาที่เหมาะสมกับการใช้งาน

๖) ข้อมูลมีคุณภาพ โดยมีมาตรการในการควบคุมคุณภาพของข้อมูลให้มีคุณภาพสูง ซึ่งจะสนับสนุนให้การดำเนินงานของหน่วยงานเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

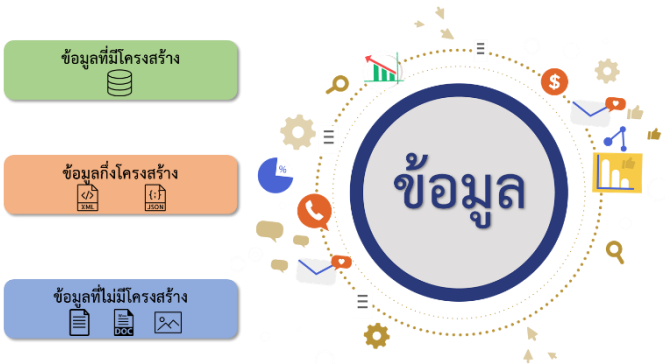
๒.๒ ข้อมูล (Data)

ข้อมูล คือ “ข้อเท็จจริงซึ่งใช้เป็นพื้นฐานสำหรับการอธิบายเหตุผล การสนทนา หรือการคำนวณ” (Australian Institute of Health and Welfare, 2014) ข้อมูลจัดเป็นองค์ประกอบหลักในการขับเคลื่อนหน่วยงาน ซึ่งมีความสัมพันธ์กับกระบวนการปฏิบัติงาน เทคโนโลยีสารสนเทศ สถานที่ รวมถึงบุคลากร

ข้อมูลจึงเปรียบเสมือนสินทรัพย์ที่มีความสำคัญเช่นเดียวกับสินทรัพย์ประเภทอื่น ดังนั้นหน่วยงานจึงจำเป็นต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล เช่น การรักษาความลับของข้อมูล (Confidentiality) การป้องกันไม่ให้เกิดเหตุการณ์ที่ทำให้ไม่สามารถใช้งานข้อมูลได้ (Loss of Availability) การรักษาความถูกต้องครบถ้วนของข้อมูล (Integrity) การทำให้ข้อมูลเป็นปัจจุบันอยู่เสมอ (Timeliness) ทั้งนี้เพื่อตอบสนองต่อการตัดสินใจทั้งในระดับปฏิบัติการและระดับยุทธศาสตร์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

๒.๒.๑ ประเภทข้อมูล (Types of Data)

ข้อมูลถูกจัดแบ่งออกได้เป็น ๓ ประเภท ดังนี้



รูปที่ ๑ ประเภทข้อมูล

๑) ข้อมูลที่มีโครงสร้าง (Structured Data) เป็นข้อมูลที่มีการนิยามโครงสร้างของข้อมูลไว้ โดยนิยามความหมายและคุณสมบัติของแต่ละฟิลด์ข้อมูล โครงสร้างมีชั้นเดียวทำให้ง่ายต่อการค้นหา เช่น ตารางข้อมูลในฐานข้อมูล Comma-Separated Values – CSV ดังแสดงในตารางที่ ๑

๒) ข้อมูลกึ่งโครงสร้าง (Semi-structured Data) เป็นข้อมูลที่มีการนิยามโครงสร้างของข้อมูลไว้ แต่โครงสร้างเป็นแบบลำดับขั้น (Hierarchy) เช่น Extensible Markup Language - XML JavaScript Object Notation - JSON

๓) ข้อมูลที่ไม่มีโครงสร้าง (Unstructured Data) เป็นข้อมูลที่ไม่ได้มีการนิยามโครงสร้างของข้อมูลไว้ มักจะอยู่ในรูปแบบ เช่น ข้อความ รูปภาพ เสียง วิดิทัศน์

๒.๒.๒ ชุดข้อมูล (Datasets)

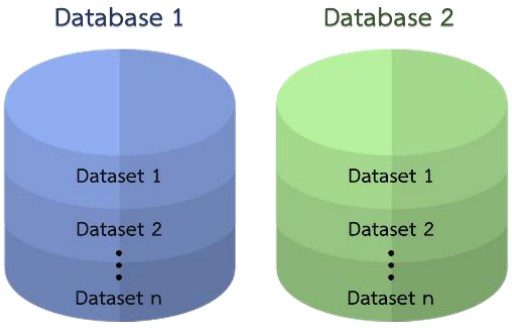
คือ “ข้อมูลที่มีการรวบรวมไว้ โดยปกติอยู่ในรูปแบบของตารางข้อมูล” (Askham et al., 2013) ตารางที่ ๑ แสดงตัวอย่างชุดข้อมูลพนักงานในรูปแบบตารางข้อมูลหรือข้อมูลที่มีโครงสร้าง (Structured Data) มีทั้งหมด ๓ แถว ๕ ฟิลด์ (Data Field/Element/Attribute) ได้แก่ ชื่อ นามสกุล เพศ อายุ และระดับการศึกษา

ตารางที่ ๑ ตัวอย่างชุดข้อมูลพนักงาน

ชื่อ	นามสกุล	เพศ	อายุ	ระดับการศึกษา
วิชัย	ใจดี	ชาย	26	ปริญญาตรี
พิเชษฐ์	วิเศษศิลป์	ชาย	28	ปริญญาโท
วิมลมาส	วงศ์สกุล	หญิง	25	ปริญญาตรี

๒.๒.๓ ฐานข้อมูล (Database)

คือ “กลุ่มข้อมูลที่มีความสัมพันธ์กันได้ถูกรวบรวมเข้าไว้ด้วยกัน ซึ่งสนับสนุนกิจกรรมของหน่วยงาน” (Malinowski, E. & Zimányi, E., 2009) หรือกล่าวได้ว่า แต่ละฐานข้อมูลจะประกอบไปด้วยหลาย ๆ ชุดข้อมูลที่มีความสัมพันธ์กันดังแสดงในรูปที่ ๒



รูปที่ ๒ ความสัมพันธ์ระหว่างฐานข้อมูลกับชุดข้อมูล

๒.๓ การบริหารจัดการข้อมูล (Data Management)

การบริหารจัดการข้อมูล คือ “คำจำกัดความที่อธิบายถึงกระบวนการที่ใช้ในการวางแผน (Plan) ระบุ (Specify) เปิดใช้งาน (Enable) สร้าง (Create) รับ (Acquire) ดูแลรักษา (Maintain) ใช้ (Use) จัดเก็บถาวร (Archive) ดึงข้อมูล (Retrieve) ควบคุม (Control) และทำลายข้อมูล (Purge)” (Cupola et al., 2014)

การบริหารจัดการข้อมูลเป็นสิ่งสำคัญสำหรับทุกหน่วยงาน ซึ่งแต่ละหน่วยงานต้องตระหนักว่าข้อมูลที่มีอยู่เป็นสินทรัพย์ที่มีค่า และจากการเกิดขึ้นของข้อมูลที่มีปริมาณมหาศาล ไม่ว่าจะเป็นข้อมูลที่รวบรวมมาโดยอัตโนมัติจากระบบหรืออุปกรณ์ต่าง ๆ หรือข้อมูลที่เกิดขึ้นจากการป้อนข้อมูลหรือโต้ตอบกับผู้ใช้งาน เพื่อให้หน่วยงานสามารถนำข้อมูลเหล่านี้ไปประมวลผลหรือใช้ในการตัดสินใจได้อย่างแม่นยำ จึงต้องได้รับการบริหารจัดการอย่างถูกต้อง เหมาะสม และสอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูลของหน่วยงาน เช่น

๑) เพื่อการจัดเก็บ นำมาใช้งาน และประมวลผลข้อมูลตามที่หน่วยงานต้องการ
๒) เพื่อควบคุม ตรวจสอบ และป้องกัน โดยใช้กระบวนการกำกับดูแลข้อมูลและความปลอดภัยของข้อมูล
๓) เพื่อจัดหมวดหมู่ และกำหนดมาตรฐานของข้อมูล โดยใช้การจำแนกข้อมูล และกำหนดกรอบการทำงานที่เป็นที่รู้จักแพร่หลาย
๔) เพื่อให้สามารถนำข้อมูลกลับมาใช้ได้ในภายหลัง โดยกำหนดข้อมูลให้อยู่ในรูปแบบที่เรียกใช้ได้อย่างมีประสิทธิภาพ
๕) เพื่อการปรับปรุงข้อมูลให้เป็นปัจจุบัน และมีความถูกต้องสมบูรณ์อยู่เสมอ
๖) เพื่อการปกป้องข้อมูลจากการลักลอบใช้งานหรือแก้ไขโดยมิชอบ รวมถึงจากเหตุการณ์ที่อาจเกิดจากภัยธรรมชาติหรือความบกพร่องภายในระบบคอมพิวเตอร์

ซึ่งในการบริหารจัดการข้อมูลนั้น มีองค์ประกอบในการบริหารจัดการตลอดทั้งวงจรชีวิตของข้อมูล ดังรูปที่ ๓

รูปที่ ๓ วงจรชีวิตของข้อมูล และองค์ประกอบในการบริหารจัดการข้อมูล

๒.๓.๑ วงจรชีวิตของข้อมูล (Data Life Cycle)

วงจรชีวิตของข้อมูล คือ “ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล” ประกอบด้วย ๖ ขั้นตอน ดังนี้

๑) กระบวนการสร้างข้อมูล (Create) เป็นการสร้างข้อมูลขึ้นมาใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคล หรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์ตรวจจับสัญญาณ (Sensor) รวมถึงการซื้อข้อมูล หรือการรับข้อมูลจากหน่วยงานอื่น เพื่อนำมาจัดเก็บในภายหลัง

๒) กระบวนการจัดเก็บข้อมูล (Store) เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้างหรือข้อมูลที่ได้จากการแลกเปลี่ยนกับหน่วยงานอื่น เพื่อให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหายหรือถูกทำลาย และให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS)

๓) กระบวนการใช้ข้อมูล (Use) เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ รวมถึงการสำรอง (Backup) ข้อมูล โดยการคัดลอกข้อมูลที่ใช้งานอยู่ในปัจจุบัน เพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)

๔) กระบวนการเผยแพร่ข้อมูล (Publish) เป็นการแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition)

๕) กระบวนการจัดเก็บข้อมูลถาวร (Archive) เป็นการคัดลอกเอาข้อมูลที่มีช่วงอายุเกินช่วงใช้งานหรือไม่ได้ใช้งานแล้ว เพื่อทำสำเนาสำหรับการเก็บรักษา โดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ

๖) กระบวนการทำลายข้อมูล (Destroy) เป็นการทำลายข้อมูล ซึ่งปกติจะเป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด

๒.๓.๒ องค์ประกอบในการบริหารจัดการข้อมูล (Data Management Component)

จากการศึกษาแนวคิดของ DAMA International (Henderson et al., 2017) ในการบริหารจัดการข้อมูล ได้กำหนดองค์ประกอบในการบริหารจัดการข้อมูล ดังนี้

๒.๓.๒.๑ สถาปัตยกรรมข้อมูล (Data Architecture)

สถาปัตยกรรมข้อมูล (Data Architecture) เป็นส่วนหนึ่งของการพัฒนาสถาปัตยกรรมองค์กร (Enterprise Architecture) เป็นการอธิบายเกี่ยวกับกลุ่มของข้อมูลทั้งหมดที่มีในหน่วยงาน ความสัมพันธ์ระหว่างข้อมูลกับกระบวนการปฏิบัติงาน ความสัมพันธ์ระหว่างข้อมูลกับแอปพลิเคชัน สถาปัตยกรรมเทคโนโลยีข้อมูล สถาปัตยกรรมการบูรณาการข้อมูล สถาปัตยกรรมเมทาดาตา เป็นต้น สถาปัตยกรรมข้อมูลจะอยู่ในรูปแบบของแบบจำลองข้อมูลที่มองเห็นภาพรวม ความเชื่อมโยง และการไหลของข้อมูลในระดับต่าง ๆ ทั้งหมดของหน่วยงาน ทั้งที่เป็นหน่วยงานต้นน้ำ กลางน้ำ หรือปลายน้ำ สามารถอธิบายสถานะที่มีอยู่ใน

ปัจจุบัน และกำหนดความต้องการสำหรับอนาคต เพื่อให้หน่วยงานเกิดความเข้าใจและเห็นเป็นภาพเดียวกัน ดังนั้นจึงเป็นพื้นฐานที่สำคัญในการวางแผนบริหารจัดการข้อมูล

รูปที่ ๔ ตัวอย่างความสัมพันธ์ระหว่างกลุ่มข้อมูลกับกลุ่มกระบวนการปฏิบัติงาน

จากรูปที่ ๔ ตัวอย่างความสัมพันธ์ระหว่างกลุ่มข้อมูลกับกลุ่มกระบวนการปฏิบัติงาน ซึ่งชี้ให้เห็นถึงภาพรวมของข้อมูลทั้งหมดที่มีการดำเนินการในแต่ละกลุ่มกระบวนการปฏิบัติงาน กอง หรือส่วนงานภายในหน่วยงาน ความสัมพันธ์นี้สามารถใช้เป็นจุดเริ่มต้นในการจัดลำดับความสำคัญของข้อมูล กำหนดขอบเขต กำหนดอัตรากำลังคน และจัดสรรงบประมาณในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูล จากตารางที่ ๒ แสดงความสัมพันธ์ระหว่างข้อมูลกับแอปพลิเคชันในงานบริหารจัดการพัสดุ ซึ่งชี้ให้เห็นว่าข้อมูลเดียวกันอาจจะมีการใช้งานหรือเก็บซ้ำซ้อนกันในหลาย ๆ แอปพลิเคชัน

ดังนั้นความสัมพันธ์ระหว่างข้อมูลกับแอปพลิเคชันสามารถสนับสนุนการบูรณาการข้อมูล (Data Integration) ได้จากการที่ข้อมูลกระจายอยู่ตามแอปพลิเคชันต่าง ๆ ตัวอย่างสถาปัตยกรรมการบูรณาการข้อมูล ดังแสดงในรูปที่ ๘ ซึ่งแสดงความสัมพันธ์ระหว่างคลังข้อมูล ทะเลสาบข้อมูล ระบบรายงานอัจฉริยะ และดาตาอนาไลติกส์

ตารางที่ ๒ ตัวอย่างความสัมพันธ์ระหว่างข้อมูลกับแอปพลิเคชัน สำหรับงานบริหารจัดการพัสดุ

ข้อมูล / แอปพลิเคชัน		แอปพลิเคชัน								
		ระบบจัดการครุภัณฑ์ด้าน IT	ระบบเบิกวัสดุ	ระบบแจ้งซ่อม	ระบบรายการครุภัณฑ์	ระบบบริหารจัดการบุคลากร	ระบบบริหารการจัดซื้อจัดจ้าง	ระบบครุภัณฑ์องค์กร	ระบบพิมพ์รหัสครุภัณฑ์	ระบบบัญชีการเงิน
D32 : ข้อมูลพัสดุ	ข้อมูลครุภัณฑ์	X	X	X	X		X	X	X	X
	ข้อมูลการตรวจสอบพัสดุ		X					X		
	ข้อมูลบาร์โค้ด							X	X	
	ข้อมูลสถานะพัสดุ	X	X					X		
	ข้อมูลการโอนคืน									
	ข้อมูลการจำหน่าย		X					X		
	ข้อมูลตราสินค้า	X	X				X	X		
	ข้อมูลการรับประกัน	X						X		
	ข้อมูลการซ่อมบำรุง			X						
D30 : ข้อมูลพนักงาน	ข้อมูลพนักงาน	X		X		X	X	X		X
D31 : ข้อมูลการจัดซื้อจัดจ้าง	ข้อมูลใบสั่งซื้อ (PO)		X				X	X		X

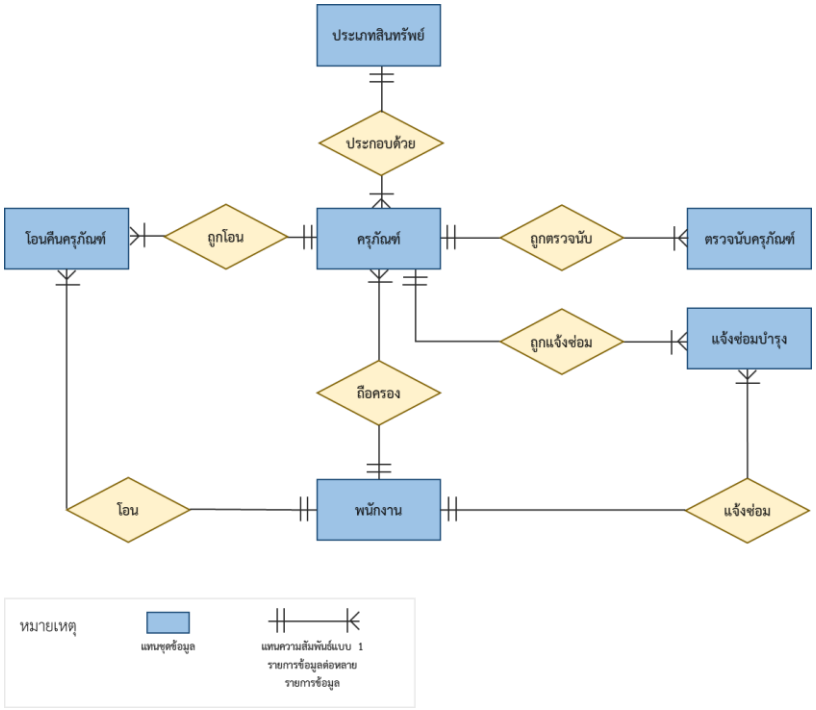
ตารางที่ ๓ สรุปการบริหารจัดการสถาปัตยกรรมข้อมูล

วิธีดำเนินการ	• ทำความเข้าใจกับความต้องการข้อมูลของหน่วยงาน • ประเมินสถานะและข้อกำหนดของสถาปัตยกรรมข้อมูลในปัจจุบัน • ออกแบบ พัฒนา และปรับปรุงแบบจำลองข้อมูลของหน่วยงาน • สร้างความสอดคล้องของข้อมูลของหน่วยงานกับส่วนงานอื่น ๆ ที่เกี่ยวข้อง เช่น กระบวนการธุรกิจ แอปพลิเคชัน • ออกแบบ พัฒนา และปรับปรุงสถาปัตยกรรมข้อมูล
สิ่งที่นำเข้า	• สถาปัตยกรรมองค์กร (Enterprise Architecture) • มาตรฐานและเป้าหมายที่เกี่ยวกับเทคโนโลยีสารสนเทศ
เครื่องมือที่ใช้	• เครื่องมือจัดทำแบบจำลองข้อมูล (Data Modeling Tool) สำหรับจัดทำแบบจำลองข้อมูลระดับหน่วยงาน • เครื่องมือบริหารจัดการแบบจำลอง (Model Management Tool) สำหรับจัดเก็บแบบจำลองข้อมูลและควบคุมการเปลี่ยนแปลงของแบบจำลองข้อมูล
ผลที่ได้รับ	• แบบจำลองข้อมูลระดับหน่วยงาน (Enterprise Data Model) • ความสัมพันธ์ระหว่างข้อมูลกับส่วนงาน ข้อมูลกับกระบวนการปฏิบัติงาน และข้อมูลกับแอปพลิเคชัน เป็นต้น • สถาปัตยกรรมเทคโนโลยีข้อมูล (Data Technology Architecture)
ผู้ที่เกี่ยวข้อง	• สถาปนิกข้อมูล (Data Architect)

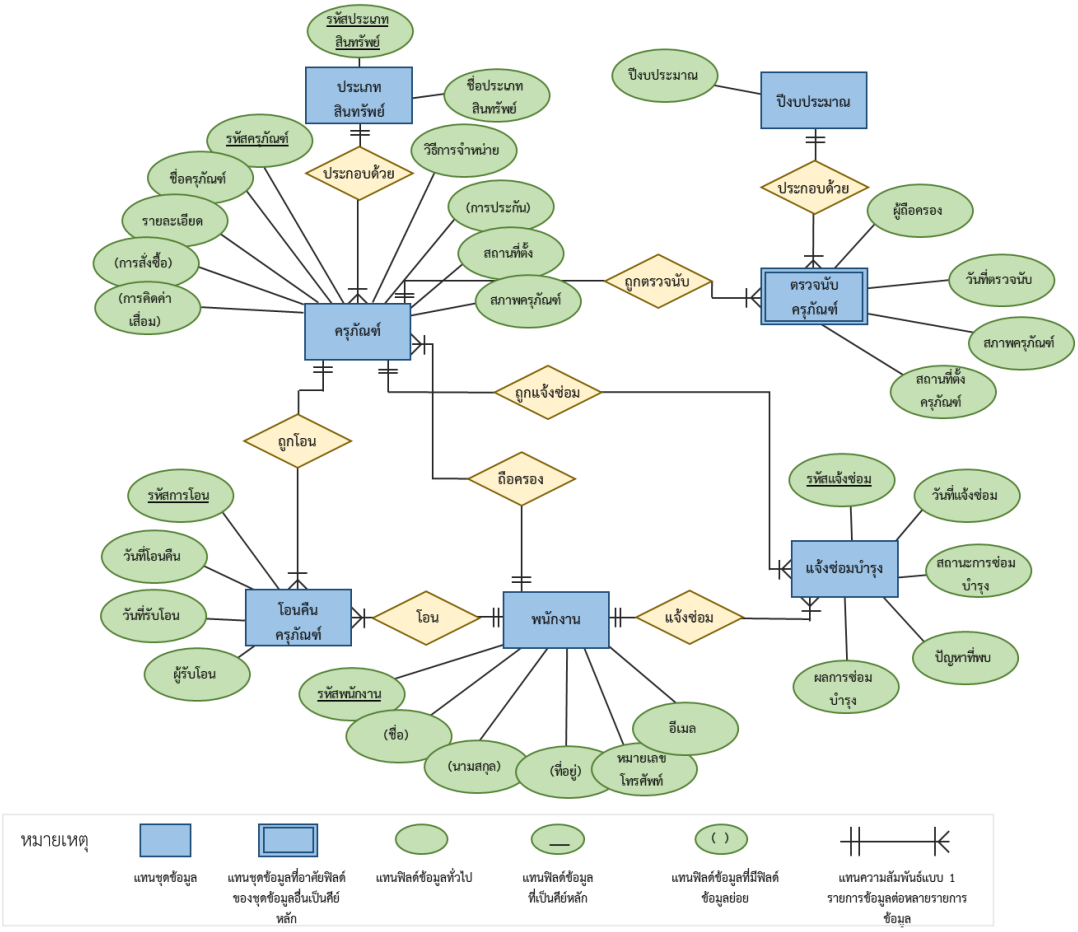
๒.๓.๒.๒ การจำลองและการออกแบบข้อมูล (Data Modeling and Design)

การจำลองและการออกแบบข้อมูล (Data Modeling and Design) เป็นวิธีการวิเคราะห์ความต้องการของผู้ใช้งาน รวมถึงระบุข้อกำหนดและการแก้ปัญหาต่าง ๆ ที่เกี่ยวข้อง แบบจำลองข้อมูลแสดงในรูปแบบของไดอะแกรม (Diagram) ที่มีการออกแบบลักษณะโครงสร้างของข้อมูล เพื่อใช้ในการสื่อสารภายในหน่วยงานให้เข้าใจตรงกัน แบบจำลองข้อมูลจะแสดงถึงความสัมพันธ์ระหว่างข้อมูลที่เกี่ยวข้องกันพร้อมทั้งรายละเอียดของโครงสร้างของข้อมูล โดยแบ่งออกเป็น ๓ ระดับ ได้แก่ แบบจำลองข้อมูลเชิงความคิด (Conceptual Data Model) แบบจำลองข้อมูลเชิงตรรกะ (Logical Data Model) และแบบจำลองข้อมูลเชิงกายภาพ (Physical Data Model)

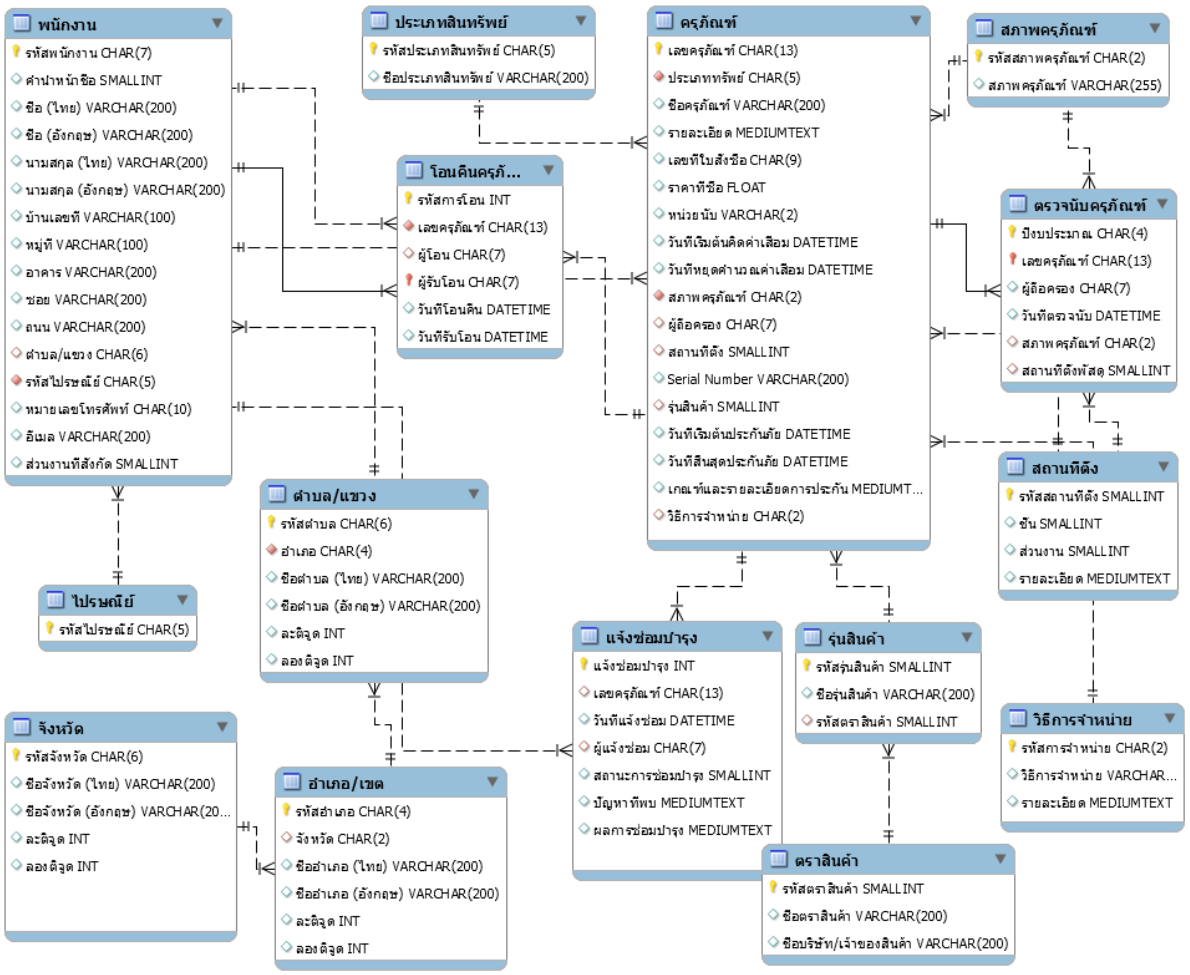
ขั้นตอนในการสร้างแบบจำลองและการออกแบบข้อมูล เริ่มตั้งแต่การวิเคราะห์ความต้องการของผู้ใช้เพื่อกำหนดเป็นแบบจำลองข้อมูลเชิงความคิดของข้อมูลขึ้นมา เป็นขั้นตอนของการกำหนดเค้าโครงในระดับเบื้องต้น สามารถมองเห็นถึงความสัมพันธ์ของข้อมูล แต่ยังไม่สามารถนำไปใช้งานได้จริงเพราะเป็นเพียงแนวคิดเท่านั้น หลังจากนั้นทำการออกแบบข้อมูลให้มีความชัดเจนมากขึ้นโดยกำหนดเป็นแบบจำลองข้อมูลเชิงตรรกะ ซึ่งเป็นการให้รายละเอียดของข้อมูลที่มากขึ้น (เช่น ฟิลด์ข้อมูล) ขั้นตอนสุดท้ายจึงกำหนดแบบจำลองข้อมูลเชิงกายภาพ เพื่อให้สามารถใช้งานได้จริง โดยกำหนดรายละเอียดของข้อมูลเพิ่มเติม เช่น รูปแบบของข้อมูล ขนาดของข้อมูล



รูปที่ ๕ ตัวอย่างแบบจำลองข้อมูลเชิงความคิด (Conceptual Data Model) สำหรับงานบริหารจัดการพัสดุ



รูปที่ ๖ ตัวอย่างแบบจำลองข้อมูลเชิงตรรกะ (Logical Data Model) สำหรับงานบริหารจัดการพัสดุ



รูปที่ ๗ ตัวอย่างแบบจำลองข้อมูลเชิงกายภาพ (Physical Data Model) สำหรับงานบริหารจัดการพัสดุ

จากรูปที่ ๕ แสดงตัวอย่างแบบจำลองข้อมูลเชิงความคิดสำหรับงานบริหารจัดการพัสดุ ซึ่งแสดงให้เห็นว่า ประเภทสินทรัพย์ ๑ ประเภท ประกอบด้วยครุภัณฑ์หลายรายการ พนักงาน ๑ ราย ถือครองครุภัณฑ์ได้หลายรายการ และแจ้งซ่อมได้หลายครั้ง ครุภัณฑ์ ๑ รายการ สามารถโอน ตรวจนับ และแจ้งซ่อมได้หลายครั้ง สำหรับฟิล์ดข้อมูลของแต่ละชุดข้อมูลแสดงในแบบจำลองเชิงตรรกะตามรูปที่ ๖ ทั้งนี้รายละเอียดด้านเทคนิคอธิบายไว้ในรูปที่ ๗ ประกอบด้วย คีย์หลัก ประเภทข้อมูล และความกว้างของฟิลด์ข้อมูล

ตารางที่ ๔ สรุปการบริหารจัดการการจำลองและการออกแบบข้อมูล

วิธีการดำเนินการ	• วิเคราะห์ความต้องการข้อมูลของหน่วยงาน • ออกแบบและพัฒนาแบบจำลองของข้อมูล รวมถึงฐานข้อมูล
สิ่งที่นำเข้า	• สถาปัตยกรรมองค์กร (Enterprise Architecture) • มาตรฐานและเป้าหมายที่เกี่ยวกับเทคโนโลยีสารสนเทศ
เครื่องมือที่ใช้	• เครื่องมือจัดทำแบบจำลองข้อมูล (Data Modeling Tool) • เครื่องมือบริหารจัดการแบบจำลอง (Model Management Tool) • ระบบการจัดการฐานข้อมูล (Database Management System - DBMS) สำหรับออกแบบ แบบจำลองข้อมูลเชิงกายภาพ

ผลที่ได้รับ	• ความต้องการของข้อมูล (Data Requirement) และข้อกำหนดทางธุรกิจ (Business Rules) • แบบจำลองข้อมูลเชิงแนวคิด (Conceptual Data Models) • แบบจำลองข้อมูลเชิงตรรกะ (Logical Data Models) • แบบจำลองข้อมูลเชิงกายภาพ (Physical Data Models)
ผู้เกี่ยวข้อง	• สถาปนิกข้อมูล (Data Architect) • นักวิทยาการข้อมูล (Data Scientist) • นักวิเคราะห์ข้อมูล (Data Analyst) • นักวิเคราะห์ธุรกิจ (Business Analyst) • นักออกแบบจำลองข้อมูล (Data Modeler)

๒.๓.๒.๓ การจัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operations)

การจัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operations) เป็นการจัดเก็บข้อมูลที่มีโครงสร้าง โดยจัดเก็บในรูปแบบของฐานข้อมูล ส่วนการดำเนินการกับข้อมูล จะเกี่ยวข้องตั้งแต่การวางแผนการใช้งาน การสำรองข้อมูล (Backup) การกู้คืนข้อมูล (Restore) การจัดเก็บข้อมูลถาวร (Archive) กระบวนที่เกี่ยวข้องกับข้อมูล (Create Read Update Delete – CRUD) ตลอดทั้งวงจรชีวิตของข้อมูล การโอนย้ายข้อมูล (Migration) รวมถึงการปรับปรุงประสิทธิภาพของฐานข้อมูลให้พร้อมใช้งานได้ตลอดเวลา เพื่อรักษาความมั่นคงปลอดภัยและความถูกต้องของข้อมูล

ตารางที่ ๕ สรุปการบริหารจัดการการจัดเก็บและการดำเนินการกับข้อมูล

วิธีการดำเนินการ	• สนับสนุนในส่วนของฐานข้อมูล เช่น การจัดเก็บ การสำรอง การกู้คืน การปรับปรุงประสิทธิภาพของระบบการจัดการฐานข้อมูล • จัดการในส่วนของเทคโนโลยีด้านข้อมูล เช่น ศึกษาความต้องการของเทคโนโลยีด้านข้อมูล
สิ่งที่นำเข้า	• ข้อกำหนดและเงื่อนไขการให้บริการ (Service Level Agreement) • สถาปัตยกรรมข้อมูล (Data Architecture) • ข้อเสนอแนะในการโอนย้ายข้อมูล (Migration)
เครื่องมือที่ใช้	• ระบบการจัดการฐานข้อมูล (Database Management System - DBMS) • เครื่องมือบริหารจัดการฐานข้อมูล (Database Administration Tool)
ผลที่ได้รับ	• แผนการสำรองและข้อมูลได้รับการสำรอง • แผนการกู้คืนข้อมูลและข้อมูลได้รับการกู้คืน • แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plans)
ผู้เกี่ยวข้อง	• ผู้บริหารจัดการฐานข้อมูล (Database Administrator - DBA) • วิศวกรข้อมูล (Data Engineer)

๒.๓.๒.๔ การบูรณาการและความสามารถในการทำงานร่วมกัน (Data Integration and Interoperability)

การบูรณาการข้อมูล (Data Integration) เป็นการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ในรูปแบบที่สอดคล้องกันเข้ามารวมอยู่ในแหล่งข้อมูลเดียวกัน เพื่อนำไปใช้ในการจัดทำข้อมูลหลัก (Master Data) คลังข้อมูล (Data Warehouse) ทะเลสาบข้อมูล (Data Lake) รวมถึงการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน รูปที่ ๘ แสดงความสัมพันธ์ระหว่างการบูรณาการข้อมูล คลังข้อมูล และทะเลสาบข้อมูล ส่วนความสามารถในการทำงานร่วมกัน (Interoperability) จะมีการกำหนดมาตรฐานหรือข้อตกลงร่วมกันระหว่างหน่วยงานหรือระบบ โดยมีการอ้างถึงคุณลักษณะของระบบต่าง ๆ ที่สามารถแลกเปลี่ยนข้อมูลกันหรือสื่อสารกันได้ เช่น มีการแลกเปลี่ยนข้อมูลในรูปแบบของ Application Programming Interfaces – API

ในการรวบรวมข้อมูลจากแหล่งต่าง ๆ เข้าด้วยกัน ทำให้การบูรณาการข้อมูล มีส่วนช่วยควบคุมและจัดการคุณภาพของข้อมูลให้ดียิ่งขึ้น ขณะที่การแลกเปลี่ยนข้อมูลจะสนับสนุนให้เกิดประสิทธิภาพของการดำเนินงานระหว่างหน่วยงานหรือส่วนงาน เพราะทั้งหมดนี้มุ่งเน้นการแปลงข้อมูล (Transform) และรวมข้อมูลจากหน่วยงานหรือระบบต้นทางไปจนถึงหน่วยงานหรือระบบกลาง และจากหน่วยงานหรือระบบกลางไปยังหน่วยงานหรือระบบปลายทาง เพื่อใช้ในการวิเคราะห์ข้อมูลต่อไป

ตารางที่ ๖ สรุปการบริหารจัดการการบูรณาการและความสามารถในการทำงานร่วมกัน

วิธีการดำเนินการ	• กำหนดมาตรฐานและแบบจำลองอ้างอิงของการทำงานร่วมกัน • พัฒนาแผนการดำเนินงานการบูรณาการและการทำงานร่วมกัน
สิ่งที่นำเข้า	• หลักเกณฑ์การแลกเปลี่ยนและเชื่อมโยงผ่านระบบและเครือข่ายสารสนเทศและการสื่อสาร
เครื่องมือที่ใช้	• เครื่องมือจัดทำแบบจำลองข้อมูล (Data Modeling Tool) • Enterprire Service Bus (ESB) คือ ตัวกลางที่ทำให้ผู้ต้องการเรียกใช้งานบริการ (Services) ต่าง ๆ จากระบบสามารถเรียกผ่าน ESB ได้
ผลที่ได้รับ	• รายละเอียดของสิ่งที่เกี่ยวข้อง เช่น ฐานข้อมูล API • แนวปฏิบัติในการแลกเปลี่ยนข้อมูล • ข้อตกลงในการเข้าถึงข้อมูลและแลกเปลี่ยนข้อมูล
ผู้เกี่ยวข้อง	• วิศวกรข้อมูล (Data Engineer)

๒.๓.๒.๕ การบริหารจัดการเอกสารและเนื้อหา (Document and Content Management)

การบริหารจัดการเอกสารและเนื้อหา (Document and Content Management) เป็นการวางแผนการจัดการ การเข้าถึง การใช้งาน และการควบคุมกิจกรรมต่าง ๆ ที่เกี่ยวกับข้อมูลที่ไม่มีโครงสร้างหรือแบบกึ่งโครงสร้าง เช่น การจัดเก็บ การป้องกันความเสียหาย การเข้าถึงข้อมูล ทั้งที่เก็บอยู่ในรูปแบบกระดาษ และไฟล์อิเล็กทรอนิกส์ มีข้อความ รูปภาพ เสียง ภาพเคลื่อนไหว เป็นต้น การบริหารจัดการดังกล่าวมุ่งเน้นที่การรักษาความถูกต้องสมบูรณ์ และช่วยให้สามารถเข้าถึงเอกสารและข้อมูลที่ไม่มีโครงสร้างหรือแบบกึ่งโครงสร้างได้

ตารางที่ ๗ สรุปการบริหารจัดการเอกสารและเนื้อหา

วิธีการดำเนินการ	• พัฒนาระบบจัดการเอกสาร เพื่อการจัดเก็บ การเข้าถึง และการควบคุมความปลอดภัย • จัดทำนโยบายการจัดทำเนื้อหา (Content Handling Policies)
สิ่งที่นำเข้า	• ข้อมูลที่เป็นสื่อสังคมออนไลน์ (Social Media) • เอกสารที่เป็นกระดาษ
เครื่องมือที่ใช้	• เครื่องมือบริหารจัดการเอกสาร (Document Management Tool) • เครื่องมือบริหารจัดการเนื้อหา (Content Management Tool)
ผลที่ได้รับ	• เอกสารหรือรายงาน
ผู้เกี่ยวข้อง	• พนักงานหรือเจ้าหน้าที่

๒.๓.๒.๖ ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data)

ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data) เป็นการบริหารจัดการข้อมูลเพื่อให้ทั้งหน่วยงานสามารถเข้าถึง และใช้ข้อมูลร่วมกันได้ โดยข้อมูลถูกจัดเก็บไว้แหล่งเดียว มีการกำหนดมาตรฐานของข้อมูล เพื่อช่วยลดความซ้ำซ้อนของข้อมูล ทำให้ข้อมูลมีคุณภาพ ความแตกต่างระหว่างข้อมูลหลัก (Master Data) กับข้อมูลอ้างอิง (Reference Data) กล่าวคือ ข้อมูลอ้างอิง จะเป็นข้อมูลที่เป็นสากล มีการเปลี่ยนแปลงค่อนข้างน้อย เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัดระยะทาง ขณะที่ข้อมูลหลักมีโอกาสเปลี่ยนแปลงได้มากกว่า มีรายละเอียดหรือจำนวนฟิลด์ข้อมูลที่มากกว่า และใช้เป็นข้อมูลในการดำเนินงานภายในหน่วยงาน เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลผู้ขาย ข้อมูลสินค้า ข้อมูลครุภัณฑ์ ข้อมูลสถานที่

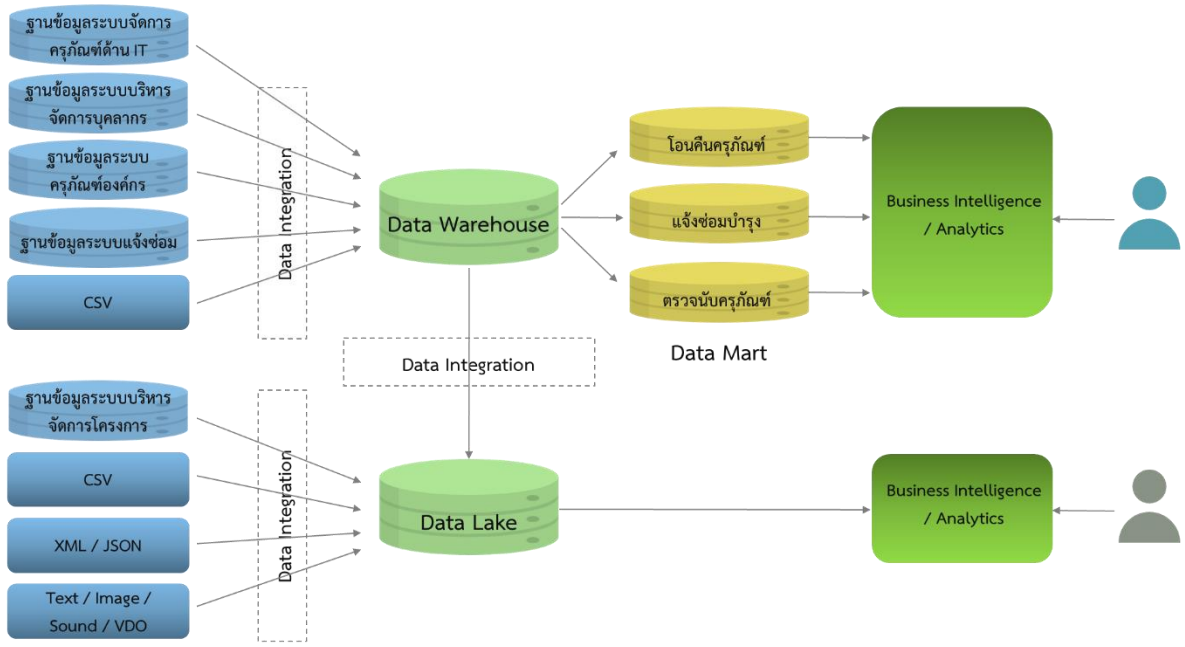
ตารางที่ ๘ สรุปการบริหารจัดการข้อมูลหลักและข้อมูลอ้างอิง

วิธีการดำเนินการ	• ทำความเข้าใจเกี่ยวกับความต้องการข้อมูลทั้งข้อมูลหลักและข้อมูลอ้างอิง • กำหนดแหล่งที่มา (Source) ของข้อมูลหลักและข้อมูลอ้างอิง • ดำเนินการจัดทำข้อมูลหลักและข้อมูลอ้างอิง
สิ่งที่นำเข้า	• อภิธานศัพท์ข้อมูล (Data Glossary)
เครื่องมือที่ใช้	• เครื่องมือบริหารจัดการข้อมูลหลัก (Master Data Management Tools) • เครื่องมือบริหารจัดการข้อมูลอ้างอิง (Reference Data Management Tools) • เครื่องมือจัดทำแบบจำลองข้อมูล (Data Modeling Tools) • เครื่องมือสำหรับบูรณาการข้อมูล (Data Integration Tools)
ผลที่ได้รับ	• ข้อมูลหลักและข้อมูลอ้างอิง
ผู้เกี่ยวข้อง	• สถาปนิกข้อมูล (Data Architect) • นักวิทยาการข้อมูล (Data Scientist) • วิศวกรข้อมูล (Data Engineer) • นักออกแบบจำลองข้อมูล (Data Modeler)

๒.๓.๒.๗ คลังข้อมูล ทะเลสาบข้อมูล ระบบรายงานอัจฉริยะ และดาตาอนาไลติกส์ (Data Warehouse, Data Lake, Business Intelligence, and Data Analytics)

คลังข้อมูล (Data Warehouse) เป็นข้อมูลที่ได้จากการบูรณาการข้อมูล (Data Integration) ซึ่งเกิดจากการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ที่มีหลากหลายรูปแบบมาเก็บในคลังข้อมูล โดยผ่านกระบวนการของ Extract Transform Load (ETL) ในรูปแบบข้อมูลที่มีโครงสร้าง และถูกจัดทำให้อยู่ในรูปแบบที่เหมาะสมสำหรับการนำไปวิเคราะห์ข้อมูล ทั้งในรูปแบบของรายงานอัจฉริยะ (Business Intelligence) และดาตาอนาไลติกส์ (Data Analytics)

ทะเลสาบข้อมูล (Data Lake) เป็นแหล่งสำหรับเก็บรวบรวมข้อมูลที่มีหลากหลายรูปแบบ ข้อมูลที่จัดเก็บเป็นข้อมูลที่มีโครงสร้าง ข้อมูลกึ่งโครงสร้าง และข้อมูลที่ไม่มีโครงสร้าง โดยข้อมูลถูกเก็บรักษาไว้ในรูปแบบที่เหมือนหรือใกล้เคียงกับรูปแบบที่ได้รับมาจากแหล่งข้อมูลต้นฉบับ และสามารถใช้เป็นที่สำรองข้อมูลต้นฉบับได้



รูปที่ ๘ ตัวอย่างความสัมพันธ์ระหว่างคลังข้อมูล ทะเลสาบข้อมูล ระบบรายงานอัจฉริยะและดาตาอนาไลติกส์สำหรับงานบริหารจัดการพัสดุ

จากรูปที่ ๘ คลังข้อมูลและทะเลสาบข้อมูลจะเกิดจากการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ซึ่งแต่ละแหล่งอาจจะมีรูปแบบของข้อมูลที่แตกต่างกัน การรวบรวมข้อมูลใช้วิธีการบูรณาการข้อมูล (ดูที่หัวข้อ ๒.๓.๒.๔) โดยข้อมูลจากคลังข้อมูลสามารถรวมเข้าไปที่ทะเลสาบข้อมูลเพื่อใช้สำหรับการวิเคราะห์ข้อมูลที่ซับซ้อนมากยิ่งขึ้น ข้อมูลในคลังข้อมูลจะต้องถูกจัดกลุ่มออกเป็น ตลาดข้อมูล (Data Mart) โดยต้องสอดคล้องกับหน่วยงานที่จะนำไปใช้ เช่น ตลาดข้อมูลของฝ่ายบุคคล ตลาดข้อมูลของฝ่ายการตลาด ตลาดข้อมูลของฝ่ายการเงิน หลังจากนั้นข้อมูลในตลาดข้อมูลถูกนำไปใช้สำหรับการทำรายงานอัจฉริยะ (Business Intelligence) หรือการทำนายสิ่งที่จะเกิดขึ้นในอนาคตผ่านวิธีการของดาตาอนาไลติกส์ ในกรณีของทะเลสาบข้อมูลสามารถนำข้อมูลไปใช้สำหรับทำรายงานอัจฉริยะและดาตาอนาไลติกส์ได้ทันทีโดยไม่ต้องสร้างตลาดข้อมูล

หลังจากข้อมูลต่าง ๆ ถูกทำการวิเคราะห์ออกเป็นรายงานอัจฉริยะและผลการทำนายแล้ว จะถูกนำไปใช้ เพื่อสนับสนุนการตัดสินใจของหน่วยงานทั้งในระดับปฏิบัติการและระดับบริหารต่อไป

ตารางที่ ๙ สรุปการบริหารจัดการคลังข้อมูล ทะเลสาบข้อมูล ระบบรายงานอัจฉริยะ และดาตาอนาไลติกส์

วิธีการดำเนินการ	• จัดเตรียมข้อมูลจากหลาย ๆ แหล่งมารวมกันในคลังข้อมูล • ประมวลผลข้อมูลสำหรับทำการวิเคราะห์
สิ่งที่นำเข้า	• ความต้องการทางธุรกิจ (Business Requirement) • ข้อมูลหลักและข้อมูลอ้างอิง
เครื่องมือที่ใช้	• เครื่องมือสำหรับบูรณาการข้อมูล (Data Integration Tools) • เครื่องมือบริหารจัดเก็บข้อมูล (Data Storage Tools) • เครื่องมือสำหรับจัดทำรายงานอัจฉริยะ (Business Intelligence Tools) • เครื่องมือวิเคราะห์ทางสถิติ (Statistics Tools) • การเรียนรู้ของเครื่องและปัญญาประดิษฐ์ (Machine Learning and Artificial Intelligence)
ผลที่ได้รับ	• รายงาน และ Dashboard • ผลการทำนาย
ผู้เกี่ยวข้อง	• สถาปนิกข้อมูล (Data Architect) • นักวิทยาการข้อมูล (Data Scientist) • วิศวกรข้อมูล (Data Engineer) • นักวิเคราะห์ข้อมูล (Data Analyst)

๒.๓.๒.๘ เมทาดาตา (Metadata)

เมทาดาตา (Metadata) เป็นข้อมูลที่ใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่น ๆ ที่เกี่ยวข้องทั้งกระบวนการเชิงธุรกิจและเชิงเทคโนโลยีสารสนเทศ กฎและข้อจำกัดของข้อมูล และโครงสร้างของข้อมูล เมทาดาตาช่วยให้หน่วยงานสามารถเข้าใจข้อมูล ระบบ และขั้นตอนการทำงานได้ดียิ่งขึ้น โดยการบริหารจัดการเมทาดาตา (Metadata Management) เริ่มตั้งแต่ การเก็บรวมรวม การจัดกลุ่ม การดูแล และการควบคุมเมทาดาตา ทั้งนี้ข้อมูลแต่ละชุดควรมีเมทาดาตา เพื่อให้ผู้ใช้งานทราบเกี่ยวกับชุดข้อมูล เช่น รายละเอียดชุดข้อมูล สิ่งที่เกี่ยวข้องกับชุดข้อมูล วัตถุประสงค์การนำไปใช้ ฟิลด์ข้อมูล

ตารางที่ ๑๐ ตัวอย่างเมทาดาตาของข้อมูลครุภัณฑ์

ชื่อข้อมูล	ข้อมูลครุภัณฑ์			
คำอธิบายอย่างย่อ	อ้างถึงครุภัณฑ์ที่หน่วยงานถือครองทั้งจากการซื้อมาหรือรับมารวมถึงพัสดุประเภทวัสดุควบคุม			
เจ้าของข้อมูล	ส่วนจัดซื้อและพัสดุ			
Attribute	**Description**	**Type**	**Allowed Null**	**Key**
เลขครุภัณฑ์	รูปแบบเลขครุภัณฑ์: xx-xxxx-xxx-xxxx รูปแบบเลขวัสดุควบคุม: ED-xx-xxxx-xxx-xxxx (ในกรณีเป็นวัสดุควบคุม ขณะแสดงรหัสวัสดุควบคุมให้นำ “ED” ไว้ข้าง xx-xxxx-xxx-xxxx)	CHAR(13)	N	PK
ประเภทสินทรัพย์	อ้างอิง: รหัสประเภทสินทรัพย์	CHAR(5)	N	FK
ชื่อครุภัณฑ์		VARCHAR(200)	N	
รายละเอียด		MEDIUMTEXT	Y	
เลขที่ใบสั่งซื้อ	รูปแบบ: DGA/XX/XXXX คำอธิบาย: XX อ้างถึง ปีงบประมาณ และ XXXX อ้างถึง Running Number ตัวอย่าง: DGA/59/0001	CHAR(9)	N	
ราคาที่ซื้อ		FLOAT	N	
หน่วยนับ	อ้างอิง: รหัสหน่วยนับ	VARCHAR(2)	N	FK
วันที่เริ่มต้นคิดค่าเสื่อม	รูปแบบ: YYYY-MM-DD คำอธิบาย: ปี ค.ศ.-เดือน-วัน ตัวอย่าง: 2016-04-15	DATETIME	N	
วันที่หยุดคำนวณค่าเสื่อม	รูปแบบ: YYYY-MM-DD คำอธิบาย: ปี ค.ศ.-เดือน-วัน ตัวอย่าง: 2016-04-15	DATETIME	N	
สภาพครุภัณฑ์	อ้างอิง: รหัสสภาพครุภัณฑ์	CHAR(2)	N	FK
ผู้ถือครอง	อ้างอิง: รหัสพนักงาน	CHAR(7)	N	FK
สถานที่ตั้งพัสดุ	อ้างอิง: รหัสสถานที่ตั้ง	SMALLINT	N	FK
รหัสรุ่นสินค้า		VARCHAR(200)	N	
รุ่นสินค้า	อ้างอิง: รหัสรุ่นสินค้า	SMALLINT	N	FK
วันที่เริ่มต้นประกัน	รูปแบบ: YYYY-MM-DD คำอธิบาย: ปี ค.ศ.-เดือน-วัน	DATETIME	Y	

ชื่อข้อมูล	ข้อมูลครุภัณฑ์			
คำอธิบายอย่างย่อ	อ้างถึงครุภัณฑ์ที่หน่วยงานถือครองทั้งจากการซื้อมาหรือรับมารวมถึงพัสดุประเภทวัสดุควบคุม			
เจ้าของข้อมูล	ส่วนจัดซื้อและพัสดุ			
Attribute	**Description**	**Type**	**Allowed Null**	**Key**
	ตัวอย่าง: 2016-04-15			
วันที่สิ้นสุดประกัน	รูปแบบ: YYYY-MM-DD คำอธิบาย: ปี ค.ศ.-เดือน-วัน ตัวอย่าง: 2016-04-15	DATETIME	Y	
เกณฑ์และรายละเอียดการประกัน	เกณฑ์ รายละเอียดการประกัน และบริษัทที่ให้การประกัน	MEDIUMTEXT	Y	
วิธีการจำหน่ายพัสดุ	อ้างอิง: รหัสวิธีการจำหน่ายพัสดุ	CHAR(2)	N	FK

ตารางที่ ๑๑ สรุปการบริหารจัดการเมทาดาตา

วิธีการดำเนินการ	• ทำความเข้าใจเกี่ยวกับความต้องการในการจัดทำเมทาดาตา • กำหนดมาตรฐานของเมทาดาตา
สิ่งที่นำเข้า	• คู่มือแนวปฏิบัติมาตรการการบริหารจัดการเมทาดาตา เช่น พจนานุกรมข้อมูล (Data Dictionary) การตั้งชื่อข้อมูล (Data Naming)
เครื่องมือที่ใช้	• เครื่องมือบริหารจัดการบัญชีข้อมูล (Data Catalog Management Tools) • เครื่องมือบริหารจัดการเมทาดาตา (Metadata Repository Management Tools)
ผลที่ได้รับ	• เมทาดาตาที่มีคุณภาพ มีความสอดคล้อง และความมั่นคงปลอดภัย
ผู้เกี่ยวข้อง	• บริกรข้อมูล (Data Stewards) • นักวิเคราะห์ข้อมูล (Data Analyst)

๒.๓.๒.๙ ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy)

ความมั่นคงปลอดภัยของข้อมูล (Data Security) หมายรวมถึง การป้องกันข้อมูลในบริบทของการรักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูล จากข้อมูลของมาตรฐาน ISO/IEC27001 โดยมีรายละเอียด ดังนี้

- การรักษาความลับ (Confidentiality) หมายถึง การรักษาข้อมูลตามสภาพของการจัดชั้นความลับ และมีการกำหนดสิทธิ์การเข้าถึงข้อมูลนั้น เนื่องจากข้อมูลในหน่วยงานอาจมีหลายประเภท ข้อมูลบางประเภทเป็นข้อมูลที่มีความสำคัญ หรืออ่อนไหว จึงต้องมีการรักษาความลับเพื่อลดความเสี่ยงของการถูกคุกคามและเป็นการป้องกันการรั่วไหลของข้อมูลโดยมิชอบ เช่น การ

ส่งข้อมูลที่ปกปิดหรือเป็นความลับต้องมีวิธีการที่ทำให้ทราบได้ว่าบุคคลที่ต้องการส่งข้อมูลมาให้หรือการที่ผู้ได้รับการอนุญาตให้เข้าถึงข้อมูลเท่านั้นที่สามารถอ่านข้อมูลได้

- ความถูกต้องของข้อมูล (Integrity) หมายถึง การคงสภาพของข้อมูลหรือการรักษาความถูกต้องสมบูรณ์ของข้อมูลให้มีความถูกต้องและน่าเชื่อถือ รวมถึงมีการปกป้องข้อมูลให้ปราศจากการถูกเปลี่ยนแปลงโดยผู้ไม่มีสิทธิ์ เช่น ข้อมูลที่ใช้จะต้องเป็นข้อมูลที่ถูกต้องอย่างแท้จริง ไม่มีการดัดแปลงหรือแก้ไขระหว่างทาง
- ความพร้อมใช้งานของข้อมูล (Availability) หมายถึง การพร้อมในการใช้งานอยู่เสมอ กล่าวคือข้อมูลต้องพร้อมสำหรับการใช้งานได้เสมอ รวมถึงมีการสำรองข้อมูลไว้เมื่อเกิดภัยพิบัติหรือเหตุการณ์ที่ไม่คาดฝัน เช่น หากต้องการใช้ข้อมูล ผู้ใช้งานสามารถใช้ข้อมูลได้ทันที และใช้ได้อย่างต่อเนื่อง

โดยความมั่นคงปลอดภัยของข้อมูลต้องดำเนินการตั้งแต่การวางแผน การจัดทำ การปฏิบัติตาม และการบังคับใช้นโยบายและขั้นตอนด้านการรักษาความปลอดภัย เพื่อสนับสนุนในด้านที่เกี่ยวข้องกับการพิสูจน์ตัวตน การกำหนดสิทธิ์ การเข้าถึงข้อมูล การตรวจสอบ และความพร้อมใช้ของข้อมูลอย่างเหมาะสม

นอกจากนี้ ต้องมีการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy) ตั้งแต่การรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูล โดยจะต้องมีการระบุวัตถุประสงค์เป็นหลักฐานให้ชัดเจน ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดที่ไม่สอดคล้องกับวัตถุประสงค์ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลนั้น ๆ หรือมีกฎหมายกำหนดให้สามารถกระทำสิ่งนั้นได้

ตารางที่ ๑๒ สรุปการบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล

วิธีการดำเนินการ	• กำหนดนโยบายและมาตรฐานด้านความปลอดภัยของข้อมูล • บริหารจัดการเกี่ยวกับข้อมูลตั้งแต่วิธีการจัดเก็บ การประมวลผล การเข้าถึงข้อมูล การนำไปใช้ การเปิดเผย และการทำลาย
สิ่งที่นำเข้า	• มาตรฐาน แนวปฏิบัติ และนโยบายที่เกี่ยวกับความปลอดภัยของข้อมูล • มาตรฐาน แนวปฏิบัติ และนโยบายที่เกี่ยวกับการรักษาความเป็นส่วนบุคคลของข้อมูล • มาตรฐานและหลักเกณฑ์การพิสูจน์และยืนยันตัวตนทางดิจิทัล
เครื่องมือที่ใช้	• ระบบการจัดการฐานข้อมูล (Database Management System - DBMS) • เทคโนโลยีจัดการข้อมูลเพื่อแสดงตัวตน (Identity Management Technology) • ระบบจัดการการเปลี่ยนแปลง (Change Control System) • หนังสือให้ความยินยอม (Letter of Consent)
ผลที่ได้รับ	• นโยบายด้านการรักษาความปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policy) • มาตรฐานชั้นความลับข้อมูล (Data Classification Standard)

ผู้เกี่ยวข้อง	• ผู้บริหารจัดการฐานข้อมูล (Database Administrator) • บริกรข้อมูล (Data Stewards) • ผู้ตรวจสอบภายใน (Internal Auditor)

๒.๓.๒.๑๐ คุณภาพของข้อมูล (Data Quality)

คุณภาพของข้อมูล (Data Quality) เป็นเครื่องมือในการวัดความน่าเชื่อถือและประสิทธิภาพของการนำข้อมูลไปใช้ ต้องมีการวางแผน การดำเนินการ และการควบคุมกิจกรรมต่าง ๆ รวมถึงการปรับปรุง เพื่อให้ข้อมูลมีคุณภาพ เนื่องจากข้อมูลที่มีคุณภาพสูงทำให้การดำเนินงานของหน่วยงานเป็นไปอย่างมีประสิทธิภาพ การทำให้ข้อมูลมีคุณภาพ ประกอบด้วย การทำให้ข้อมูลมีความถูกต้อง (Accuracy) ข้อมูลมีความครบถ้วน (Completeness) ข้อมูลมีความต้องกัน (Consistency) ข้อมูลมีความเป็นปัจจุบัน (Timeliness) ข้อมูลตรงตามความต้องการของผู้ใช้ (Relevancy) และข้อมูลมีความพร้อมใช้ (Availability) ดังแสดงรายละเอียดเพิ่มเติมในบทที่ ๓.๖.๒ การประเมินคุณภาพของข้อมูล (Data Quality Assessment)

ตารางที่ ๑๓ สรุปการบริหารจัดการคุณภาพข้อมูล

วิธีการดำเนินการ	• กำหนดข้อมูลที่จำเป็นต้องมีคุณภาพ • พัฒนาและส่งเสริมการให้ความสำคัญกับคุณภาพของข้อมูล (Awareness) • กำหนดขอบเขตของการประเมิน (Assessment) คุณภาพของข้อมูล • กำหนดและระบุลำดับความสำคัญ (Prioritize) ของการปรับปรุงข้อมูลให้มีคุณภาพ
สิ่งที่นำเข้า	• มาตรฐาน แนวปฏิบัติ และนโยบายที่เกี่ยวกับการทำให้ข้อมูลมีคุณภาพ เช่น การจัดทำโปรไฟล์ข้อมูล (Data Profiling) การทำความสะอาดข้อมูล (Data Cleansing) • เมทาดาตาทั้งด้านธุรกิจและเทคโนโลยีสารสนเทศ
เครื่องมือที่ใช้	• เครื่องมือในการทำความสะอาดข้อมูล (Data Cleansing Tools) • เครื่องมือวิเคราะห์ทางสถิติ (Statistical Analysis Tools)
ผลที่ได้รับ	• รายงานการรับรองคุณภาพของข้อมูล (Data Quality Certification Reports) • ข้อตกลงระดับคุณภาพของข้อมูล (Data Quality Service Level Agreements)
ผู้เกี่ยวข้อง	• นักวิเคราะห์ข้อมูล (Data Analyst) • บริกรข้อมูล (Data Stewards)

ทั้งนี้ระดับคุณภาพข้อมูลในมุมมองของข้อมูลขนาดใหญ่ (Big Data) หรือวิทยาการข้อมูล (Data Science) มีความแตกต่างกับระดับคุณภาพข้อมูลทั่วไป เช่น ความพร้อมใช้ของผลการวิเคราะห์ที่ได้รับจากข้อมูลขนาดใหญ่ (Timely) ความเชื่อมั่นในผลการวิเคราะห์ (Reliable) ข้อมูลขนาดใหญ่มีความสัมพันธ์กับวัตถุประสงค์ของการวิเคราะห์หรือสิ่งที่ต้องการทำนาย (Meaningful) และความสามารถในการผลักดันผลการวิเคราะห์ถูกนำไปใช้ในสถานการณ์จริง (Sufficient) (Kim, H. Y., & Cho, J. S., 2017)

๒.๔ ความสัมพันธ์ระหว่างการบริหารจัดการข้อมูลกับการกำกับดูแลข้อมูล

จากผลการศึกษาที่เกี่ยวข้องการบริหารจัดการข้อมูลของสมาคมบริหารจัดการข้อมูลระหว่างประเทศ (Data Management Association International) จะเห็นว่า การกำกับดูแลข้อมูล (Data Governance) เป็นส่วนที่สำคัญในการบริหารจัดการข้อมูล (Data Management) เป็นกลไกในการกำหนดทิศทาง ควบคุม และทวนสอบการบริหารจัดการข้อมูล เพื่อให้มั่นใจได้ว่าหน่วยงานได้ดำเนินการบริหารจัดการข้อมูลเป็นไปตามนโยบาย กฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้

ดังนั้นสิ่งที่ควรริเริ่มเป็นอันดับแรกของการวางแผนในการบริหารจัดการข้อมูล ก็คือ การกำกับดูแลข้อมูล เพราะเป็นเรื่องของการกำหนดบทบาท หน้าที่ความรับผิดชอบ และการตัดสินใจ เพื่อสร้างความเชื่อมั่นว่าการกำกับดูแล ความรับผิดชอบ และความเป็นเจ้าของหรือผู้มีส่วนได้ส่วนเสียกับสินทรัพย์ข้อมูลนั้น เป็นไปอย่างมีระเบียบ ถูกต้อง และมีความยั่งยืน โดยการกำกับดูแลข้อมูลจะต้องเข้าไปมีส่วนร่วมในทุก ๆ องค์ประกอบหรือกิจกรรมของการบริหารจัดการข้อมูล

อย่างไรก็ตามการบริหารจัดการข้อมูลนั้นมีความหมายที่กว้างกว่าและเกี่ยวข้องกับแง่มุมของการใช้ข้อมูลและดำเนินงานในกระบวนการที่เกิดขึ้นซ้ำ ๆ ในแต่ละช่วงของวงจรชีวิตของข้อมูล

ทั้งนี้หากภาครัฐมีการกำกับดูแลข้อมูลที่ดีจะก่อให้เกิดการบริหารจัดการข้อมูลที่ดีเช่นกัน ส่งผลให้ข้อมูลมีความมั่นคงปลอดภัย มีคุณภาพ สามารถเชื่อมโยงกันได้ มีคุณค่าทางเศรษฐกิจและสังคม และได้รับความคุ้มทุนต่อการดำเนินงาน

๒.๕ แนวคิดในการกำกับดูแลข้อมูลจากต่างประเทศ

ในส่วนนี้อธิบายแนวคิดในการกำกับดูแลข้อมูลของหน่วยงานต่างประเทศ เพื่อใช้เป็นแนวทางในการจัดทำกรอบการกำกับดูแลข้อมูลสำหรับหน่วยงานภาครัฐ ซึ่งมีรายละเอียดดังนี้

๒.๕.๑ แนวคิดของ Data Governance Institute (DGI)

DGI (Thomas, 2009) เป็นหน่วยงานที่ให้แนวทางและแนวปฏิบัติในการกำกับดูแลข้อมูล โดยหน่วยงานต่าง ๆ จากทั่วโลกสามารถนำไปประยุกต์ใช้อย่างกว้างขวาง DGI เสนอกรอบการกำกับดูแลข้อมูล ซึ่งมี ๑๐ องค์ประกอบ และถูกจัดกลุ่มเป็น ๓ หมวด ดังต่อไปนี้

๑) กฎเกณฑ์ (Rules of Engagement)
- องค์ประกอบที่ ๑ วิสัยทัศน์และภารกิจ (Vision and Mission)
- องค์ประกอบที่ ๒ เป้าหมาย การวัดการกำกับดูแล/การวัดความสำเร็จ และยุทธศาสตร์การจัดหาเงินทุน (Goals, Governance Metrics / Success Measures, Funding Strategies)
- องค์ประกอบที่ ๓ นิยามข้อมูลและกฎเกณฑ์ (Data Definitions and Rules)
- องค์ประกอบที่ ๔ สิทธิในการตัดสินใจ (Decision Rights)
- องค์ประกอบที่ ๕ ความสามารถในการตรวจสอบได้และการรับผิดชอบในผลของการดำเนินการ (Accountabilities)
- องค์ประกอบที่ ๖ การควบคุมความเสี่ยง (Control)

๒) โครงสร้างการกำกับดูแลและบุคลากร (People and Organizational Bodies)

- องค์ประกอบที่ ๗ ผู้มีส่วนได้ส่วนเสีย (Data Stakeholders) คือ บุคลากรของหน่วยงานที่มีส่วนเกี่ยวข้องกับข้อมูล เช่น บุคคลที่ทำหน้าที่ บันทึกข้อมูล ใช้ข้อมูล และกำหนดกฎเกณฑ์และความต้องการที่เกี่ยวข้องกับข้อมูล ผู้มีส่วนได้ส่วนเสียระดับบริหาร (Executive Stakeholders) จะถูกกำหนดให้เป็นคณะกรรมการกำกับดูแลข้อมูล (Data Governance Board) เพื่อทำหน้าที่ดูแลภาพรวมของการกำกับดูแลข้อมูล กำหนดนโยบายข้อมูล และแก้ไขปัญหา
- องค์ประกอบที่ ๘ สำนักงานกำกับดูแลข้อมูล (Data Governance Office) คือ กลุ่มคนที่ทำหน้าที่ช่วยเหลือและสนับสนุนกลุ่มบุคคลอื่น ๆ ที่ดำเนินการเกี่ยวกับการกำกับดูแลข้อมูล เช่น สนับสนุนการสื่อสารระหว่างบุคคลในกิจกรรมที่เกี่ยวข้องกับการกำกับดูแลข้อมูล สนับสนุนการเข้าถึงแหล่งข้อมูล ให้ความรู้ที่เกี่ยวข้องกับการกำกับดูแลข้อมูล
- องค์ประกอบที่ ๙ บริกรข้อมูล (Data Stewards) คือ บุคคลที่อยู่ในคณะกรรมการบริกรข้อมูล (Data Stewardship Council) ทำหน้าที่ร่างนโยบายข้อมูล ระบุมาตรฐานที่จะใช้ และอาจให้คำแนะนำต่อคณะกรรมการกำกับดูแลข้อมูล

๓) กระบวนการกำกับดูแลข้อมูล (The Process of Governing Data)

- องค์ประกอบที่ ๑๐ กระบวนการกำกับดูแลข้อมูล ประกอบด้วย กำหนดเป้าหมายและยุทธศาสตร์ เตรียมแผนงาน วางแผนงานและงบประมาณ ออกแบบแผนดำเนินการ ประกาศใช้แผนดำเนินการ กำกับดูแลข้อมูล และติดตามการดำเนินงาน/วัดผลการดำเนินงาน/รายงานผลการดำเนินงาน

๒.๕.๒ แนวคิดของ Data Management Association International (DAMA International)

DAMA International (Henderson et al., 2017) เป็นองค์กรอิสระที่รวบรวมผู้เชี่ยวชาญด้านข้อมูลเข้าด้วยกัน เพื่อส่งเสริมให้เกิดความรู้ ความเข้าใจ และสนับสนุนให้เกิดการพัฒนาแนวคิด และแนวปฏิบัติในการบริหารจัดการข้อมูล โดยมีการกำกับดูแลข้อมูลเป็นหนึ่งในองค์ประกอบหลักของการบริหารจัดการข้อมูล วัตถุประสงค์ของการกำกับดูแลข้อมูล เป็นการตรวจสอบเพื่อให้ทราบแน่ชัดว่าข้อมูลต่าง ๆ มีการบริหารจัดการอย่างถูกต้องตรงตามนโยบาย และแนวทางปฏิบัติอย่างดีที่สุด รวมถึงมีการปฏิบัติตามกฎระเบียบ ซึ่งการกำกับดูแลข้อมูลที่ดีต้องสอดคล้องกับยุทธศาสตร์ของหน่วยงาน มุ่งเน้นการลดความเสี่ยง ทั้งด้านความปลอดภัยของข้อมูล รักษาความเป็นส่วนบุคคล หรือปรับปรุงกระบวนการปฏิบัติงาน เพื่อให้ได้ข้อมูลที่มีคุณภาพ สำหรับเป้าหมายของการกำกับดูแลข้อมูล เพื่อทำให้หน่วยงานสามารถบริหารจัดการข้อมูลในลักษณะของสินทรัพย์ได้ โดยนำเสนอหลักการ นโยบาย กระบวนการ กรอบการกำกับดูแล และบริหารจัดการข้อมูล เพื่อเป็นแนวทางในการบริหารจัดการข้อมูลทุกระดับ DAMA International ได้กล่าวถึง โครงสร้างของบุคลากรที่รับผิดชอบในการกำกับดูแลข้อมูลและกระบวนการกำกับดูแลข้อมูล ดังนี้

๑) โครงสร้างของบุคลากรที่รับผิดชอบในการกำกับดูแลข้อมูล ประกอบด้วย

- คณะกรรมการขับเคลื่อนการกำกับดูแลข้อมูล (Data Governance Steering Committee) เป็นผู้มีอำนาจสูงสุดในการขับเคลื่อนให้เกิดการกำกับดูแลข้อมูล โดยมีหน้าที่รับผิดชอบในการกำกับดูแล สนับสนุน และระดมทุนของกิจกรรมที่เกี่ยวข้อง ส่วนใหญ่คณะกรรมการจะเป็นผู้บริหารระดับสูงของแต่ละหน่วยงานมาดำเนินงานร่วมกัน

- คณะกรรมการกำกับดูแลข้อมูล (Data Governance Council) เป็นกลุ่มบุคคลที่ริเริ่ม และยกระดับการบริหารจัดการการกำกับดูแลข้อมูลภายในหน่วยงาน ซึ่งคณะกรรมการจะเป็นผู้บริหารจากฝ่ายงานต่าง ๆ ทั้งจากฝ่ายบริหารและฝ่ายเทคโนโลยีสารสนเทศรวมไปถึงระดับหัวหน้างาน ทำหน้าที่จัดทำและตัดสินใจในเชิงนโยบาย
- สำนักงานกำกับดูแลข้อมูล (Data Governance Office) มีหน้าที่ในการนิยามข้อมูลและมาตรฐานข้อมูลในภาพรวมของทั้งหน่วยงาน โดยการประสานงานกับบริกรข้อมูล (Data Stewards) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) และเจ้าของข้อมูล (Data Owner)
- ทีมบริกรข้อมูล (Data Steward Team) กลุ่มบุคคลที่มุ่งเน้นการดำเนินงาน และกำหนดมาตรฐานในการบริหารจัดการตามองค์ประกอบของการบริหารจัดการข้อมูลอย่างน้อยหนึ่งองค์ประกอบ กลุ่มบุคคลที่เกี่ยวข้องประกอบไปด้วยบริกรข้อมูล (Data Stewards) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) และนักวิเคราะห์ข้อมูล (Data Analyst)
- คณะกรรมการกำกับดูแลข้อมูลภายในหน่วยงาน (Local Data Governance Committee) ในหน่วยงานขนาดใหญ่อาจมีส่วนงานที่ดูแลเกี่ยวกับการกำกับดูแลข้อมูลโดยเฉพาะที่อยู่ภายใต้การทำงานของคณะกรรมการกำกับดูแลข้อมูล

๒) กระบวนการกำกับดูแลข้อมูล เริ่มตั้งแต่การวางแผนไปจนถึงการดำเนินการกำกับดูแลอย่างต่อเนื่อง มีรายละเอียดดังต่อไปนี้

- การวางแผนการกำกับดูแลข้อมูล โดยการกำหนดเป้าหมาย หลักการ นโยบาย กลยุทธ์ และประเด็นปัญหาในการกำกับดูแล มีการประเมินความพร้อมของหน่วยงาน เตรียมการสำหรับการบริหารการเปลี่ยนแปลง และดำเนินงานให้เป็นไปตามเป้าหมาย และระยะเวลาที่กำหนด
- ดำเนินการที่เกี่ยวข้องกับข้อมูลให้เป็นไปตามกรอบการกำกับดูแลข้อมูล เช่น การกำหนดมาตรฐานข้อมูล
- ดำเนินการกำกับดูแลข้อมูลในหน่วยงานให้สอดคล้องกับแผนงานที่ได้กำหนดไว้

๒.๖ กรณีศึกษาในการกำกับดูแลข้อมูลจากต่างประเทศ

ในส่วนนี้กล่าวถึงกรณีศึกษาในการกำกับดูแลข้อมูลของหน่วยงานต่างประเทศ ซึ่งเป็นการประยุกต์ใช้แนวคิดในการกำกับดูแลข้อมูล โดยมีรายละเอียดดังนี้

๒.๖.๑ กรณีศึกษาของประเทศออสเตรเลีย

ประเทศออสเตรเลียมีหน่วยงานกลางในการกำกับดูแลข้อมูล เพื่อกำหนดมาตรฐานในการจัดเก็บ การใช้ การเชื่อมโยงระหว่างหน่วยงาน และการบริหารจัดการข้อมูลที่เกิดขึ้นภายในประเทศออสเตรเลีย อย่างไรก็ตามหน่วยงานภาครัฐบางส่วนมีการกำหนดกรอบการกำกับดูแลข้อมูลของหน่วยงานเอง เช่น Workplace Gender Equality Agency และ Australian Institute of Health and Welfare ซึ่งมีรายละเอียด ดังนี้

๑) หน่วยงานกลางในการกำกับดูแลข้อมูล

ประเทศออสเตรเลียมีการจัดตั้ง Data Governance Australia (DGA) เพื่อกำกับดูแลข้อมูลและสร้างความเชื่อมั่นให้กับหน่วยงานต่าง ๆ (ทั้งภาครัฐและภาคเอกชน) ในการแลกเปลี่ยนข้อมูลโดยไม่ผิดข้อกฎหมาย ซึ่งจะทำให้การดำเนินการของภาครัฐและภาคเอกชนที่ใช้ข้อมูลเป็นไปได้ด้วยดี DGA ได้ก่อตั้งขึ้นเมื่อปี พ.ศ. ๒๕๕๙ โดยคณะกรรมการบริหารเป็นผู้เชี่ยวชาญเกี่ยวกับข้อมูลจากหลากหลายองค์กร ได้แก่ มหาวิทยาลัย หน่วยงานภาครัฐ และหน่วยงานเอกชน

เป้าหมายของ DGA คือการสร้างมาตรฐานในกระบวนการเก็บ การใช้ และการบริหารจัดการข้อมูลที่เกิดขึ้นภายในประเทศออสเตรเลีย โดยทำหน้าที่ให้ข้อมูลเกี่ยวกับการกำกับดูแลข้อมูลและการเชื่อมโยงข้อมูลระหว่างหน่วยงานกับผู้ที่เป็นสมาชิก ซึ่งหน่วยงานที่เป็นสมาชิกจะได้รับการอบรมเรื่องต่าง ๆ ที่เกี่ยวข้องกับการกำกับดูแลข้อมูล ไม่ว่าจะเป็นข้อกำหนดในการกำกับดูแล การแลกเปลี่ยนข้อมูลโดยไม่ขัดกับข้อกำหนด กฎหมาย หรือนโยบายที่ถูกกำหนดโดยรัฐบาลกลางออสเตรเลีย นอกจากนี้ยังมีการให้บริการข้อมูลที่เกี่ยวข้องกับสมาชิก โดยเฉพาะเรื่องเกี่ยวกับแนวโน้มการกำกับดูแลข้อมูลจากต่างประเทศอีกด้วย โดยประโยชน์ที่สมาชิกจะได้รับมี ๗ ข้อ ดังนี้

- **การสนับสนุนจากรัฐบาล** โดยหน่วยงานที่เป็นสมาชิกจะได้รับการดูแลในเรื่องที่สำคัญเกี่ยวกับข้อมูล ได้แก่ ความเป็นส่วนบุคคล ความปลอดภัยจากจู่โจมทางอินเทอร์เน็ต การควบคุมและดูแลข้อมูล การใช้ และความเสี่ยงในการใช้งานข้อมูล
- **มาตรฐานและคู่มือการใช้งาน** มีการจัดทำคู่มือและมาตรฐานให้ศึกษาเพื่อทำให้สมาชิกสามารถดำเนินกิจกรรมที่เกี่ยวข้องกับข้อมูลได้เป็นอย่างดี
- **เครื่องหมายความไว้วางใจ**ของ DGA โดยสมาชิกจะได้รับการดูแลจนกระทั่งได้ตามมาตรฐานของ DGA ซึ่งการมีมาตรฐาน DGA จะทำให้สมาชิกเป็นที่ยอมรับจากสมาชิกอื่น ๆ ทำให้การเชื่อมโยงข้อมูลกับหน่วยงานอื่น ๆ ที่มีมาตรฐานเดียวกันเป็นไปได้ด้วยดี
- **มาตรฐานของการกำกับดูแลข้อมูล** มาตรฐานของ DGA เป็นที่ยอมรับจากมหาวิทยาลัยในเรื่องการกำกับดูแลข้อมูล
- **หลักสูตร** มีการกำหนดหลักสูตรการศึกษาต่าง ๆ ที่จะช่วยให้สมาชิกมีความเข้าใจในการกำกับดูแลรวมถึงหลักปฏิบัติในการกำกับดูแลข้อมูล
- **กิจกรรม** มีกิจกรรมส่งเสริมความเข้าใจในเรื่องการกำกับดูแลข้อมูลให้กับสมาชิกสามารถเข้าร่วมได้โดยไม่มีค่าใช้จ่าย
- **งานวิจัยและบทความ** สมาชิกสามารถอ่านบทความและงานวิจัยที่วิเคราะห์การกำกับดูแลข้อมูล รวมถึงแนวโน้มการเปลี่ยนแปลงของการกำกับดูแลข้อมูลของโลกด้วย

อย่างไรก็ตามพันธกิจของหน่วยงานกลางเน้นในการแลกเปลี่ยนข้อมูลเป็นหลัก แต่ไม่ได้เน้นในเรื่องของโครงสร้างการกำกับดูแลข้อมูลที่ชัดเจน ทั้งนี้โครงสร้างการกำกับดูแลข้อมูลจะขึ้นอยู่กับแต่ละหน่วยงาน ซึ่งได้อธิบายไว้ในหัวข้อ กรอบการกำกับดูแลข้อมูลของ Workplace Gender Equality Agency และ Australian Institute of Health and Welfare

๒) กรอบการกำกับดูแลข้อมูลของหน่วยงาน Workplace Gender Equality Agency (WGEA)

WGEA มีหน้าที่ในการส่งเสริมและปรับปรุงความเสมอภาคกันทางเพศในสถานที่ทำงานในประเทศออสเตรเลีย ซึ่งได้ดำเนินงานเรื่องความเสมอภาคกันทางเพศในสถานที่ทำงาน โดยการร่วมมือกับนายจ้างเพื่อให้คำปรึกษา แนะนำช่วยเหลือนายจ้างเรื่องความเสมอภาคทางเพศ เป้าหมายในการสร้างกรอบการกำกับดูแลของหน่วยงานนี้ คือ การให้หน่วยงานมีนโยบายและขั้นตอนการจัดการข้อมูลที่ดีที่สุดในการปฏิบัติงาน สนับสนุนให้เกิดการจัดการข้อมูลที่มีประสิทธิภาพและกลายเป็นส่วนหนึ่งของการปฏิบัติงาน โดยมีการกำกับดูแลเพื่อควบคุมการบริหารจัดการข้อมูลตลอดทั้งวงจรชีวิตข้อมูล ได้แก่ การวางแผน การเก็บข้อมูล การวิเคราะห์ และการเปิดเผย ทั้งนี้แนวคิดของกรอบการกำกับดูแลข้อมูลของหน่วยงานได้ร่างแบบศึกษามาจากกรอบการกำกับดูแลของ DGI และกรอบการบริหารจัดการข้อมูลของ DAMA International กรอบการกำกับดูแลของหน่วยงานประกอบด้วย ๓ ส่วนสำคัญ ได้แก่

- **บุคลากร** มีการกำหนดหน้าที่และความรับผิดชอบที่ชัดเจน ประกอบด้วย ของบริกรข้อมูล (Data Stewards) และบริกรข้อมูลด้านเทคนิค (Technical Data Stewards) รวมไปถึงบุคลากรอื่น ๆ ที่เกี่ยวข้องกับข้อมูล
- **การกำกับดูแลและการปกครอง** มีสาระสำคัญคือกลยุทธ์และเป้าหมายทางธุรกิจของหน่วยงานตลอดจนขอบเขตการทำงาน นอกจากนี้ยังได้กำหนดกิจกรรมการจัดการและการสนับสนุนทรัพยากรของหน่วยงานด้วย
- **ระบบการดำเนินการ** ประกอบด้วย นโยบาย ขั้นตอนความปลอดภัย อุปกรณ์ โปรแกรมคอมพิวเตอร์ แอปพลิเคชัน และเครื่องมือต่าง ๆ ที่สนับสนุนการจัดการข้อมูลที่มีประสิทธิภาพ รวมไปถึงมาตรฐานในการดำเนินงานเพื่อทำให้เกิดการกำกับดูแลข้อมูล โดยมีกลุ่มบุคลากรจำนวนหนึ่งทำหน้าที่สร้างมาตรฐาน และดำเนินงานเกี่ยวกับมาตรฐานของข้อมูล นอกจากนี้ บุคลากรกลุ่มนี้ต้องมีการวัดมาตรฐานของข้อมูลในปีที่ผ่านมา และต้องมีการตรวจสอบการดำเนินการข้อมูลของบุคลากรที่เกี่ยวข้องกับข้อมูลอีกด้วย

๓) กรอบการกำกับดูแลข้อมูลของหน่วยงาน Australian Institute of Health and Welfare (AIHW)

AIHW เป็นหน่วยงานที่ให้ข้อมูลที่น่าเชื่อถือเกี่ยวกับสุขภาพและสวัสดิการของออสเตรเลีย นอกจากนี้ยังสนับสนุนการพัฒนานโยบาย โครงการด้านสุขภาพและสวัสดิการของประเทศออสเตรเลีย

- ภาพรวมของกรอบการกำกับดูแลข้อมูลของ AIHW ได้แก่
  - คำอธิบายของแนวคิดหลักในการจัดการข้อมูล
  - กฎหมายที่เกี่ยวข้องกับการกำกับดูแลของ AIHW
  - โครงสร้างและบทบาทของการจัดการข้อมูล
  - ภาพรวมของนโยบายขั้นตอนและหลักเกณฑ์เกี่ยวกับข้อมูล AIHW
  - ระบบและเครื่องมือที่สนับสนุนการจัดการข้อมูล
  - แนวทางการปฏิบัติตามกฎระเบียบ

- แนวคิดการกำกับดูแลข้อมูล ได้แก่ การเก็บรวบรวมข้อมูล การกำกับดูแลและจัดการข้อมูล การลงทะเบียนข้อมูล มาตรฐานเมทาดาตา คู่มือเกี่ยวกับนโยบาย หลักเกณฑ์ และวิธีการในการดำเนินการ และเครื่องมือที่จะใช้ในการทำงาน
- กรอบการกำกับดูแลข้อมูลของ AIHW มีรายละเอียด ดังนี้
    - กฎหมาย นโยบายที่เกี่ยวข้องกับการกำกับดูแลข้อมูล มีการระบุถึงกฎหมายภายนอกหน่วยงานที่อาจจะเกี่ยวข้องกับการดำเนินการกำกับดูแลข้อมูลของ AIHW นอกจากนี้ยังระบุถึงนโยบายการใช้ข้อมูลของหน่วยงาน
    - โครงสร้างและบทบาทของ AIHW ในการจัดการข้อมูล มีการกำหนดบทบาทที่ชัดเจนภายในหน่วยงาน ตั้งแต่ บอร์ดบริหาร ไปจนถึงบุคลากรที่ทำงานกับข้อมูลโดยตรง รวมไปถึงผู้ตรวจสอบข้อมูล
    - นโยบายข้อมูลและขั้นตอนในการปฏิบัติงาน ระบุถึงการดำเนินงานเกี่ยวกับข้อมูลภายใน AIHW นอกจากนี้ยังได้ระบุถึง Data Linkage ซึ่งระบุถึงการเชื่อมโยงข้อมูลระหว่างหน่วยงาน ว่าต้องมีมาตรฐานตามที่หน่วยงานกลางกำหนด
    - ระบบ AIHW และเครื่องมือเพื่อสนับสนุน ระบุถึงมาตรฐานและเครื่องมือในการกำกับดูแลข้อมูล

โดยสรุปแล้ว การกำกับดูแลข้อมูลของประเทศออสเตรเลียเป็นส่วนสำคัญให้เป็นประเทศที่ติดอันดับ ๑ ใน ๓ ของ Global E-Government Index ทั้งนี้หลายหน่วยงานในประเทศออสเตรเลียมีการเปิดเผยกรอบการกำกับดูแลข้อมูลสู่สาธารณะ ซึ่งสามารถนำไปเป็นแนวทางในการกำหนดกรอบการกำกับดูแลของประเทศไทย

๒.๖.๒ กรณีศึกษาของประเทศเกาหลีใต้

ในการพัฒนาข้อมูลขนาดใหญ่ สำหรับระบบการให้บริการบำเหน็จบำนาญแห่งชาติของประเทศเกาหลีใต้ (National Pension Service of South Korea) (Kim, H. Y., & Cho, J. S., 2017) ได้กำหนดกรอบการกำกับดูแลข้อมูล โดยมี ๔ องค์ประกอบ ดังต่อไปนี้

๑) วัตถุประสงค์ (Objective)

การกำกับดูแลข้อมูลขนาดใหญ่มีความต้องการเพื่อสร้างมูลค่าทางธุรกิจแบบใหม่ ซึ่งจะช่วยให้บริการของข้อมูลขนาดใหญ่สามารถบรรลุเป้าหมาย

๒) ยุทธศาสตร์ (Strategy)

- การคุ้มครองข้อมูลส่วนบุคคล (Personal Information Protection) ได้แก่ นิยามระดับของการคุ้มครองข้อมูลส่วนบุคคลและกำหนดอุปกรณ์สำหรับการคุ้มครองข้อมูลส่วนบุคคล
- ระดับคุณภาพข้อมูล (Data Quality Level) ได้แก่ ความพร้อมใช้ของผลการวิเคราะห์ที่ได้รับจากข้อมูลขนาดใหญ่ ความเชื่อมั่นในผลการวิเคราะห์ ข้อมูลขนาดใหญ่มีความสัมพันธ์กับวัตถุประสงค์ของการวิเคราะห์หรือสิ่งที่ต้องการทำนาย และความสามารถในการผลักดันผลการวิเคราะห์ถูกนำไปใช้ในสถานการณ์จริง

- การเปิดเผยข้อมูลและความรับผิดชอบ (Data Disclosure and Responsibility) ได้แก่ การกำหนดหน้าที่ความรับผิดชอบของเจ้าของข้อมูล การกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการบริหารจัดการข้อมูล และการกำหนดขอบเขตของการเปิดเผยข้อมูล

๓) ส่วนประกอบ (Component)

- โครงสร้างของการบริหารจัดการข้อมูลขนาดใหญ่ (Organization) บุคคลที่อยู่ภายในโครงสร้างนี้มีบทบาทและความรับผิดชอบในการบริหารจัดการข้อมูล การบริหารจัดการความมั่นคงปลอดภัย และการบริหารจัดการคุณภาพข้อมูล
- การจัดทำมาตรฐานและแนวปฏิบัติ (Standardization and Guideline) เช่น แนวปฏิบัติในการกำหนดโครงสร้างข้อมูลและวิธีการประมวลผลข้อมูล
- นโยบายข้อมูลและกระบวนการเกี่ยวกับข้อมูล (Policy and Process) เช่น การควบคุมดูแลและการวัดประสิทธิภาพจากการดำเนินงานเกี่ยวกับข้อมูล

๔) โครงสร้างพื้นฐานด้านเทคโนโนยีสารสนเทศ (IT Infrastructure)

โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศสำหรับข้อมูลขนาดใหญ่ต้องการทรัพยากรด้านการคำนวณ (ซีพียู แรม) และอุปกรณ์แบบใหม่ ในการลงทุนด้านทรัพยากรและอุปกรณ์ต้องมีความเหมาะสมกับระดับการบริการและการบำรุงรักษาที่ได้รับ นอกจากนี้ต้องมีการควบคุมและตรวจความสอดคล้องกันระหว่างการดำเนินการ (ตั้งแต่ การรวบรวมข้อมูล การประมวลผลข้อมูล การวิเคราะห์ข้อมูล และการนำเสนอผลการวิเคราะห์) กับนโยบายข้อมูลที่กำหนดไว้

๒.๖.๓ กรณีศึกษาของสหราชอาณาจักร

สหราชอาณาจักรมีประเทศและหน่วยงานที่ได้ดำเนินการบริหารจัดการข้อมูลและกำกับดูแลข้อมูลดังต่อไปนี้

๑) Scottish Government’s Data Linkage มีการบริหารจัดการข้อมูลของหน่วยงานภาครัฐอย่างมีประสิทธิภาพและมีความน่าเชื่อถือเพื่อประโยชน์ในการบริการสาธารณะในด้าน

- การแลกเปลี่ยนข้อมูลส่วนบุคคลระหว่างหน่วยงานภาครัฐ
- การเชื่อมโยงข้อมูลระหว่างหน่วยงานภาครัฐ
- การเผยแพร่ข้อมูลทั่วไปแก่สาธารณชน
- วิเคราะห์ข้อมูลที่มีอยู่ด้วยวิธีใหม่ ๆ (Data Innovation)

๒) British Academy เน้นการกำกับดูแลข้อมูลของผู้มีส่วนได้ส่วนเสียกับข้อมูลเพื่อ

- การบริหารจัดการข้อมูล
- การจัดการเกี่ยวกับบุคคลที่มีส่วนได้ส่วนเสียกับข้อมูล
- การกำหนดมาตรการและแนวปฏิบัติเกี่ยวข้อง
- การสร้างความโปร่งใสและตรวจสอบได้

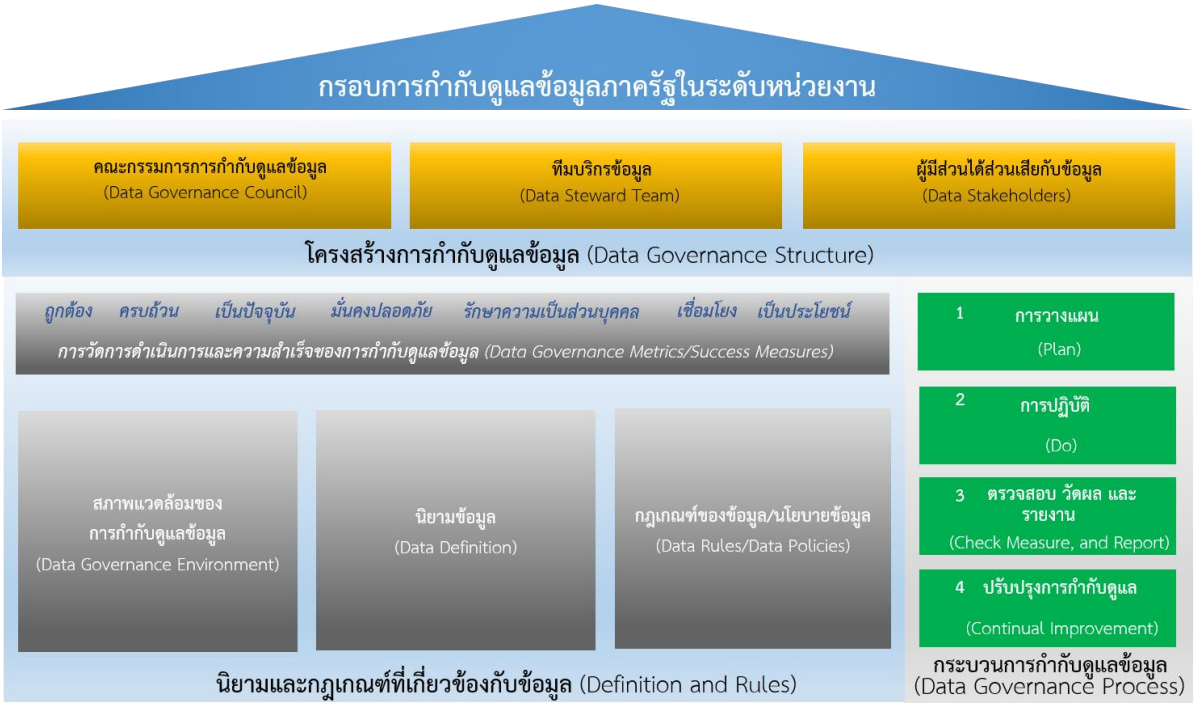
จากผลการศึกษาแนวคิดและกรณีศึกษาจากต่างประเทศสรุปได้ว่า การกำกับดูแลข้อมูลเป็นหนึ่งในองค์ประกอบหลักของการบริหารจัดการข้อมูลเพื่อมุ่งเน้นการลดความเสี่ยง ทั้งด้านความปลอดภัยของข้อมูล

รักษาความเป็นส่วนบุคคล หรือปรับปรุงกระบวนการเพื่อให้ได้ข้อมูลที่มีคุณภาพ สามารถเชื่อมโยง แลกเปลี่ยน เปิดเผยข้อมูลได้

ในบทที่ ๓ จะกล่าวถึงรายละเอียดของกรอบการกำกับดูแลข้อมูล (Data Governance) สำหรับหน่วยงานภาครัฐ ซึ่งมี ๓ องค์ประกอบหลัก ได้แก่ นิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล (Definition and Rules) โครงสร้างการกำกับดูแลข้อมูล (Data Governance Structure) และกระบวนการกำกับดูแลข้อมูล (Data Governance Process)

บทที่ ๓ กรอบการกำกับดูแลข้อมูล (DATA GOVERNANCE FRAMEWORK)

กรอบการกำกับดูแลข้อมูลประกอบด้วยองค์ประกอบต่าง ๆ ผนวกเข้าด้วยกัน ทั้งในด้านของนิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล บุคคล และกระบวนการ ซึ่งองค์ประกอบเหล่านี้มีความสำคัญที่ก่อให้เกิดประสิทธิภาพและประสิทธิผลในการดำเนินงาน อันจะนำไปสู่การบรรลุเป้าหมายในการดำเนินงานตามที่กำหนดไว้ โดยสรุปรายละเอียดดังรูปที่ ๙



รูปที่ ๙ กรอบการกำกับดูแลข้อมูลในระดับหน่วยงาน

จากรูปที่ ๙ แสดงกรอบการกำกับดูแลข้อมูลในระดับหน่วยงาน ประกอบด้วย นิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล (Definition and Rules) โครงสร้างการกำกับดูแลข้อมูล (Data Governance Structure) และกระบวนการกำกับดูแลข้อมูล (Data Governance Process) โดยบุคคลต่าง ๆ ที่เกี่ยวข้องกับโครงสร้างการกำกับดูแลข้อมูลจะถูกแต่งตั้งโดยผู้บริหารระดับสูงของหน่วยงาน เพื่อทำหน้าที่กำหนดยุทธศาสตร์และเป้าหมาย ตรวจสอบสภาพแวดล้อมในการกำกับดูแลข้อมูล นิยามความหมายและขอบเขตของข้อมูล กำหนดกฎเกณฑ์และนโยบายข้อมูล และดำเนินการตรวจสอบการปฏิบัติตามกฎเกณฑ์และนโยบายข้อมูล ดังรายละเอียดต่อไปนี้

๓.๑ สภาพแวดล้อมของการกำกับดูแลข้อมูล (Data Governance Environment)

๓.๑.๑ กฎหมาย ระเบียบ ข้อบังคับ แนวนโยบาย และแนวปฏิบัติ ที่เกี่ยวข้องกับการกำกับดูแลข้อมูล

ปัจจุบันกฎหมายที่เกี่ยวข้องกับข้อมูล ข่าวสาร หรือสิทธิส่วนบุคคลในประเทศไทย มีประเด็นที่อาจส่งผลกระทบต่อหลักแนวคิดการกำกับดูแลข้อมูล ซึ่งหากหน่วยงานในประเทศไทยต้องการสร้างหรือปรับปรุงระบบภายในให้มีการกำกับดูแลข้อมูล จะต้องพิจารณาประเด็นหลัก ๆ ที่เกี่ยวข้องกับกฎหมาย ดังต่อไปนี้

รูปที่ ๑๐ กฎหมาย ระเบียบ ข้อบังคับ แนวนโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล

๑) การเปิดเผยข้อมูล

การเปิดเผยข้อมูลเป็นสิ่งจำเป็นต่อการดำเนินงานของรัฐบาล ซึ่งแสดงความโปร่งใสในการดำเนินงานและความสามารถในการตรวจสอบได้จากภาคเอกชนและประชาชน รวมไปถึงการสนับสนุนให้ภาคเอกชนและประชาชนนำข้อมูลที่เปิดเผยไปสร้างนวัตกรรมผลิตภัณฑ์และบริการเพื่อยกระดับการพัฒนาประเทศ โดยแนวคิดการเปิดเผยข้อมูลเป็นที่ยอมรับของหน่วยงานระหว่างประเทศและรัฐบาลประเทศต่าง ๆ โดยในประเทศไทยมีกฎหมายที่เกี่ยวข้องกับการเปิดเผยข้อมูลดังนี้

- รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. ๒๕๖๐ ในมาตราที่ ๕๙ ได้ระบุว่า รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการ
- พระราชบัญญัติ (พ.ร.บ.) ข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ โดยมี ๓ ประเด็นที่เกี่ยวกับการเปิดเผยข้อมูล ได้ถูกระบุไว้ใน พ.ร.บ. ฉบับนี้ ได้แก่
  - ข้อมูลภาครัฐ ต้อง “เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น”
  - กำหนดหลักเกณฑ์และกลไกการเปิดเผยข้อมูล
  - กำหนดประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้
- แนวทางปฏิบัติการเปิดเผยข้อมูลภาครัฐ (Government Open Data Publication Guidelines) ให้แนวทางปฏิบัติเพื่อการเปิดเผยข้อมูลภาครัฐ ซึ่งมีวัตถุประสงค์เพื่อเป็นแนวปฏิบัติสำหรับการเปิดเผยข้อมูลภาครัฐ[1] ได้แก่
  - แนวปฏิบัติและมาตรฐานเชิงเทคนิค เพื่อให้หน่วยงานภาครัฐนำไปใช้เป็นแนวปฏิบัติในการดำเนินการเกี่ยวกับการเปิดเผยข้อมูลของหน่วยงานให้เป็นไปในทิศทางเดียวกัน รวมถึงการกำหนดมาตรฐานเชิงเทคนิค รูปแบบ วิธีการเผยแพร่

1 https://data.go.th/Documents.aspx

ข้อมูลผ่านศูนย์กลางข้อมูลเปิดภาครัฐ หรือ data.go.th และการกำหนดสัญญาอนุญาต (License) ที่เหมาะสมสำหรับข้อมูลเปิดภาครัฐ

- แบบฟอร์มเมทาดาตา เพื่อเป็นตัวอย่างการจัดทำเมทาดาตา โดยหน่วยงานสามารถนำไปประยุกต์ใช้งานที่เหมาะสมกับหน่วยงานได้
- คู่มือการเปิดเผยข้อมูล (Open Data Handbook) เพื่อสร้างความรู้ ความเข้าใจให้แก่หน่วยงานภาครัฐ ภาคเอกชน และผู้ที่ต้องการศึกษาเกี่ยวกับข้อมูลเปิด (Open Data)
- คู่มือการนำข้อมูลขึ้นเผยแพร่บน data.go.th เพื่อให้ผู้ใช้งานสามารถศึกษาทำความเข้าใจการทำงานต่าง ๆ ของระบบได้ และสามารถตรวจสอบปัญหาที่เกิดจากการใช้งานและสามารถแก้ปัญหาในขั้นต้นได้

- คู่มือแสดงรายการชุดข้อมูลที่สำคัญ เพื่อเป็นการสร้างแหล่งข้อมูลที่ใช้ประกอบในการใช้งานที่เกี่ยวกับชุดข้อมูลที่สำคัญให้แก่หน่วยงานภาครัฐ ภาคเอกชน และผู้ที่ต้องการศึกษาเกี่ยวกับข้อมูลเปิด (Open Data)
- แนวปฏิบัติในการออกแบบความคิดเชิงนวัตกรรม (Data Innovation Guideline) เป็นคู่มือที่ช่วยให้เข้าใจปัญหาที่แท้จริง และสามารถออกแบบแนวทางแก้ไขปัญหาที่เป็นแนวคิดเชิงนวัตกรรมตลอดจนสามารถเข้าถึงชุดข้อมูล (Datasets) ต่าง ๆ เพื่อให้ได้มาซึ่งแนวทางในการแก้ปัญหา นอกจากนั้นผู้ที่ต้องการศึกษากระบวนการออกแบบนวัตกรรมสามารถนำไปประยุกต์หรือปรับใช้กับหน่วยงานได้

๒) การแลกเปลี่ยนข้อมูล

การแลกเปลี่ยนข้อมูลเป็นสิ่งสำคัญต่อการบูรณาการการดำเนินงานระหว่างหน่วยงานภาครัฐ ซึ่งเป็นประโยชน์ต่อหน่วยงานภาครัฐและประชาชนในการขอใช้บริการจากภาครัฐ โดยมีกฎหมายที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูล ดังนี้

- ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน[2] มีวัตถุประสงค์ในการสนับสนุนการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัยและน่าเชื่อถือ รวมทั้งให้ผู้ประกอบการและหน่วยงานต่าง ๆ ได้มีแนวทางในการสร้างเอกสารอิเล็กทรอนิกส์ให้อยู่ในรูปแบบข้อความ XML ให้เป็นมาตรฐานเดียวกัน
- ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยรหัสสถานที่ออกหนังสือ[3] ให้ข้อเสนอแนะสำหรับการกำหนดรหัสสถานที่ออกหนังสือรับรอง ซึ่งจะส่งผลให้ทราบที่มาของหนังสือรับรองและการอำนวยความสะดวกทางการค้า พร้อมการบริหารจัดการ มาตรฐานการแลกเปลี่ยนข้อมูลสารสนเทศด้านการค้าระหว่างประเทศผ่านระบบ National Single Window ให้เป็นไปในทิศทางเดียวกัน

2 https://standard.etda.or.th/wp-content/uploads/2017/08/20170523-ER-eDocumentStandard-V08-14F-0816.pdf

3https://standard.etda.or.th/wp-content/uploads/2017/05/20170526-ER-CertificationLocations-V08-08F-0529.pdf

๓) การคุ้มครองข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคล (Privacy Data Protection) เป็นสิ่งสำคัญที่ภาครัฐต้องดำเนินการ โดยปัจจุบันมีการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย ซึ่งหน่วยงานภาครัฐอาจจะมีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคลของผู้ใช้บริการในรูปของข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการป้องกันการละเมิดข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิขั้นพื้นฐานสำคัญในความเป็นส่วนบุคคล (Privacy Right) ของประชาชนที่ต้องได้รับการคุ้มครอง อันจะทำให้ประชาชนมีความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์ ดังนั้นการคุ้มครองข้อมูลส่วนบุคคลจำเป็นที่จะต้องนำมาวิเคราะห์เพื่อให้เกิดการกำกับดูแลข้อมูลที่ดี โดยมีกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

- พระราชบัญญัติ (พ.ร.บ.) ข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ กำหนดประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้ ซึ่งเป็นสิ่งที่จำเป็นต้องมีการพิจารณาในกรณีที่เป็นข้อมูลส่วนบุคคล เนื่องจากข้อมูลที่เป็นข้อมูลส่วนบุคคลจำเป็นต้องได้รับการคุ้มครองอย่างมีหลักเกณฑ์
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.) เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ได้ระบุเรื่องการคุ้มครองข้อมูลส่วนบุคคลไว้ว่า “กำหนดให้ภาครัฐที่ให้บริการทางอิเล็กทรอนิกส์ต้องมีนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล”
- แนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคลได้ (Guideline to protect the Personally Identifiable Information) ให้แนวปฏิบัติสำหรับหน่วยงานเจ้าของข้อมูลในการดำเนินการเตรียมข้อมูลให้เหมาะสมต่อการบูรณาการข้อมูลเข้าด้วยกัน โดยการนำเสนอขั้นตอนในการดำเนินการปกป้องข้อมูลที่ระบุตัวบุคคลได้ นอกจากนั้นนำเสนอวิธีการเชื่อมโยงข้อมูลแบบรวมชุดข้อมูล (Integrated Datasets) การเชื่อมโยงข้อมูลผ่านตัวแบบข้อมูล (Data Model Market place) และการเชื่อมโยงข้อมูลแบบกลุ่ม (Batch)

๔) การรักษาความลับ

การรักษาความลับทางราชการเป็นสิ่งที่จำเป็นต่อการดำเนินงานของหน่วยงานภาครัฐ ซึ่งเป็นการป้องกันความเสียหายที่จะเกิดขึ้นต่อภาครัฐ ทั้งในด้านชื่อเสียง การเงิน ความสามารถในการพัฒนาประเทศ และความมั่นคงของประเทศ โดยมีกฎหมาย ระเบียบที่เกี่ยวข้องกับการรักษาความลับ ดังนี้

- ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ ได้มีข้อกำหนดที่เกี่ยวข้องกับการกำกับดูแลข้อมูล ได้แก่ กำหนดนิยามข้อมูลข่าวสารลับ และกำหนดหลักเกณฑ์และวิธีการในการรักษาความลับของหน่วยงานภาครัฐ
- แนวทางปฏิบัติในการรักษาความปลอดภัยเกี่ยวกับบุคคล เอกสาร และสถานที่ที่จัดทำขึ้นจากระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ ควรนำมาพิจารณาในการกำกับดูแลข้อมูล

นอกจากการพิจารณากฎหมาย ระเบียบ และข้อบังคับที่มีอยู่ในปัจจุบัน หน่วยงานต้องพิจารณากฎหมาย ระเบียบ นโยบาย หรือ พ.ร.บ. ที่กำลังจะเกิดขึ้นในอนาคตควบคู่ไปกับการกำกับ

ดูแลข้อมูลด้วย ซึ่งกฎหมายที่อยู่ระหว่างการยกร่างที่เกี่ยวข้อง และอาจส่งผลกระทบต่อการกำกับดูแลข้อมูล ดังนี้

๑) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มีการยกร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล โดยมีการกำหนดหลักเกณฑ์ กลไก และมาตรการที่กำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป

๒) มีการยกร่าง พ.ร.บ. ข้อมูลข่าวสารสาธารณะ ขึ้นมาใหม่ โดยจะทำการยกเลิก พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ ซึ่งสาระสำคัญที่เกี่ยวข้องกับการกำกับดูแลข้อมูล คือ มีการกำหนดให้หน่วยงานของรัฐต้องจัดทำช่องทางในการเปิดเผยหรือเข้าถึงข้อมูลข่าวสารสาธารณะ

๓) มีการพิจารณาร่าง พ.ร.บ. ส่งเสริมการประกอบธุรกิจด้วยเทคโนโลยีทางการเงิน (Fin Tech) โดยมีสาระสำคัญ ดังนี้

- ภาคธุรกิจเข้าถึงข้อมูลที่สามารถนำมาวิเคราะห์ วิจัย และพัฒนาผลิตภัณฑ์หรือบริการได้
- อำนวยความสะดวกในการทำธุรกรรมเกี่ยวกับการเงินการลงทุน การเข้าถึงข้อมูล และการพัฒนาเทคโนโลยีทางการเงิน

๔) คณะอนุกรรมการด้านการรักษาความลับของทางราชการทางอิเล็กทรอนิกส์ มีการพิจารณาร่างระเบียบว่าด้วยการรักษาความลับของทางราชการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยออกภายใต้ พ.ร.บ. ข้อมูลข่าวสารราชการ พ.ศ. ๒๕๔๐ โดยเสนอให้มีการเพิ่มกำหนดหลักเกณฑ์และวิธีการในการรักษาความลับด้วยวิธีการทางอิเล็กทรอนิกส์ มีการร่าง พ.ร.บ. ข้อมูลความมั่นคงของรัฐและความลับของทางราชการ เพื่อกำหนดคำนิยามและความหมายของคำว่า “ความมั่นคงของรัฐ” และ “ความลับของทางราชการ” พร้อมกับกำหนดหลักเกณฑ์และเงื่อนไขในการเปิดเผยหรือไม่เปิดเผยข้อมูล

๓.๑.๒ หลักการของสภาพแวดล้อมและวัฒนธรรมของหน่วยงานที่เอื้อต่อการมีการกำกับดูแลข้อมูล

การกำกับดูแลข้อมูลมีองค์ประกอบหลายอย่างที่สนับสนุนให้เกิดการกำกับดูแลข้อมูลที่ดี ในขณะเดียวกันจะต้องคำนึงถึงข้อจำกัดที่อาจส่งผลในเชิงลบต่อการปรับเปลี่ยนหรือปฏิรูปให้เกิดการกำกับดูแลข้อมูลในหน่วยงานด้วย วัฒนธรรมองค์กรและสภาพแวดล้อมเป็นหนึ่งในข้อจำกัดที่อาจส่งผลต่อการเปลี่ยนแปลงในการกำกับดูแลข้อมูลหน่วยงานได้ เนื่องจากแต่ละหน่วยงานล้วนมีวัฒนธรรมองค์กรและสภาพแวดล้อมที่แตกต่างกัน

ดังนั้นการตระหนักถึงวัฒนธรรมองค์กรและสภาพแวดล้อมที่แตกต่างกันมีความจำเป็นต่อการกำหนดโครงสร้าง นโยบาย บทบาทหน้าที่ การดำเนินงานที่เอื้อต่อการกำกับดูแลข้อมูล ตั้งแต่เริ่มต้น นอกจากนี้ยังต้องมีมาตรการรองรับกรณีที่มีการปรับเปลี่ยนโครงสร้างองค์กร เนื่องจากหากมีการปรับเปลี่ยนโครงสร้างองค์กร การกำกับดูแลข้อมูลก็จะเปลี่ยนตามไปด้วย

๓.๒ การนิยามข้อมูล (Data Defnition)

การนิยามข้อมูลต้องมีความถูกต้องและชัดเจน เพื่อสร้างความเข้าใจที่ตรงกันระหว่างผู้ที่เกี่ยวข้อง ทั้งนี้การจัดหมวดหมู่ของข้อมูลทำให้มองเห็นถึงภาพรวมของข้อมูล ขณะที่การทำเมทาดาตาเพื่อสร้างความเข้าใจต่อข้อมูลมากยิ่งขึ้น โดยมีรายละเอียดดังนี้

๓.๒.๑ หมวดหมู่ของข้อมูล (Data Catagory)

ข้อมูลแบ่งออกได้เป็น ๔ หมวดหมู่ ดังนี้

รูปที่ ๑๑ หมวดหมู่ของข้อมูล

๑) ข้อมูลส่วนบุคคล มีนิยามและที่มา ดังต่อไปนี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม (ร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล)

“ข้อมูลข่าวสารส่วนบุคคล” หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงานบรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึก ลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย (พ.ร.บ. ข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐)

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึก ลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลส่วนบุคคลที่มีกฎหมายบัญญัติไว้เป็นการเฉพาะ (ร่าง พ.ร.บ. ข้อมูลข่าวสารสาธารณะ)

จากนิยามข้างต้น จึงได้ข้อสรุปว่า ข้อมูลส่วนบุคคล คือ “ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล ที่ทำให้สามารถระบุตัวหรือรู้ตัวของบุคคลนั้น ๆ ได้ ไม่ว่าจะเป็นข้อมูลการศึกษา ประวัติสุขภาพ ลายพิมพ์นิ้วมือ เป็นต้น”

๒) ข้อมูลความมั่นคง มีนิยามและที่มา ดังต่อไปนี้

มาตรา ๕๙ รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการตามที่กฎหมายบัญญัติ และต้องจัดให้ประชาชนเข้าถึงข้อมูลหรือข่าวสารดังกล่าวได้โดยสะดวก (รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. ๒๕๖๐)

จากนิยามข้างต้น จึงได้ข้อสรุปว่า ข้อมูลความมั่นคง คือ “ข้อมูลเกี่ยวกับความมั่นคงของรัฐที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น”

๓) ข้อมูลความลับทางราชการ มีนิยามและที่มา ดังต่อไปนี้

“ข้อมูลข่าวสารลับ” หมายความว่า ข้อมูลข่าวสารตามมาตรา ๑๔ หรือมาตรา ๑๕ ที่มีคำสั่งไม่ให้เปิดเผยและอยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นเรื่องที่เกี่ยวกับการดำเนินงานของรัฐหรือที่เกี่ยวกับเอกชน ซึ่งมีการกำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือชั้นลับที่สุด ตามระเบียบนี้โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานของรัฐและประโยชน์แห่งรัฐประกอบกัน (ระเบียบว่าด้วยการรักษาความลับของราชการ พ.ศ. ๒๕๔๔)

“สิ่งที่เป็นความลับของทางราชการ” หมายความว่า ข้อมูลข่าวสาร บริภัณฑ์ ยุทธภัณฑ์ ที่สงวน การรหัส ประมวลลับ และสิ่งอื่นใดบรรดาที่ถือว่าเป็นความลับของทางราชการ (ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒)

“ข้อมูลข่าวสารของราชการ” หมายความว่า ข้อมูลข่าวสารที่อยู่ในครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐไม่ว่าจะเป็นข้อมูลข่าวสารเกี่ยวกับเอกชน (ร่าง พ.ร.บ. ข้อมูลข่าวสารสาธารณะ)

จากนิยามข้างต้น จึงได้ข้อสรุปว่า ข้อมูลความลับทางราชการ คือ “ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล”

๔) ข้อมูลสาธารณะ มีนิยามและที่มา ดังต่อไปนี้

มาตรา ๕๙ รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการตามที่กฎหมายบัญญัติ และต้องจัดให้ประชาชนเข้าถึงข้อมูลหรือข่าวสารดังกล่าวได้โดยสะดวก (รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. ๒๕๖๐)

“ข้อมูลข่าวสารสาธารณะ” หมายความรวมถึง ข้อมูลข่าวสารทุกประเภท รวมถึงข้อมูลข่าวสารของราชการ ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ ซึ่งเกี่ยวข้องกับบุคคล องค์กร หรือหน่วยงานที่ดำเนินการใด ๆ โดยใช้ทรัพยากรธรรมชาติ สาธารณสมบัติ งบประมาณแผ่นดิน อำนาจของหน่วยงานรัฐ สิทธิหรือหน้าที่ของหน่วยงานรัฐที่มอบหมายให้เอกชนเป็นผู้ดำเนินการแทนเพื่อประโยชน์สาธารณะ (ร่าง พ.ร.บ. ข้อมูลข่าวสารสาธารณะ)

จากนิยามข้างต้น จึงได้ข้อสรุปว่า ข้อมูลสาธารณะ คือ “ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ เป็นต้น”

๓.๒.๒ เมทาดาตา (Metadata)

เมทาดาตา คือ “ข้อมูลที่ใช้กำกับและอธิบายข้อมูลหลักหรือกลุ่มของข้อมูลอื่น”[4] แบ่งออกเป็น ๒ กลุ่ม ดังนี้

๑) เมทาดาตาเชิงธุรกิจ (Business Metadata) ซึ่งให้รายละเอียดของชุดข้อมูล (Datasets) ในด้านธุรกิจ เหมาะสำหรับผู้ใช้งานข้อมูล (Data User) นักวิเคราะห์ข้อมูล (Data Analyst) และนักวิทยาการข้อมูล (Data Scientist) ตัวอย่างรายการเมทาดาตาเชิงธุรกิจ เช่น ชื่อข้อมูล ชื่อเจ้าของข้อมูล คำสำคัญ คำอธิบายอย่างย่อ วันที่เริ่มต้นใช้งาน วันที่ทำการเปลี่ยนแปลงข้อมูล ภาษาที่ใช้ ชื่อฟิลด์ข้อมูล (ชื่อพนักงาน นามสกุล และเพศ) ในภาคผนวก ก อธิบายเมทาดาตาเชิงธุรกิจ ซึ่งไม่รวมชื่อฟิลด์ข้อมูล เนื่องจากชื่อฟิลด์ข้อมูลของแต่ละชุดข้อมูลมีความแตกต่างกัน

๒) เมทาดาตาเชิงเทคนิค (Technical Metadata) ซึ่งให้รายละเอียดของชุดข้อมูล (Datasets) ในด้านเทคนิค (Technical) และปฏิบัติการ (Operational) เหมาะสำหรับผู้บริหารจัดการฐานข้อมูล (Database Administrator) ตัวอย่างรายการเมทาดาตาเชิงเทคนิค เช่น ชื่อตารางข้อมูลในฐานข้อมูล ชื่อฟิลด์ข้อมูลในตารางข้อมูล ประเภทข้อมูล (ตัวเลข ตัวหนังสือ หรือวันที่) ความกว้างของฟิลด์ข้อมูล (๑๐ ตัวอักษร ๕๐ ตัวอักษร หรือ ๑๐๐ ตัวอักษร) คีย์ข้อมูล (Primary Key หรือ Foreign Key) รวมไปถึงข้อมูลสำหรับการสำรองข้อมูล (Backup) และกู้คืนข้อมูล (Restore)

๓.๒.๓ บัญชีข้อมูล (Data Catalog)

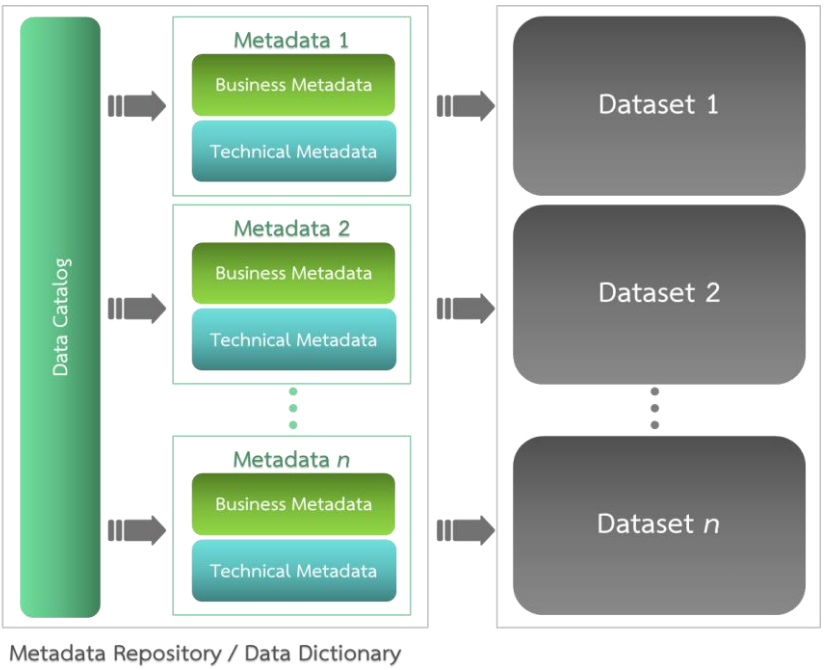
บัญชีข้อมูล คือ “รายการของชุดข้อมูลที่หน่วยงานถือครองหรือบริหารจัดการ” (Australian Institute of Health and Welfare, 2014) ซึ่งรายการของชุดข้อมูลสามารถจัดเตรียมได้ในรูปแบบของตารางรายชื่อชุดข้อมูล รายงาน หรือแอปพลิเคชัน บัญชีข้อมูลถูกใช้เพื่ออำนวยความสะดวกในการค้นหาชุดข้อมูล (Datasets) หรือเมทาดาตา (Metadata) ซึ่งเป็นประโยชน์ต่อผู้ที่เกี่ยวข้องกับข้อมูล เช่น ผู้ใช้งานข้อมูล (Data User) ใช้สำหรับการค้นหาข้อมูลที่ต้องการใช้งาน นักวิเคราะห์ข้อมูล (Data Analyst) และนักวิทยาการข้อมูล (Data Scientist) ใช้สำหรับการค้นหาข้อมูลที่ต้องการวิเคราะห์หรือประมวลผล บริกรข้อมูล (Data Stewards) ใช้สำหรับการค้นหาข้อมูลที่ต้องการตรวจสอบการปฏิบัติตามนโยบายข้อมูล (Data Policy Compliance) คณะกรรมการกำกับดูแลข้อมูล (Data Governance Council) ใช้สำหรับการค้นหาข้อมูลที่ต้องการตัดสินใจหรือแก้ไขปัญหาเกี่ยวกับข้อมูลในระดับนโยบาย

๓.๒.๔ คลังเมทาดาตา (Metadata Repository) หรือพจนานุกรมข้อมูล (Data Dictionary)

คลังเมทาดาตาหรือพจนานุกรมข้อมูลเป็นเครื่องมือในการรวบรวมและจัดเก็บเมทาดาตา เพื่อสนับสนุนให้ผู้ที่ต้องการใช้ข้อมูลสามารถค้นหาและเข้าถึงได้โดยสะดวก อย่างไรก็ตามผู้ที่มีสิทธิในการเข้าถึงควรได้รับสิทธิ์ที่แตกต่างกันขึ้นอยู่กับบทบาทและความรับผิดชอบ เช่น ผู้ใช้งานข้อมูลสามารถเข้าถึงได้เฉพาะเมทาดาตาเชิงธุรกิจ ขณะที่บริกรข้อมูลสามารถเข้าถึงได้ทั้งเมทาดาตาเชิงธุรกิจและเมทาดาตาเชิงเทคนิค โดย

[4] https://data.go.th/~/document/14

ความสัมพันธ์ระหว่างบัญชีข้อมูล เมทาดาตา คลังเมทาดาตา พจนานุกรมข้อมูล และชุดข้อมูล แสดงดังรูปที่ ๑๒



รูปที่ ๑๒ ความสัมพันธ์ระหว่างบัญชีข้อมูล เมทาดาตา คลังเมทาดาตา พจนานุกรมข้อมูล และชุดข้อมูล

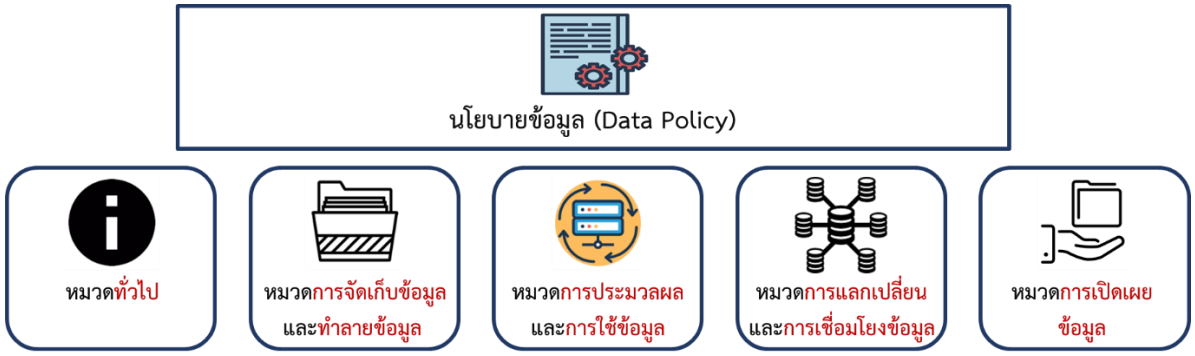
จากรูปที่ ๑๒ บัญชีข้อมูลเปรียบเสมือนสารบัญ เมนู หรือตัวชี้ไปยังเมทาดาตาที่ถูกจัดเก็บอยู่ในคลังเมทาดาตา โดยเมทาดาตาจะให้รายละเอียดต่าง ๆ ที่เกี่ยวข้องกับชุดข้อมูลนั้น ๆ ทั้งนี้คลังเมทาดาตาหรือพจนานุกรมข้อมูลมักจะถูกพัฒนาให้อยู่ในรูปแบบของซอฟต์แวร์

๓.๓ กฎเกณฑ์ข้อมูล (Data Rules)

กฎเกณฑ์ข้อมูลมักจะอ้างถึงนโยบายและมาตรฐานที่เกี่ยวข้องกับข้อมูล โดยนโยบายข้อมูลอธิบายถึงข้อควรปฏิบัติและข้อห้ามปฏิบัติ ขณะที่มาตรฐานข้อมูลอธิบายถึงวิธีการหรือขั้นตอนการปฏิบัติ ดังนั้นในการจัดทำมาตรฐานควรจะมีความสอดคล้องกับนโยบายข้อมูลที่กำหนดไว้ ดังรายละเอียดต่อไปนี้

๓.๓.๑ นโยบายข้อมูล (Data Policies)

การกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในพื้นฐานของการกำกับดูแลข้อมูล ดังนั้นเพื่อให้การกำกับดูแลข้อมูลมีประสิทธิภาพ จึงต้องมีการกำหนดนโยบายที่ระบุอย่างชัดเจน สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง โดยผ่านการอนุมัติจากผู้บริหาร มีการเผยแพร่และสื่อสารให้กับเจ้าหน้าที่และผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน รวมถึงควรมีการทบทวนนโยบายอย่างสม่ำเสมอ เพื่อให้นโยบายข้อมูลได้ถูกนำมาปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง โดยนโยบายข้อมูลควรจะครอบคลุมวงจรชีวิตของข้อมูล ซึ่งอาจจะประกอบไปด้วยนโยบายต่าง ๆ หรือหมวดนโยบาย ทั้งนี้หน่วยงานควรจัดทำนโยบายข้อมูลภายใต้กรอบนโยบายข้อมูล (Data Policy Framework) ดังรายละเอียดต่อไปนี้



รูปที่ ๑๓ นโยบายข้อมูล

๑) หมวดทั่วไป (General Domain)

เพื่อกำหนดนโยบายทั่วไปที่เกี่ยวข้องกับข้อมูล เช่น โครงสร้างที่เกี่ยวข้อง หน้าที่ความรับผิดชอบ โดยมีรายละเอียด ดังนี้

- กำหนดบทบาทและความรับผิดชอบที่ประกอบกันเป็นโครงสร้างการกำกับดูแลข้อมูล โดยต้องได้รับการมอบอำนาจและการอนุมัติจากผู้บริหาร
- กำหนดกลุ่มบุคคลหรือบุคคลภายในหน่วยงาน เพื่อเป็นเจ้าของข้อมูลในการบริหารจัดการข้อมูลของหน่วยงาน เพราะหน่วยงานถือเป็นเจ้าของข้อมูลทุกประเภทที่เกิดจากการดำเนินงานภายในหน่วยงานนั้น ๆ
- กำหนดขอบเขตข้อมูลที่นโยบายข้อมูลครอบคลุม เช่น ข้อมูลที่มีโครงสร้าง (ฐานข้อมูล และ CSV) ข้อมูลกึ่งโครงสร้าง (XML และ JSON) ข้อมูลที่ไม่มีโครงสร้าง (เอกสาร เสียง ภาพ และภาพเคลื่อนไหว)
- กำหนดนโยบาย มาตรการการรักษาความปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับการอนุญาต
- นำระบบเทคโนโลยีสารสนเทศหรือระบบอัตโนมัติมาใช้ในการจัดทำเมทาดาตา
- ตรวจสอบความสอดคล้องกันระหว่างนโยบายข้อมูลกับการดำเนินการใด ๆ ของผู้มีส่วนได้ส่วนเสีย อย่างน้อยปีละ ๑ ครั้ง
- ทบทวนนโยบายข้อมูล อย่างน้อยปีละ ๑ ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่อง หากพบว่านโยบายข้อมูลยังไม่มีประสิทธิภาพเพียงพอ
- สื่อสารและเผยแพร่นโยบายข้อมูลให้กับผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน
- สนับสนุนให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงการกำกับดูแลข้อมูล และการบริหารจัดการข้อมูล โดยให้ครอบคลุมทุกกระบวนการของการบริหารจัดการและวงจรชีวิตของข้อมูล

๒) หมวดการจัดเก็บข้อมูลและทำลายข้อมูล (Data Storage and Destruction Domain)

เพื่อกำหนดนโยบายในการจัดเก็บข้อมูลและทำลายข้อมูลอย่างมีคุณภาพ มีการรักษาความปลอดภัยของข้อมูล โดยมีรายละเอียด ดังนี้

- กำหนดสภาพแวดล้อมของการจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล
- กำหนดชั้นความลับของข้อมูล และจัดเก็บให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Guideline/Standard) ที่กำหนดไว้ เพื่อให้ข้อมูลมีความมั่นคงปลอดภัย และรักษาคุณภาพของข้อมูล
- กำหนดสิทธิ์การเข้าถึงข้อมูล และเครื่องมือที่ใช้ในการเข้าถึงข้อมูล
- จัดเก็บข้อมูลให้สอดคล้องกับความต้องการ และวัตถุประสงค์ในการดำเนินงาน โดยข้อมูลนั้นจะต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบันอยู่เสมอ ทั้งนี้ควรจัดทำเมทาดาตาสำหรับชุดข้อมูลที่มีการจัดเก็บ
- ในกรณีที่มีการร้องขอให้ทำลายข้อมูลส่วนบุคคลจากเจ้าของข้อมูล ผู้ควบคุมหรือหน่วยงานที่จัดเก็บต้องดำเนินการทำลายให้เร็วที่สุด ทั้งนี้ต้องไม่ขัดต่อข้อตกลงระหว่างเจ้าของข้อมูลกับผู้ควบคุม หรือไม่ขัดต่อข้อกฎหมายใด ๆ
- กำหนดแนวทางในการทำลายข้อมูล เมื่อข้อมูลนั้นไม่มีการใช้งานหรือมีการเก็บข้อมูลไว้นานเกินกว่าระยะเวลาที่กำหนด แต่ควรมีการเก็บรักษาเมทาดาตาของข้อมูลที่ทำลายไว้เพื่อใช้สำหรับการตรวจสอบภายหลัง
- สร้างความรู้ความเข้าใจในการจัดเก็บและทำลายข้อมูลแก่ผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน

๓) หมวดการประมวลผลข้อมูลและการใช้ข้อมูล (Data Processing and Use Domain)

เพื่อกำหนดนโยบายในการประมวลผลข้อมูลและการใช้ข้อมูล ให้ได้ข้อมูลที่มีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ โดยมีรายละเอียดดังนี้

- กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูล และทำการสื่อสารให้แก่ผู้ที่เกี่ยวข้องรับทราบ
- การดำเนินการประมวลผลข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ให้เป็นไปตามขอบเขต เงื่อนไข หรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น
- จัดทำเมทาดาตาสำหรับข้อมูลที่จัดเก็บอยู่ในคลังข้อมูล (Data Warehouse)
- ต้องมีการบันทึกประวัติการประมวลผลและการใช้ข้อมูล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

๔) หมวดการแลกเปลี่ยนและการเชื่อมโยงข้อมูล (Data Exchange and Integration Domain)

เพื่อกำหนดนโยบายในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานให้มีความมั่นคงปลอดภัยและข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีรายละเอียด ดังนี้

- กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)
- กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลให้ชัดเจนเริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ
- กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการแลกเปลี่ยนที่จำเป็นให้ครบถ้วน

- ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้
- กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล
- บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้
- สามารถตรวจสอบได้ว่าการแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติ กระบวนการแลกเปลี่ยน และมาตรฐานตามที่กำหนด

๕) หมวดการเปิดเผยข้อมูล (Data Disclosure Domain)

เพื่อกำหนดนโยบายในการเปิดเผยข้อมูล เพื่อให้สามารถเปิดเผยข้อมูลได้อย่างถูกต้องตรงตามวัตถุประสงค์ของการให้นำข้อมูลไปใช้ประโยชน์ โดยมีรายละเอียด ดังนี้

- ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม
- ต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล
- ควรมีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย
- ควรมีการเปิดเผยเมทาดาตาควบคู่ไปกับข้อมูลที่เปิดเผย
- สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล

๓.๓.๒ มาตรฐานข้อมูล (Data Standards)

มาตรฐานข้อมูลอ้างถึงมาตรฐานที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและการใช้ข้อมูล ซึ่งเป็นกลไกอย่างหนึ่งในการกำกับดูแลข้อมูล มีวัตถุประสงค์เพื่อสร้างความเข้าใจที่ตรงกัน และลดความหลากหลายของวิธีการปฏิบัติ เช่น มาตรฐานเมทาดาตา (Metadata Standard) มาตรฐานชุดข้อมูล (Datasets Standard) มาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Standard)

มาตรฐานเมทาดาตา (Metadata Standard) คือ การกำหนดรูปแบบและข้อกำหนดของเมทาดาตาเพื่อให้สามารถเข้าใจได้ถูกต้องตรงกันตลอดทั้งหน่วยงาน ISO/IEC 11179 และ Dublin Core Metadata Initiative (DCMI)[5] ได้กำหนดมาตรฐานเมทาดาตาสำหรับอธิบายชุดข้อมูล เช่น ชื่อข้อมูล ชื่อเจ้าของข้อมูล คำอธิบายข้อมูล ขอบเขตการจัดเก็บ รูปแบบข้อมูล ภาษา สิทธิการเข้าถึง ทั้งนี้มาตรฐานเมทาดาตามักจะอ้างถึงทั้งเมทาดาตาเชิงธุรกิจและเมทาดาตาเชิงเทคนิค แต่มักจะไม่รวมองค์ประกอบของฟิลด์ข้อมูลซึ่งเป็นคุณลักษณะเฉพาะของแต่ละชุดข้อมูล

มาตรฐานชุดข้อมูล (Datasets Standard) คือ การกำหนดรูปแบบและข้อกำหนดของข้อมูลที่มีการใช้ร่วมกันจากหลาย ๆ ส่วนงานหรือหน่วยงาน เพื่อลดความซ้ำซ้อนของข้อมูล ลดความยุ่งยากในการบริหารจัดการ และสนับสนุนให้ข้อมูลมีคุณภาพ ซึ่งส่วนงานหรือหน่วยงานต้องร่วมกันกำหนดเมทาดาตาขึ้นมาเพื่ออธิบายคุณลักษณะของชุดข้อมูลที่ใช้ร่วมกัน แล้วดำเนินการบูรณาการข้อมูล (Data Integration) ที่กระจายอยู่ตามส่วนงานหรือหน่วยงานต่าง ๆ เข้าด้วยกัน มาตรฐานชุดข้อมูลมักจะอธิบายถึงองค์ประกอบของฟิลด์

[5] http://dublincore.org/documents/dcmi-terms/

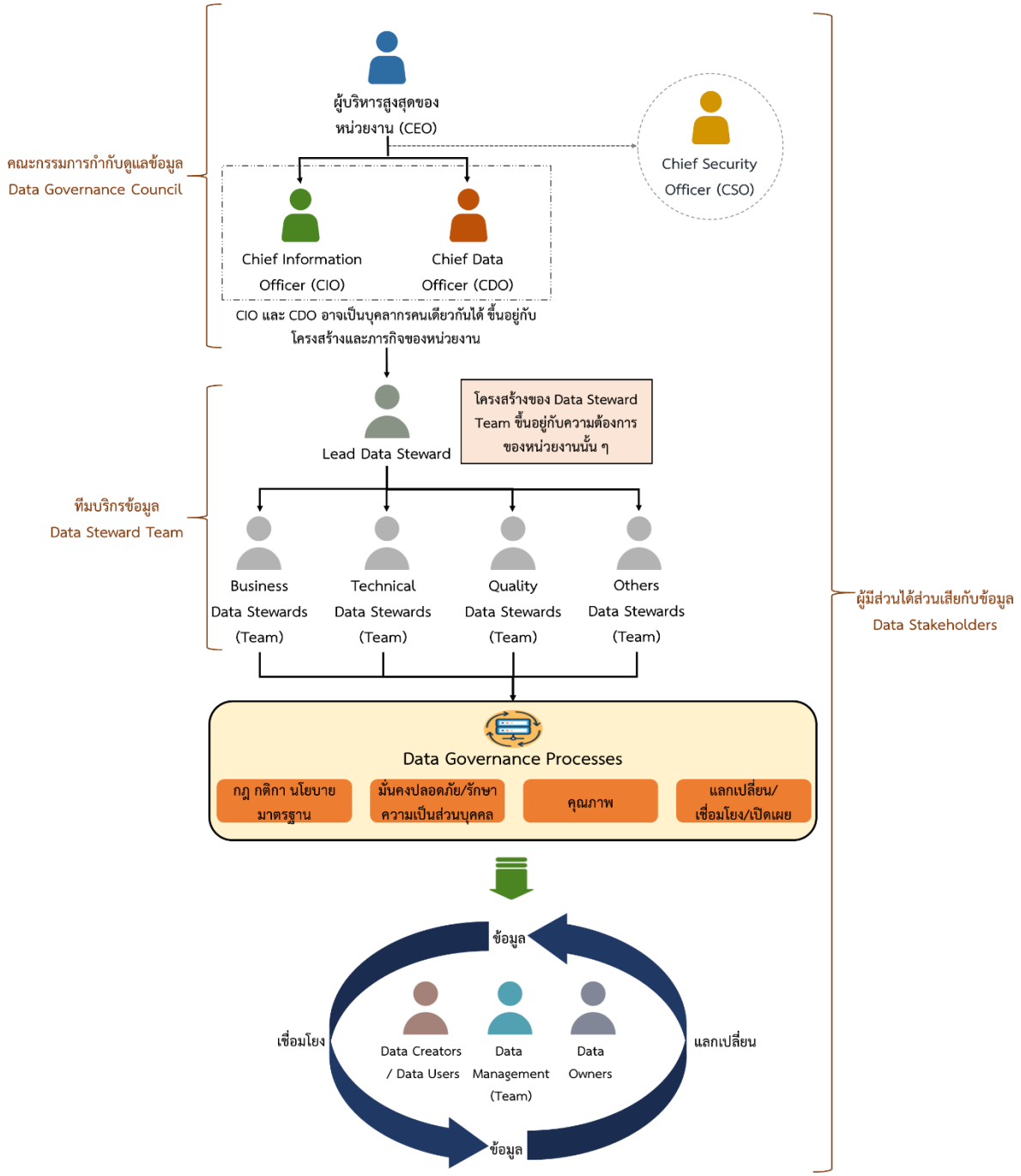
ข้อมูล เช่น ชื่อฟิลด์ข้อมูล ประเภทข้อมูล (ตัวเลข ตัวหนังสือ และวันที่) ช่วงค่าของข้อมูล และการอนุญาตให้ฟิลด์ข้อมูลเป็นค่าว่าง

มาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Standard) คือ การกำหนดรูปแบบและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อป้องกันการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ชั้นความลับของข้อมูลมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของประเทศ ตัวอย่างชั้นความลับ ได้แก่ ลับที่สุด ลับมาก ลับ ใช้ภายในหน่วยงาน และเปิดเผยได้ ตัวอย่างประเภทของผลกระทบ ๑) ด้านชื่อเสียง เช่น ข้อมูลในเชิงลบของหน่วยงานถูกเปิดเผยส่งผลให้หน่วยงานหรือประเทศเสียชื่อเสียง ๒) ด้านความต่อเนื่องของการดำเนินการ เช่น ข้อมูลระบบเครือข่ายถูกเปิดเผยทำให้ระบบเครือข่ายหรือระบบอินเทอร์เน็ตถูกโจมตี ซึ่งส่งผลให้การดำเนินงานของหน่วยงานหยุดชะงักหรือล่าช้า ๓) ด้านการเงิน เช่น ข้อมูลบัตรเครดิตในหน่วยงานถูกเปิดเผย ทำให้สูญเสียงบประมาณของหน่วยงาน ๔) ด้านทรัพยากรบุคคล เช่น ข้อมูลเงินเดือนถูกเปิดเผย ส่งผลให้บุคลากรคนสำคัญต้องลาออก

๓.๔ โครงสร้างของการกำกับดูแลข้อมูล (Data Governance Structure)

๓.๔.๑ โครงสร้างของบุคลากรที่รับผิดชอบในการกำกับดูแลข้อมูล (Data Governance Structure)

การกำหนดโครงสร้างการกำกับดูแลข้อมูลเพื่อแสดงลำดับขั้นระหว่างกลุ่มบุคคลที่เกี่ยวข้องกับการกำกับดูแลข้อมูล และแสดงถึงสิทธิ์ในการสั่งการตามลำดับขั้น ทั้งนี้จำนวนบุคลากรและความลึกของลำดับขั้นให้พิจารณาตามความเหมาะสมของแต่ละหน่วยงาน ทั้งนี้หน่วยงานสามารถจัดตั้งส่วนงานกำกับดูแลข้อมูลในรูปแบบที่แตกต่างกัน ได้แก่ ๑) รูปแบบทีมเสมือน (Virtual Team) ที่คัดเลือกมาจากส่วนงานต่าง ๆ ๒) รูปแบบที่มีส่วนงานรับผิดชอบชัดเจนซึ่งอาจจะจัดตั้งใหม่หรือกำหนดหน้าที่ให้กับส่วนงานที่มีหน้าที่คล้ายกับโครงสร้าง และ ๓) รูปแบบผสมซึ่งจะต้องแยกหน้าที่ให้ชัดเจนระหว่างส่วนงานที่รับผิดชอบหลักกับทีมเสมือน รูปที่ ๑๔ แสดงตัวอย่างโครงสร้างการกำกับดูแลข้อมูล ซึ่งแบ่งออกเป็น ๓ ส่วน ประกอบด้วย ๑) คณะกรรมการกำกับดูแลข้อมูล (Data Governance Council) ๒) ทีมบริกรข้อมูล (Data Steward Team) และ ๓) ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholder)



รูปที่ ๑๔ ตัวอย่างโครงสร้างการกำกับดูแลข้อมูลภายในหน่วยงาน

คณะกรรมการกำกับดูแลข้อมูล (Data Governance Council) ประกอบไปด้วย ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) ผู้บริหารด้านการรักษาความปลอดภัยระดับสูง (Chief Security Officer) ผู้บริหารจากส่วนงานต่าง ๆ ทั้งจากฝ่ายบริหารและฝ่ายเทคโนโลยีสารสนเทศ รวมไปถึงหัวหน้าทีมบริกรข้อมูล (Lead Data Steward) คณะกรรมการกำกับดูแลข้อมูลมีอำนาจสูงสุดในการกำกับดูแลข้อมูลภายในหน่วยงาน ซึ่งทำหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการภายในคณะกรรมการกำกับดูแลข้อมูล ทั้งนี้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงอาจจะทำหน้าที่แทนผู้บริหารข้อมูลระดับสูง ซึ่งขึ้นอยู่กับความพร้อมของหน่วยงาน

ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) มีหน้าที่นำข้อมูลและวิเคราะห์ข้อมูลของหน่วยงานเพื่อสร้างและส่งมอบเทคโนโลยี เครื่องมือ แนวทาง และวิธีการในการทำให้ข้อมูลของหน่วยงานมีคุณค่า และเกิดประโยชน์สูงสุดต่อหน่วยงาน เพื่อขยายผลต่อไปให้เกิดผลสัมฤทธิ์ในการส่งเสริมให้หน่วยงานภาครัฐต่าง ๆ ใช้ข้อมูลได้อย่างถูกต้องและมีประสิทธิภาพ นอกจากนี้ยังต้องวิเคราะห์และร่วมกับผู้บริหารส่วนอื่น ๆ เพื่อจัดทำยุทธศาสตร์และดำเนินการกำกับดูแลข้อมูลคุณภาพและการควบคุมอื่น ๆ เพื่อรักษาความสมบูรณ์ของข้อมูลของหน่วยงาน และนำแนวปฏิบัติและมาตรฐานของหน่วยงานไปปรับปรุงข้อมูลและยุทธศาสตร์ของประเทศ โดยในส่วนของการทำงานในระดับประเทศ ผู้บริหารข้อมูลระดับสูง จะต้องทำหน้าที่เป็นตัวกลางระหว่างหน่วยงานภาครัฐในการแลกเปลี่ยน เชื่อมโยงข้อมูล รวมไปถึงการจัดการความเสี่ยงที่อาจเกิดจากข้อมูลของหน่วยงานภาครัฐ รวมถึงส่งเสริมนวัตกรรมที่ใช้ประโยชน์จากข้อมูลในการวิเคราะห์ปัญหาเพื่อแก้ไขจนสามารถลดปัญหาของประเทศที่เกิดขึ้นในปัจจุบัน และลดความเสี่ยงของปัญหาที่อาจเกิดขึ้นในอนาคตได้ พร้อมทั้งต้องวิเคราะห์หาเทคโนโลยีใหม่ ๆ มาใช้ในการวิเคราะห์ข้อมูลให้ตอบสนองความต้องการของประชาชนด้วย

ในบางหน่วยงาน กรณีที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงมีหน้าที่และความรับผิดชอบใกล้เคียงหรือสามารถทำหน้าที่ของผู้บริหารข้อมูลระดับสูงได้ ดังนั้นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และผู้บริหารข้อมูลระดับสูงจึงสามารถเป็นบุคคลเดียวกันได้

ผู้บริหารด้านการรักษาความปลอดภัยระดับสูง (Chief Security Officer) เป็นผู้บริหารที่มีบทบาทสูงสุดในการทำให้หน่วยงานมีความปลอดภัยเพียงพอสำหรับการทำงานทั้งด้านการบริหารจัดการดูแล และด้านข้อมูล ทำให้เกิดการเชื่อมต่อระหว่างหน่วยงาน ตัวอย่างเช่น หน่วยงานไม่มีความกังวลเกี่ยวกับช่องโหว่ด้านความปลอดภัย ทำให้การทำงานของหน่วยงานเป็นไปได้อย่างราบรื่น ดังนั้นการมีผู้บริหารด้านการรักษาความปลอดภัยระดับสูงที่ดี สามารถลดความหวาดระแวงในการทำงานระหว่างส่วนงานต่าง ๆ ทำให้เพิ่มมูลค่าให้กับหน่วยงานได้ ดังนั้นหน้าที่หลักของผู้บริหารด้านการรักษาความปลอดภัยระดับสูง คือ การปรับปรุงความมั่นคงทางกายภาพและความปลอดภัยด้านเทคโนโลยีให้มากขึ้น รวมถึงต้องมีทำงานร่วมกับผู้บริหารอื่น ๆ ในการตัดสินใจเกี่ยวกับลำดับความสำคัญของความต้องการด้านความปลอดภัย เพื่อกำหนดเป้าหมายและวัตถุประสงค์ของการป้องกันหน่วยงานเพื่อให้สอดคล้องกับแผนกลยุทธ์ของหน่วยงาน นอกจากนี้ยังต้องดูแลเครือข่ายของคณะกรรมการ ผู้บริหาร ผู้จัดการ และเจ้าหน้าที่รักษาความปลอดภัยและทำงานร่วมกับหน่วยงานด้านความมั่นคงในท้องถิ่น และหน่วยงานรักษาความปลอดภัยอื่น ๆ

ทีมบริกรข้อมูล (Data Steward Team) ประกอบไปด้วย หัวหน้าบริกรข้อมูล (Lead Data Steward) บริกรข้อมูลด้านธุรกิจ (Business Data Stewards) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) บริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards) รวมไปถึงบุคคลที่ทำหน้าที่เกี่ยวกับความมั่นคงปลอดภัย กฎหมาย และบุคคลที่ให้ความรู้เกี่ยวกับนโยบายข้อมูลและความรู้อื่น ๆ ที่จะสนับสนุนให้เกิดการกำกับดูแลข้อมูลที่ดีภายในหน่วยงาน ทีมบริกรข้อมูลรับคำสั่งโดยตรงจากคณะกรรมการกำกับดูแลข้อมูล ในขณะเดียวกันมีการให้ข้อมูลสนับสนุนในการตัดสินใจต่อคณะกรรมการกำกับดูแลข้อมูล โดยบริกรข้อมูลด้านธุรกิจเป็นผู้ให้การสนับสนุนด้านธุรกิจ ขณะที่บริกรข้อมูลด้านเทคนิคเป็นผู้ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศ อย่างไรก็ตามบริกรข้อมูลด้านธุรกิจและบริกรข้อมูลด้านเทคนิคอาจจะเป็นบุคคลเดียวกัน ซึ่งขึ้นอยู่กับคุณสมบัติของบุคคลหรือความเหมาะสมของหน่วยงาน

หัวหน้าบริกรข้อมูลทำหน้าที่เป็นผู้ควบคุมและสั่งการภายในทีมบริกรข้อมูล และเป็นหนึ่งในคณะกรรมการกำกับดูแลข้อมูล

นอกเหนือจากคณะกรรมการกำกับดูแลข้อมูลและทีมบริกรข้อมูล ยังมีผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders) อื่น ๆ ซึ่งทำหน้าที่ให้การสนับสนุนการกำกับดูแลข้อมูลต่อทีมบริกรข้อมูลและคณะกรรมการกำกับดูแลข้อมูล ประกอบไปด้วย เจ้าของข้อมูล (Data Owners) ทีมบริหารจัดการข้อมูล (Data Management Team) ผู้สร้างข้อมูล (Data Creators) และผู้ใช้ข้อมูล (Data Users) สำหรับรายละเอียดของบทบาทและความรับผิดชอบภายในโครงสร้างการกำกับดูแลข้อมูลได้แสดงไว้ในหัวข้อถัดไป

๓.๔.๒ บทบาทและความรับผิดชอบ (Roles and Responsibilities)

บทบาท (Roles) และความรับผิดชอบ (Responsibilities) ที่เหมาะสมจะนำไปสู่การดำเนินงานที่มีประสิทธิภาพและประสิทธิผลต่อหน่วยงาน ซึ่งการกำหนดบทบาทและความรับผิดชอบจะต้องไม่ขัดแย้งต่อกฎระเบียบ ข้อบังคับ หรือกฎหมาย มีรายละเอียด ดังนี้

ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) และผู้บริหารข้อมูลระดับสูง (Chief Data Officer) คือ บุคคลที่ทำหน้าที่ กำหนดวิสัยทัศน์ ให้ข้อเสนอแนะ และอนุมัตินโยบายข้อมูล มาตรฐานข้อมูล แนวทางปฏิบัติงาน เกณฑ์การวัดคุณภาพ ระเบียบ และข้อบังคับอื่น ๆ ที่เกี่ยวข้องกับข้อมูล รวมไปถึงการจัดลำดับความสำคัญและแก้ไขปัญหาที่เกี่ยวข้องกับข้อมูล

บริกรข้อมูลด้านธุรกิจ (Business Data Stewards) คือ บุคคลที่ทำหน้าที่รับผิดชอบในการ นิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัยซึ่งอาจจะได้รับมาจากผู้ใช้ข้อมูล (Data Users) หรือผู้มีส่วนได้ส่วนเสียอื่น ๆ นิยามเมทาดาตาโดยการสนับสนุนจากผู้ใช้ข้อมูล สถาปนิกข้อมูล (Data Architects) และนักวิเคราะห์ระบบ (System Analyst) ร่างนโยบายข้อมูลด้วยการช่วยเหลือจากทีมบริหารจัดการข้อมูล (Data Management Team) ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ แล้วรายงานผลลัพธ์ไปยังคณะกรรมการกำกับดูแลข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ ให้ทราบ บริกรข้อมูลด้านธุรกิจมักจะเป็นบุคคลที่มาจากฝ่ายธุรกิจแต่มีความเข้าใจด้านเทคโนโลยีสารสนเทศ

บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) คือ บุคคลที่ทำหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูลด้านธุรกิจ เช่น นิยามเมทาดาตาเชิงเทคนิคซึ่งอาจจะได้รับการช่วยเหลือจากทีมบริหารจัดการข้อมูล ให้ข้อเสนอแนะเชิงเทคนิคในการร่างนโยบายข้อมูล ตรวจสอบคุณภาพข้อมูล ความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามนโยบายข้อมูลในเชิงเทคนิค ทั้งนี้บริกรข้อมูลด้านเทคนิคมักจะเป็นบุคคลฝ่ายเทคโนโลยีสารสนเทศแต่ที่มีความเข้าใจเกี่ยวกับธุรกิจ

บริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards) คือ บุคคลที่ทำหน้าที่ดำเนินการในเรื่องคุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูล และการวิเคราะห์คุณภาพข้อมูล นอกจากนี้หน่วยงานอาจจะกำหนดบริกรข้อมูลด้านอื่น ๆ เพื่อดูแลเรื่องต่าง ๆ โดยเฉพาะ เช่น บริกรข้อมูลด้านความมั่นคงปลอดภัย บริการข้อมูลด้านการอบรมและให้ความรู้

เจ้าของข้อมูล (Data Owners) คือ บุคคลที่ทำหน้าที่ตรวจสอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย เจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตาและเกณฑ์การทำความสะอาดข้อมูล (Data Cleansing) นอกจากนี้ยังหน้าที่ในการให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล เจ้าของข้อมูลมักจะอยู่ในตำแหน่งบริหาร เช่น ผู้อำนวยการฝ่ายหรือหัวหน้าส่วนงานบุคคลเป็นเจ้าของข้อมูลบุคคล ผู้อำนวยการฝ่ายหรือหัวหน้าส่วนงานการเงินเป็นเจ้าของข้อมูลการเงิน

ทีมบริหารจัดการข้อมูล (Data Management Team) มีหน้าที่หลักในการบริหารจัดการข้อมูลสอดคล้องกับ ๑๐ องค์ประกอบ ตามรายละเอียดในหัวข้อ ๒.๓.๒ องค์ประกอบในการบริหารจัดการข้อมูล ซึ่งมักจะเป็นเจ้าหน้าที่ภายในฝ่ายเทคโนโลยีสารสนเทศของหน่วยงาน ประกอบด้วย สถาปนิกข้อมูล (Data Architects) นักจัดการฐานข้อมูล (Database Administrators - DBA) นักวิเคราะห์ (Data Analysts) และนักวิทยาการข้อมูล (Data Scientists) ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ทีมบริหารจัดการข้อมูลสนับสนุนกิจกรรมของการกำกับดูแลข้อมูล เช่น ช่วยเหลือในการนิยามเมทาดาตา ร่างนโยบายข้อมูลและมาตรฐานข้อมูล และกำหนดสิทธิการเข้าถึงข้อมูลโดย DBA

ผู้สร้างข้อมูล (Data Creators) คือ บุคคลที่ทำหน้าที่ บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ นอกจากนี้ยังมีหน้าที่ในการทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย

ผู้ใช้ข้อมูล (Data Users) คือ บุคคลที่ทำหน้าที่นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร และสนับสนุนการกำกับดูแลข้อมูลโดยการให้ความต้องการในการใช้ข้อมูล พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังบริกรข้อมูล

๓.๕ กระบวนการกำกับดูแลข้อมูล (Data Governance Process)

หลักพื้นฐานของการกำหนดกระบวนการและผลที่ได้รับ ประกอบด้วย การเลือกข้อมูลเพื่อดำเนินการกำกับดูแล การระบุเป้าหมาย การกำหนดมาตรฐานและแนวปฏิบัติ รวมถึงการบริหารจัดการคน

๑) การเลือกข้อมูลเพื่อดำเนินการกำกับดูแล ได้แก่ ข้อมูลส่วนบุคคล ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ และข้อมูลสาธารณะ โดยกระบวนการซึ่งได้มาด้วยข้อมูลนั้นสามารถใช้วิธีการ เช่น กระบวนการย้อนกลับทางวิศวกรรม (Reverse Engineer) การวิเคราะห์ข้อมูล (Data Analysis) การสำรวจข้อมูล (Survey)

๒) การระบุเป้าหมาย ต้องพิจารณาครอบคลุมในประเด็นดังต่อไปนี้เป็นอย่างน้อย คือ คุณภาพข้อมูล การเข้าถึงและการจัดการ ความปลอดภัยและความเป็นส่วนตัว การปฏิบัติตามระเบียบและกฎหมาย ต้นทุนและประสิทธิภาพ

๓) การกำหนดมาตรฐานและแนวปฏิบัติ เป็นการกำหนดมาตรฐานโดยทั่วไป แนวทางที่ใช้ เช่น การตั้งชื่อ คุณภาพของข้อมูล การโอนย้ายข้อมูล กระบวนที่เกี่ยวข้องกับข้อมูล (Create Read Update Delete – CRUD) การเก็บข้อมูลถาวร (Archive)

๔) การบริหารจัดการคน เช่น การสร้างวัฒนธรรมองค์กร การบริหารจัดการแรงต้าน การสื่อสารที่ชัดเจน การสร้างความพึงพอใจกับผู้ที่มีส่วนได้ส่วนเสีย การใช้ประโยชน์จากเทคโนโลยี ซึ่งจะช่วยให้การดำเนินงานสำเร็จลุล่วงได้ดี

๓.๕.๑ กระบวนการกำกับดูแลข้อมูล (Data Governance Process)

กระบวนการกำกับดูแลข้อมูล (Data Governance Process) เป็นขั้นตอนที่ใช้สำหรับกำกับดูแลการการดำเนินการใด ๆ ต่อข้อมูลให้เป็นไปตาม กฎ ระเบียบ ข้อบังคับ หรือนโยบายที่เกี่ยวข้องกับข้อมูล กระบวนการกำกับดูแลข้อมูลเริ่มตั้งแต่การวางแผนไปจนถึงการปรับปรุงอย่างต่อเนื่อง ดังรายละเอียดต่อไปนี้

รูปที่ ๑๕ กระบวนการกำกับดูแลข้อมูล

๑) การวางแผน (Plan)

การวางแผนเริ่มตั้งแต่กำหนดวิสัยทัศน์และประเด็นปัญหา ซึ่งเป็นส่วนที่สำคัญเนื่องจากเป็นจุดเริ่มต้นที่จะกำหนด กฎระเบียบ นโยบาย มาตรฐาน หรือแนวทางปฏิบัติต่างๆ เพื่อใช้ในการกำกับดูแลและการบริหารจัดการข้อมูล หลังจากที่ได้มีการกำหนดวิสัยทัศน์และประเด็นปัญหาที่ชัดเจนแล้ว ขั้นตอนถัดไปคือการกำหนดขอบเขตการดำเนินการ ระยะเวลาดำเนินการ บุคคลที่เกี่ยวข้อง และต้นทุนที่ใช้ในการดำเนินงาน หลังจากนั้นนำแผนงาน กฎระเบียบ และนโยบายที่เกี่ยวข้องไปประกาศใช้อย่างเป็นทางการ

๒) การปฏิบัติ (Do)

การปฏิบัติในที่นี้อ้างถึงการดำเนินการใด ๆ ของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ เช่น สถาปนิกข้อมูล นักออกแบบข้อมูล นักจัดการฐานข้อมูล วิศวกรข้อมูล นักวิเคราะห์ข้อมูล นักวิทยาการข้อมูล เจ้าของข้อมูล ผู้สร้างข้อมูล ผู้บริหาร ผู้ใช้ข้อมูล ซึ่งต้องดำเนินการให้สอดคล้องกับ กฎระเบียบ นโยบาย มาตรฐาน และแนวปฏิบัติที่ได้กำหนดไว้ ขณะที่บริกรข้อมูลจะให้ความรู้และสนับสนุนให้บุคคลที่เกี่ยวข้องสามารถปฏิบัติตามกฎระเบียบเหล่านั้น ทั้งนี้รายงานความก้าวหน้า ผลการปฏิบัติงาน และประเด็นปัญหาที่พบระหว่างปฏิบัติงานจะถูกรายงานไปยังคณะกรรมการกำกับดูแลข้อมูล

๓) การตรวจสอบ วัดผล และรายงาน (Check, Measure, and Report)

ในการตรวจสอบ บริกรข้อมูลจะดำเนินการตรวจสอบความสอดคล้องกันระหว่างกฎระเบียบ นโยบาย และมาตรฐานที่กำหนด กับการปฏิบัติงานของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ พร้อมทั้งทำการวัดผลด้านคุณภาพข้อมูล หลังจากนั้นรายงานผลความสอดคล้อง คุณภาพข้อมูล ความมั่นคงปลอดภัย และความเสี่ยงที่เกี่ยวข้องกับข้อมูลไปยังคณะกรรมการกำกับดูแลข้อมูลและผู้ที่เกี่ยวข้อง เพื่อให้ทราบถึงผลการดำเนินงานและประเด็นปัญหาที่พบ

๔) การปรับปรุงอย่างต่อเนื่อง (Continuous Improvement)

การกำกับดูแลข้อมูลเป็นสิ่งที่ต้องดำเนินการอย่างต่อเนื่องตลอดวงจรชีวิตของข้อมูล ทั้งนี้สภาพแวดล้อมหรือกฎหมายที่เปลี่ยนแปลง รายการความต้องการจากผู้บริหารและผู้มีส่วนได้ส่วนเสีย รวมไปถึงผลการตรวจสอบ เช่น รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัย รายงานความเสี่ยงต่อข้อมูล จะถูกใช้สำหรับการปรับปรุงกระบวนการกำกับดูแลข้อมูล นโยบาย กฎ ระเบียบข้อบังคับที่เกี่ยวข้องกับข้อมูล เกณฑ์การประเมินความพร้อมของการกำกับดูแลข้อมูล เกณฑ์การวัดระดับคุณภาพข้อมูล และโครงสร้างการกำกับดูแลข้อมูล

๓.๕.๒ แนวทางการจัดการกระบวนการกำกับดูแลข้อมูล (Data Governance Process Guidelines)

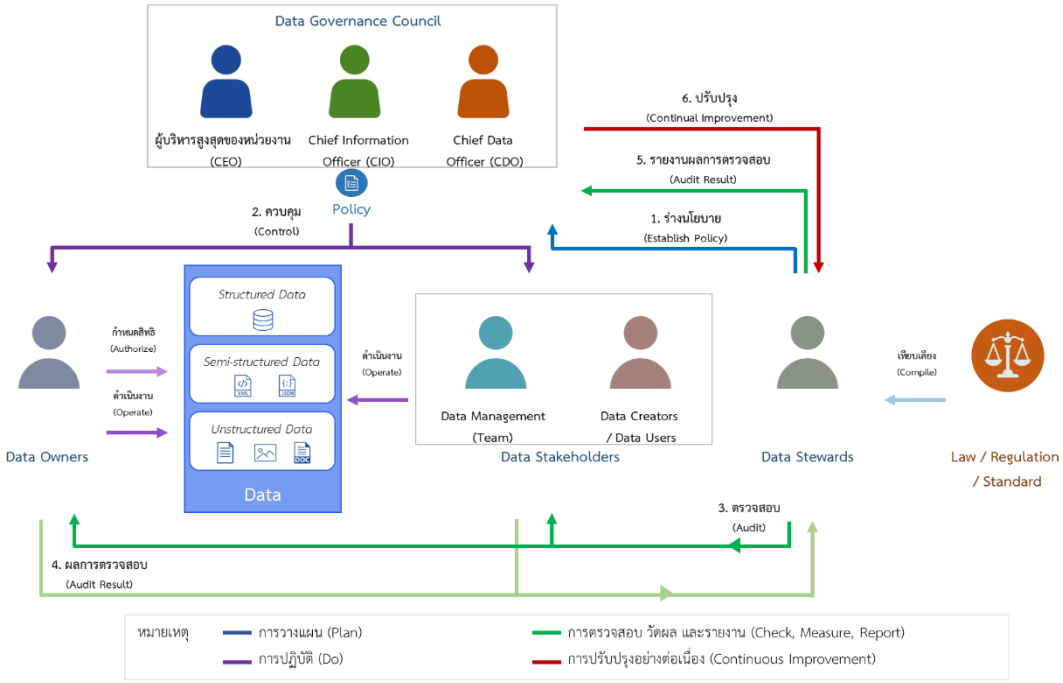
แนวทางการจัดการกระบวนการกำกับดูแลข้อมูลจะช่วยให้เข้าใจถึงกระบวนการและสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ ซึ่งชี้ให้เห็นถึงความสัมพันธ์ระหว่างกระบวนการกำกับดูแล เครื่องมือหรือเอกสารที่ใช้ในการกำกับดูแล ผลลัพธ์ที่ได้จากการกำกับดูแล และผู้ที่เกี่ยวข้องหรือผู้มีส่วนได้ส่วนเสีย ดังแสดงในตารางที่ ๑๔ แสดงตัวอย่างแผนภาพการดำเนินการกำกับดูแลข้อมูล ดังแสดงในรูปที่ ๑๖ และแสดงความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย ดังแสดงในตารางที่ ๑๕

ตารางที่ ๑๔ ความสัมพันธ์ระหว่างกระบวนการ ส่วนนำเข้า ส่วนนำออก และผู้มีส่วนได้ส่วนเสีย

กระบวนการ (Processes)	ส่วนนำเข้า (Input)	ส่วนนำออก (Output)	ผู้มีส่วนได้ส่วนเสีย (Data Stakeholder)
๑ การวางแผน	(๑) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (๒) รายการชุดข้อมูล (๓) รายการประเด็นปัญหาจากรายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล	(๑) แผนดำเนินการ (ขอบเขต เวลา กลุ่มกำกับดูแลข้อมูล และต้นทุน)	(๑) ผู้บริหารข้อมูลระดับสูงหรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (๒) คณะกรรมการกำกับดูแลข้อมูล (๓) บริกรข้อมูลด้านธุรกิจ (๔) บริกรข้อมูลด้านเทคนิค (๕) บริกรข้อมูลด้านคุณภาพ
๒ การปฏิบัติ	(๑) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (๒) แผนดำเนินการ (ขอบเขต เวลา กลุ่มกำกับดูแลข้อมูล และต้นทุน)	(๑) รายงานความก้าวหน้าในการปฏิบัติงาน (๒) ผลการปฏิบัติงาน (๓) ประเด็นปัญหาที่พบระหว่างปฏิบัติงาน	(๑) ผู้บริหารงาน (๒) ผู้ปฏิบัติงานที่เกี่ยวข้อง (๓) บริกรข้อมูลด้านธุรกิจ (๔) บริกรข้อมูลด้านเทคนิค (๕) บริกรข้อมูลด้านคุณภาพ
๓ ตรวจสอบ วัดผล และรายงาน	(๑) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (๒) เกณฑ์การประเมินความพร้อมของการกำกับดูแลข้อมูล ระดับคุณภาพข้อมูล	(๑) รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล (๒) รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล	(๑) บริกรข้อมูลด้านธุรกิจ (๒) บริกรข้อมูลด้านเทคนิค (๓) บริกรข้อมูลด้านคุณภาพ

กระบวนการ (Processes)	ส่วนนำเข้า (Input)	ส่วนนำออก (Output)	ผู้มีส่วนได้ส่วนเสีย (Data Stakeholder)
๔ ปรับปรุงการกำกับดูแล	(๑) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (๒) โครงสร้างการกำกับดูแลข้อมูล (๓) เกณฑ์การประเมินความพร้อมของการกำกับดูแลข้อมูล และระดับคุณภาพข้อมูล (๔) รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล (๕) รายการความต้องการจากผู้บริหารและผู้มีส่วนได้ส่วนเสีย	(๑) กระบวนการกำกับดูแลข้อมูล (๒) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมาย ที่เกี่ยวข้องกับข้อมูล (๓) เกณฑ์การประเมินความพร้อมของการกำกับดูแลข้อมูลและระดับคุณภาพข้อมูล (๔) โครงสร้างการกำกับดูแลข้อมูล	(๑) ผู้บริหารข้อมูลระดับสูงหรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (๒) คณะกรรมการกำกับดูแลข้อมูล (๓) บริกรข้อมูลด้านธุรกิจ (๔) บริกรข้อมูลด้านเทคนิค (๕) บริกรข้อมูลด้านคุณภาพ

รูปที่ ๑๖ แสดงขั้นตอนการตรวจสอบความสอดคล้องระหว่างนโยบายข้อมูลกับการดำเนินงานของผู้ที่เกี่ยวข้อง และความสอดคล้องระหว่างนโยบายข้อมูลกับกฎหมาย



รูปที่ ๑๖ ตัวอย่างแผนภาพการดำเนินการกำกับดูแลข้อมูล

จากรูปที่ ๑๖ แสดงให้เห็นตัวอย่างของการดำเนินการกำกับดูแลข้อมูลว่าบริกรข้อมูล (Data Stewards) ทั้งด้านธุรกิจและด้านเทคนิค เป็นผู้ร่างนโยบายข้อมูล (Data Policies) ให้สอดคล้องกับกฎหมายหรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง และนำเสนอคณะกรรมการกำกับดูแลข้อมูล ซึ่งประกอบไปด้วย CEO CIO CDO และหรือผู้บริหารทั้งฝ่ายบริหารและฝ่ายเทคโนโลยีสารสนเทศพิจารณากำหนดนโยบายเพื่อควบคุมให้เจ้าของข้อมูล (Data Owners) และผู้มีส่วนได้ส่วนเสียกับข้อมูลอื่น ๆ (Data Stakeholders) มีหน้าที่ในการปฏิบัติตามนโยบายข้อมูลที่กำหนดไว้

เจ้าของข้อมูลเป็นผู้กำหนดสิทธิการเข้าถึงและดำเนินงานใด ๆ กับข้อมูลที่ตนเป็นเจ้าของ ทั้งข้อมูลที่มีโครงสร้าง (ฐานข้อมูล) ข้อมูลกึ่งโครงสร้าง (Extensible Markup Language-XML) ข้อมูลที่ไม่มีโครงสร้าง (เสียง ภาพ ภาพเคลื่อนไหว) ขณะที่ผู้มีส่วนได้ส่วนเสียกับข้อมูล เช่น ผู้บริหารจัดการฐานข้อมูล (Database Administrators) และผู้ใช้ข้อมูล (Data Users) ต้องดำเนินการกับข้อมูลให้สอดคล้องกับสิทธิที่ได้รับจากเจ้าของข้อมูล เช่น การเพิ่ม ลบ แก้ไข ประมวลผล นำไปใช้ แลกเปลี่ยน เปิดเผยข้อมูล โดยมีบริกรข้อมูลเป็นผู้ตรวจสอบความสอดคล้องกันของการดำเนินงานตามนโยบายข้อมูล ทั้งจากเจ้าของข้อมูลและผู้มีส่วนได้ส่วนเสียกับข้อมูล พร้อมทั้งรายงานการตรวจสอบการดำเนินงานให้กับคณะกรรมการกำกับดูแลข้อมูลทราบ ทั้งนี้คณะกรรมการกำกับดูแลข้อมูลต้องทบทวนนโยบายข้อมูล และผลการดำเนินงานจากรายงานการตรวจสอบเพื่อการปรับปรุง และกำหนดแนวทางในการกำกับดูแลที่มีประสิทธิภาพต่อไป

ตารางที่ ๑๕ ความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย

กระบวนการ/กิจกรรม	ผู้มีส่วนได้ส่วนเสีย				
	คณะกรรมการกำกับดูแลข้อมูล	ทีมบริกรข้อมูล	เจ้าของข้อมูล	ทีมบริหารจัดการข้อมูล	ผู้สร้างและใช้งานข้อมูล
กำหนดและปรับปรุงนโยบายและมาตรฐานข้อมูล	A	R	S	S/C	S
ตรวจสอบการปฏิบัติตามนโยบายข้อมูล	I	R	S	S/C	S
การประเมินความพร้อมของการกำกับดูแลข้อมูล	I	R	S	S	S
ประเมินมั่นคงปลอดภัยและคุณภาพข้อมูล	I	R	S	S/C	S
รายงานผลการตรวจสอบ ความมั่นคงปลอดภัย และคุณภาพข้อมูล	I	R	I	I	I
กำหนดสิทธิในการเข้าถึงข้อมูล	I	R	A	S/C	I

หมายเหตุ : Responsible=ดำเนินการหลัก Accoutable=อนุมัติ Supportive=ให้การสนับสนุน Consulted=ให้คำปรึกษา Informed=รับทราบข้อมูล

ตารางที่ ๑๕ แสดงความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย โดย R หมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตามกระบวนการหรือกิจกรรมที่กำหนดไว้ A หมายถึง ผู้มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากปฏิบัติงาน S หน้าที่ ผู้ที่มีหน้าที่ในการสนับสนุนหรือให้การช่วยเหลือต่อปฏิบัติงาน C หมายถึง ผู้ที่ทำหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน และ I หมายถึง ผู้ที่ทำหน้าที่รับทราบผลการปฏิบัติงาน

๓.๖ การวัดการดำเนินการและความสำเร็จของการกำกับดูแลข้อมูล (Data Governance Metrics and Success Measures)

การวัดการดำเนินการกำกับดูแลข้อมูลเป็นการประเมินความพร้อมของการกำกับดูแล จะแสดงให้เห็นถึงสถานะปัจจุบันของหน่วยงานในเรื่องความพร้อมและความก้าวหน้าในการดำเนินการกำกับดูแลข้อมูล ซึ่งผลของการดำเนินงานกำกับดูแลข้อมูลจะส่งผลถึงความสำเร็จของการกำกับดูแลข้อมูล ประกอบด้วย คุณภาพของข้อมูล ความมั่นคงปลอดภัยของข้อมูล และมูลค่าเชิงธุรกิจ ระดับความพร้อมที่สูงควรจะสะท้อนถึงความสำเร็จที่สูง อย่างไรก็ตามระดับความพร้อมกับความสำเร็จอาจจะไม่สอดคล้องกัน ซึ่งอาจจะมาจากสาเหตุอื่นหรือเกณฑ์การประเมินความพร้อมยังไม่มีประสิทธิภาพเพียงพอ ดังนั้นหน่วยงานควรจะค้นหาสาเหตุที่แน่ชัดพร้อมทั้งดำเนินการแก้ไขเกณฑ์การประเมินความพร้อมเพื่อให้สอดคล้องกับลักษณะเฉพาะของหน่วยงาน แนวทางการประเมินความพร้อมของการกำกับดูแลข้อมูล การประเมินคุณภาพของข้อมูล และการประเมินความมั่นคงปลอดภัยของข้อมูล มีรายละเอียดดังต่อไปนี้

๓.๖.๑ การประเมินความพร้อมของการกำกับดูแลข้อมูล (Data Governance Readiness Assessment)

การประเมินความพร้อมของการกำกับดูแลข้อมูลจะทำให้เราได้ทราบถึงสิ่งที่เราได้ดำเนินการแล้ว และสิ่งใดบ้างที่ควรจะดำเนินการต่อไป เพื่อปรับปรุงการดำเนินงานให้เกิดประสิทธิภาพสูงสุด ระดับความพร้อมของการกำกับดูแลข้อมูลถูกใช้เป็นเครื่องมือในการประเมินความพร้อมของการกำกับดูแลข้อมูล ซึ่งประกอบด้วย ๖ ระดับดังต่อไปนี้

- ระดับ ๐ : None หมายถึง ไม่มีการกำกับดูแลข้อมูลหรือมีแต่ไม่ได้ดำเนินการอย่างเป็นทางการ นั่นคือ มีการดำเนินงานบางส่วนและไม่มีการประกาศให้ทราบอย่างเป็นทางการ
- ระดับ ๑ : Initial หมายถึง ไม่มีการกำหนดมาตรฐานของกระบวนการ นั่นคือ กระบวนการถูกกำหนดขึ้นมาเฉพาะกิจ (Adhoc) ทำให้แต่ละโครงการหรือบริการมีรูปแบบของกระบวนการที่แตกต่างกัน และอำนาจในการจัดการและกำกับดูแลข้อมูลส่วนใหญ่ถูกดำเนินการโดยฝ่ายเทคโนโลยีสารสนเทศทำให้การทำงานร่วมกันระหว่างฝ่ายธุรกิจและฝ่ายเทคโนโลยีสารสนเทศไม่สอดคล้องกัน
- ระดับ ๒ : Managed หมายถึง เริ่มมีการกำหนดมาตรฐานของกระบวนการเฉพาะแต่ละส่วนงานหรือบริการ และมีการกำหนดบุคคลที่เกี่ยวข้องกับการกำกับติดตาม เช่น บริกรข้อมูลและเจ้าของข้อมูล
- ระดับ ๓ : Standardized หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศมีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลหรือความมั่นคงปลอดภัย
- ระดับ ๔ : Advanced หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศมีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลและความมั่นคงปลอดภัย
- ระดับ ๕ : Optimized หมายถึง มีการดำเนินการสอดคล้องกับระดับ ๔ วิเคราะห์สาเหตุของปัญหา (Root Cause) ประกอบไปด้วย ความไม่สอดคล้องในการปฏิบัติงานกับนโยบายข้อมูล (Non-Conformation) คุณภาพข้อมูลที่ต่ำ และความไม่คุ้มทุนในการบริหารจัดการข้อมูล ดำเนินการปรับปรุงกระบวนการ กฎเกณฑ์และนโยบายข้อมูล หรือโครงสร้างการกำกับดูแลข้อมูลเพื่อแก้ไขปัญหาที่พบจากผลการวิเคราะห์ และให้สอดคล้องกับความต้องการของผู้ที่เกี่ยวข้องและวัตถุประสงค์ที่เปลี่ยนไปของหน่วยงาน

ตารางที่ ๑๖ ระดับความพร้อมของการกำกับดูแลข้อมูล

ระดับ	โครงสร้างการกำกับดูแล	กระบวนการกำกับดูแล	นโยบายข้อมูลและการตรวจสอบ	การประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	การวัดความคุ้มทุนและการปรับปรุงอย่างต่อเนื่อง
๐ : None	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
๑ : Initial	มีการกำหนดผู้กำกับดูแลอย่างไม่เป็นทางการ	กระบวนการยังไม่เป็นมาตรฐาน	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
๒ : Managed	มีการกำหนดผู้กำกับดูแลในแต่ละส่วนงาน/บริการ	มีกระบวนการเป็นมาตรฐานส่วนงาน/บริการ	บังคับใช้ในส่วนงาน/บริการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
๓ : Standardized	มีส่วนงานกลางในการกำกับดูแล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลหรือความมั่นคงปลอดภัย	ไม่มีหรือมีแต่ไม่เป็นทางการ
๔ : Advanced	มีส่วนงานกลางในการกำกับดูแล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	ไม่มีหรือมีแต่ไม่เป็นทางการ
๕ : Optimized	มีส่วนงานกลางในการกำกับดูแล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	มีการวัดความคุ้มทุนและปรับปรุงกระบวนการอย่างต่อเนื่อง

๓.๖.๒ การประเมินคุณภาพของข้อมูล (Data Quality Assessment)

การประเมินคุณภาพของข้อมูลเป็นการตรวจสอบผลลัพธ์หรือความสำเร็จจากการกำกับดูแลข้อมูล โดยองค์ประกอบในการประเมินคุณภาพ ประกอบด้วย

รูปที่ ๑๗ องค์ประกอบในการประเมินคุณภาพข้อมูล

๑) ข้อมูลมีความถูกต้อง (Accuracy) ข้อมูลจะมีความถูกต้องและเชื่อถือได้ขึ้นกับวิธีการที่ใช้ในการควบคุมข้อมูลนำเข้า และการควบคุมการประมวลผล การควบคุมข้อมูลนำเข้าเป็นการกระทำเพื่อให้เกิดความมั่นใจว่าข้อมูลนำเข้ามีความถูกต้องเชื่อถือได้ เพราะถ้าข้อมูลนำเข้าไม่มีความถูกต้องแล้ว ถึงแม้จะใช้วิธีการวิเคราะห์และประมวลผลข้อมูลที่ดีเพียงใด ผลลัพธ์ที่ได้ก็จะไม่มีความถูกต้อง หรือนำไปใช้ไม่ได้ ข้อมูลนำเข้าจะต้องเป็นข้อมูลที่ผ่านการตรวจสอบว่าถูกต้องแล้ว ข้อมูลบางประเภทอาจต้องแปลงให้อยู่ในรูปแบบที่เครื่องคอมพิวเตอร์สามารถเข้าใจได้อย่างถูกต้อง ซึ่งอาจต้องพิมพ์ข้อมูลมาตรวจสอบก่อนการประมวลผลถึงแม้ว่าจะมีการตรวจสอบข้อมูลนำเข้าแล้วก็ตาม ก็อาจทำให้ได้ข้อมูลที่ผิดพลาดได้ เช่น การเขียนโปรแกรมหรือใช้สูตรคำนวณผิดพลาด ดังนั้นจึงควรกำหนดวิธีการควบคุมการประมวลผล ได้แก่ การตรวจสอบยอดรวมที่ได้จากการประมวลผลแต่ละครั้งหรือการตรวจสอบผลลัพธ์ที่ได้จากการประมวลผลด้วยเครื่องคอมพิวเตอร์กับข้อมูลสมมติที่มีการคำนวณด้วยว่ามีความถูกต้องตรงกันหรือไม่

๒) ข้อมูลมีความครบถ้วน (Completeness) ข้อมูลบางประเภทหากไม่ครบถ้วน จัดเป็นข้อมูลที่ด้อยคุณภาพได้เช่นกัน เช่น ข้อมูลประวัติคนไข้ หากไม่มีหมู่เลือดของคนไข้ จะไม่สามารถใช้ได้ในกรณีที่ผู้ร้องขอข้อมูลต้องการข้อมูลหมู่เลือดของคนไข้ หรือข้อมูลที่อยู่ของลูกค้าที่กรอกผ่านแบบฟอร์ม ถ้ามีชื่อและนามสกุลโดยไม่มีข้อมูลบ้านเลขที่ ถนน แขวง/ตำบล เขต/อำเภอ หรือจังหวัด ข้อมูลเหล่านั้นก็ไม่สามารถนำมาใช้ได้เช่นกัน

๓) ข้อมูลมีความต้องกัน (Consistency) ค่าข้อมูลในชุดข้อมูลเดียวที่สอดคล้องกับค่าในชุดข้อมูลอื่น นอกจากนี้คำจำกัดความของความสอดคล้องระบุว่าหากมีการดึงข้อมูลสองค่าจากชุดข้อมูลแยกต่างหากต้องไม่ขัดแย้งกัน เช่น ข้อมูลวันที่หรือเวลาที่เก็บในฐานข้อมูลเจ้าหน้าที่ และฐานข้อมูลผู้ลงทะเบียนใช้บริการชุดข้อมูลที่มีรูปแบบต่างกัน ทั้งนี้อาจเกิดขึ้นในขณะที่การออกแบบระบบมี

การนำเข้าข้อมูลก็เป็นอีกสาเหตุหนึ่ง หรือแม้กระทั่งการใช้กฎตรวจวัดความถูกต้องของข้อมูลที่ต่างกัน เป็นต้น

๔) ข้อมูลมีความเป็นปัจจุบัน (Timeliness) ข้อมูลที่ดีนั้นนอกจากจะเป็นข้อมูลที่มีความถูกต้องเชื่อถือได้แล้วจะต้องเป็นข้อมูลที่เป็นปัจจุบัน ทั้งนี้เพื่อให้ผู้ใช้สามารถนำเอาผลลัพธ์ที่ได้ไปใช้ได้ทันเวลา นั่นคือ จะต้องเก็บข้อมูลได้รวดเร็วเพื่อทันความต้องการของผู้ใช้ เช่น ตัวอย่างข้อมูลเจ้าหน้าที่ที่เข้ามาปฏิบัติงานโดยส่วนงานที่มีหน้าที่นำเข้าข้อมูลเข้าสู่ระบบได้มีการดำเนินการตามเวลาที่กำหนดคือทำให้ข้อมูลเป็นปัจจุบันซึ่งจะทำให้หน่วยงานที่เกี่ยงข้องสามารถนำข้อมูลที่เป็นปัจจุบันไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

๕) ข้อมูลตรงตามความต้องการของผู้ใช้ (Relevancy) ระดับของข้อมูลที่บริหารจัดการต้องการนำเสนอโดยตรงและมีประสิทธิภาพ โดยสามารถใช้งานได้ตามวัตถุประสงค์ ตัวอย่างเช่น ข้อมูลทางสถิติที่จะเป็นการนำเสนอในรูปแบบตารางเข้าใจง่าย และข้อความอยู่ในหลาย ๆ ย่อหน้า ซึ่งสามารถใช้งานได้ตามความต้องการ

๖) ข้อมูลมีความพร้อมใช้ (Availability) ข้อมูลควรเข้าถึงได้ง่าย สามารถใช้งานได้จริง และสามารถใช้งานได้ตลอดเวลา ตัวอย่างเช่น นักวิเคราะห์แผนงานต้องการข้อมูลบัญชีของการประกันภัยต่อเขตต่าง ๆ แต่ข้อมูลไม่พร้อมใช้งานจนกระทั่งต้องใช้คนเขียนโปรแกรมเพื่อดึงข้อมูลนั้นออกมา ในกรณีนี้หากข้อมูลมีความพร้อมกับความต้องการใช้ ผู้ใช้สามารถใช้ข้อมูลดังกล่าวได้ทันที

ตัวอย่างการวัดคุณภาพข้อมูลที่เป็นโครงสร้าง ดังแสดงในตารางที่ ๑๗

ตารางที่ ๑๗ ตัวอย่างการวัดคุณภาพข้อมูลที่เป็นโครงสร้างสำหรับแต่ละชุดข้อมูล

คุณภาพข้อมูล	รูปแบบการวัด	หน่วยวัด	ตัวอย่าง
ความถูกต้อง	แถวxฟิลด์	ร้อยละ	ถ้าพบว่ามี ๘๐ ฟิลด์ที่มีความถูกต้องตลอดทั้ง ๑,๐๐๐ คน ดังนั้นชุดข้อมูลนี้มีความถูกต้อง = (๑,๐๐๐ x ๘๐) / (๑,๐๐๐ x ๑๐๐) x ๑๐๐ = ๘๐
ความครบถ้วน	๑) แถว ๒) แถวx ฟิลด์ ๓) แถวx ฟิลด์ที่จำเป็น	ร้อยละ	**กรณีที่ ๑ : พิจารณาเฉพาะแถวข้อมูล** ถ้าพบว่ามีการบันทึกข้อมูล ๙๐๐ คน โดยไม่สนใจจำนวนฟิลด์ที่มีการบันทึก ดังนั้นข้อมูลชุดนี้มีความครบถ้วน = (๙๐๐ /๑,๐๐๐) x ๑๐๐ = ๙๐ **กรณีที่ ๓ : พิจารณาแถวและฟิลด์ข้อมูล** ถ้าพบว่ามี ๖๐ ฟิลด์จาก ๑๐๐ ฟิลด์ ที่มีการบันทึกข้อมูลทั้ง ๑,๐๐๐ คน ดังนั้นข้อมูลชุดนี้มีความครบถ้วน = (๑,๐๐๐ x ๖๐) / (๑,๐๐๐ x ๑๐๐) x ๑๐๐ = ๖๐ **กรณีที่ ๒ : พิจารณาแถวและฟิลด์ข้อมูลที่มีความจำเป็นเท่านั้น** ถ้ากำหนดให้มี ๘๐ ฟิลด์ที่มีความจำเป็นต้องบันทึกข้อมูล แล้วพบว่ามี ๖๐ ฟิลด์จาก ๘๐ ฟิลด์ ที่มีการบันทึกข้อมูลทั้ง ๑,๐๐๐ คน ดังนั้นข้อมูลชุดนี้มีความครบถ้วน = (๑,๐๐๐ x ๖๐) / (๑,๐๐๐ x ๘๐) x ๑๐๐ = ๗๕
ความต้องกัน	ฟิลด์	ร้อยละ	ถ้าพบว่ามี ๒๐ ฟิลด์ที่เก็บซ้ำซ้อนกับชุดข้อมูลอื่นและมีรูปแบบของฟิลด์ที่แตกต่างกัน เช่น รูปแบบวันที่ รูปแบบรหัส ดังนั้นข้อมูลชุดนี้มีความความต้องกัน = (๑๐๐-๒๐ / ๑๐๐) x ๑๐๐ = ๘๐

คุณภาพข้อมูล	รูปแบบการวัด	หน่วยวัด	ตัวอย่าง
ความเป็นปัจจุบัน	๑) แถว ๒) แถวx ฟิลด์	ร้อยละ	**กรณีที่ ๑ : พิจารณาเฉพาะแถวข้อมูล** ถ้ามีพนักงานใหม่ ๑๐ คน และมีพนักงานเก่า ๕ คนที่มีการเปลี่ยนข้อมูล ซึ่งยังไม่มีการบันทึกหรือปรับปรุงให้เป็นปัจจุบัน ดังนั้นข้อมูลชุดนี้มีความเป็นปัจจุบัน = ๑๐๐ – [(๑๐ + ๕) / (๑,๐๐๐+๑๐) x ๑๐๐] = ๙๘.๕๑ **กรณีที่ ๒ : พิจารณาแถวและฟิลด์ข้อมูล** ถ้ามีพนักงานใหม่ ๑๐ คน และมีพนักงานเก่า ๕ คนที่มีการเปลี่ยนชื่อและบ้านเลขที่ ซึ่งยังไม่มีการบันทึกหรือปรับปรุงให้เป็นปัจจุบัน ดังนั้นข้อมูลชุดนี้มีความเป็นปัจจุบัน = ๑๐๐ – [[(๑๐ x ๒) + (๕ x ๒)] / [(๑,๐๐๐ + ๑๐) x ๑๐๐] x ๑๐๐] = ๙๙.๙๗ **หมายเหตุ :** ชื่อและบ้านเลขที่นับเป็น ๒ ฟิลด์
ตรงตามความต้องการใช้	ฟิลด์	ร้อยละ	ถ้าพบว่ามี ๒๐ ฟิลด์ที่ไม่เคยถูกนำไปใช้ ดังนั้นข้อมูลชุดนี้มีความตรงตามความต้องการใช้ = [(๑๐๐-๒๐) / ๑๐๐] x ๑๐๐ = ๘๐
ความพร้อมใช้	ชุดข้อมูล	ร้อยละ	= ๑๐๐ ถ้าข้อมูลเก็บอยู่ในรูปแบบ ฐานข้อมูล กำหนดให้ = ๖๖.๖๗ ถ้าข้อมูลเก็บอยู่ในรูปแบบ XML JSON และ CSV = ๓๓.๓๓ ถ้าข้อมูลเก็บอยู่ในรูปแบบ WORD PDF **หมายเหตุ :** ข้อมูลที่อยู่ในระดับที่ต่ำกว่าสามารถจัดให้อยู่ในระดับที่สูงขึ้นได้ ถ้ามีเครื่องมือหรือวิธีการที่ทำให้การนำข้อมูลไปใช้งานสะดวกมากขึ้น

หมายเหตุ : กำหนดให้ชุดข้อมูลพนักงาน มีจำนวน ๑,๐๐๐ แถว (คน) แต่ละแถวประกอบด้วย ๑๐๐ คอลัมน์ (ฟิลด์)

๓.๖.๓ การประเมินความมั่นคงปลอดภัยของข้อมูล (Data Security Assessment)

การประเมินความมั่นคงปลอดภัยของข้อมูลเป็นอีกหนึ่งวิธีในการวัดความสำเร็จจากการกำกับดูแลข้อมูล โดยใช้หลักเกณฑ์ในด้านต่าง ๆ ดังนี้

๑) จัดทำนโยบายด้านความมั่นคงปลอดภัยของข้อมูลที่รวมถึงการป้องกันข้อมูลในบริบทของการรักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูล
๒) ข้อมูลมีการจัดชั้นความลับ (Data Classification) ข้อมูลควรมีการจัดชั้นความลับให้สอดคล้องกับกฎหมาย เงื่อนไข และข้อกำหนดต่างๆ รวมถึงการคำนึงถึงมูลค่า ความสำคัญและความอ่อนไหวของข้อมูลกรณีที่ผู้ไม่ได้รับสิทธิในการเข้าถึงนั้นทำการเปิดเผยข้อมูลดังกล่าวด้วย การกำหนดระดับชั้นความลับเช่น ข้อมูลลับ ข้อมูลใช้ภายใน และข้อมูลเปิดเผย
๓) กำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูล (Data Protection) การกำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูลต้องคำนึงถึงระดับชั้นความลับของข้อมูล เช่น ข้อมูลที่มีความอ่อนไหวต้องมีการกำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูลแบบพิเศษ เพื่อป้องกันกันการเข้าถึงเพื่อเปิดเผยข้อมูลที่อ่อนไหวนั้น รวมถึงเพื่อป้องกันการดัดแปลง แก้ไข แต่งเติมข้อมูลโดยไม่ได้รับอนุญาต
๔) ข้อมูลถูกใช้งานอย่างเหมาะสม การนำข้อมูลไปใช้ควรดำเนินการให้สอดคล้องกับสัญญาอนุญาตและไม่ขัดต่อกฎหมาย
๕) ข้อมูลต้องมีความพร้อมใช้อยู่เสมอ ต้องมีการดำเนินการเตรียมความพร้อมไม่ว่าข้อมูลจะอยู่ในประเภทใดก็ตาม เช่น ข้อมูลในรูปแบบกระดาษต้องมีสถานที่จัดเก็บดูแล และสามารถเข้าถึงโดยผู้มีสิทธิได้อย่างสม่ำเสมอ ข้อมูลในรูปแบบอิเล็กทรอนิกส์ต้องมีการเตรียมความพร้อมเรื่องระบบงาน การสำรองข้อมูล รวมถึงมีแผนการดำเนินการในกรณีฉุกเฉินใดๆ ที่อาจมีผลต่อการใช้ข้อมูลด้วย

ตารางที่ ๑๘ ตัวอย่างการวัดความมั่นคงปลอดภัยของข้อมูล

ความมั่นคงปลอดภัยของข้อมูล	หน่วยวัด	ตัวอย่าง
ความลับ ความถูกต้อง ความพร้อมใช้	จำนวนครั้ง	• จำนวนการพิจารณาทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศและมาตรการควบคุมและป้องกันการเข้าถึงข้อมูล • จำนวนการส่งเสริม สื่อสารสร้างความตระหนักด้านความมั่นคงปลอดภัย • จำนวนการทดสอบความต่อเนื่องของการให้บริการและการนำข้อมูลกลับมาใช้

ความมั่นคงปลอดภัยของข้อมูล	หน่วยวัด	ตัวอย่าง
ความลับ ความถูกต้อง ความพร้อมใช้	ร้อยละ	• ร้อยละของการปฏิบัติตามนโยบายข้อมูลที่ได้กำหนดไว้ $= \frac{\text{จำนวนข้อกำหนดของนโยบายที่เป็นไปตามที่กำหนด}}{\text{จำนวนข้อกำหนดของนโยบายทั้งหมด}} x$ ๑๐๐ • ร้อยละของจำนวนเหตุละเมิดความมั่นคงปลอดภัยที่ควบคุมได้ เช่น ร้อยละของการถูกเผยแพร่ข้อมูลโดยไม่ได้รับอนุญาต สูตรการคำนวณ $= \frac{\text{จำนวนเหตุละเมิดความมั่นคงปลอดภัยที่ควบคุมได้}}{\text{จำนวนเหตุละเมิดความมั่นคงปลอดภัยทั้งหมด}} x$ ๑๐๐ • ร้อยละของจำนวนข้อร้องเรียนด้านความมั่นคงปลอดภัยข้อมูลที่ลดลง เช่นร้อยละของจำนวนข้อร้องเรียนจากการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับการอนุญาต สูตรการคำนวณ $= \frac{\text{จำนวนข้อร้องเรียนปีปัจจุบัน} - \text{ปีที่ผ่านมา}}{\text{จำนวนข้อร้องเรียนปีที่ผ่านมา}} x$ ๑๐๐ • ร้อยละของความสำเร็จในการกู้คืนข้อมูลเมื่อมีเหตุฉุกเฉิน $= \frac{\text{จำนวนกู้คืนข้อมูลที่ความสำเร็จ}}{\text{จำนวนกู้คืนข้อมูลทั้งหมด}} x$ ๑๐๐

บทสรุป

กรอบการกำกับดูแลข้อมูล (Data Governance Framework) เปรียบเสมือนเป็นแนวทางในการริเริ่มกำหนดกลไกต่าง ๆ ในการกำกับดูแลข้อมูลอย่างเป็นรูปธรรมเพื่อประโยชน์ในการบริหารจัดการข้อมูล ให้ได้ซึ่งข้อมูลที่มีคุณภาพ มีความปลอดภัย สร้างมูลค่า และสามารถเพิ่มศักยภาพในการดำเนินงานทั้งการแลกเปลี่ยนเชื่อมโยงและการสร้างประโยชน์จากข้อมูลต่อไปในอนาคต ซึ่งจะเป็นประโยชน์อย่างยิ่งต่อการดำเนินงานและการแข่งขันของประเทศ

จากกรอบการกำกับดูแลข้อมูลตามหัวข้อในบทที่ ๓ ซึ่งแสดงให้เห็นถึงโครงสร้าง กระบวนการและหลักเกณฑ์ต่าง ๆ ทั้งนี้เพื่อให้ได้มาซึ่งการกำกับดูแลข้อมูลที่ดีนั้น หน่วยงานควรคำนึงถึงการดำเนินงานดังต่อไปนี้

๑. **บทบาทของผู้บริหาร** ผู้บริหารระดับสูงของหน่วยงาน เป็นผู้มีบทบาทสำคัญยิ่งในการผลักดันให้เกิดการกำกับดูแลข้อมูล ดังนั้นผู้บริหารระดับสูงของหน่วยงานต้องมีความมุ่งมั่นในการผลักดันให้เกิดการกำกับดูแลข้อมูล โดยผู้บริหารควรมีบทบาท ดังต่อไปนี้
   - สื่อสารถึงความสำคัญของการกำกับดูแลข้อมูล ขอบเขต นโยบาย และเป้าประสงค์ของการกำกับดูแลข้อมูล
   - สนับสนุน ส่งเสริม จัดสรรทรัพยากรให้เพียงพอต่อการดำเนินงาน
   - ทบทวนการกำกับดูแลข้อมูลในหน่วยงานและส่งเสริมให้เกิดการกำกับดูแลข้อมูลอยู่สม่ำเสมอ
๒. **จัดตั้งคณะทำงาน** จัดตั้งคณะทำงานให้สอดคล้องกับหน้าที่ความรับผิดชอบของแต่ละตำแหน่งตามที่ได้กำหนดไว้ในกรอบการกำกับดูแลข้อมูล เช่น คณะกรรมการกำกับดูแลข้อมูล บริกรข้อมูล ทั้งนี้หน่วยงานสามารถดูความเหมาะสมในการบริหารจัดการบุคลากรที่มีหน้าที่ในการปฏิบัติงานดังกล่าว นอกจากนั้นบางหน่วยงานอาจมีบุคลากรที่ทำหน้าที่ในลักษณะดังกล่าวอยู่ในปัจจุบัน อย่างไรก็ตามการกำหนดบทบาทหน้าที่ที่ชัดเจนจะส่งผลต่อการทำงานที่มีประสิทธิภาพและประสิทธิผลสูงสุดต่อหน่วยงาน
๓. **กำหนดกระบวนการกำกับดูแลข้อมูล** กำหนดกระบวนการกำกับดูแลข้อมูล (Data Governance Process) ตามที่ได้กำหนดไว้ในกรอบการกำกับดูแลข้อมูล โดยพิจารณาถึง การเลือกข้อมูลเพื่อดำเนินการกำกับดูแล การระบุเป้าหมาย การกำหนดมาตรฐานและแนวปฏิบัติ รวมถึงการบริหารจัดการคน โดยกระบวนการกำกับดูแลข้อมูลเริ่มตั้งแต่การวางแผน การปฏิบัติ การตรวจสอบ วัดผลและรายงานไปจนถึงการปรับปรุงอย่างต่อเนื่อง
๔. **กำหนดนโยบาย กฎเกณฑ์ของข้อมูล** การกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในพื้นฐานของการกำกับดูแลข้อมูล นโยบายที่กำหนดสามารถใช้รายละเอียดตามที่ระบุในกรอบการกำกับดูแลข้อมูลได้ โดยคำนึงถึงความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่งหรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง มีการเผยแพร่และสื่อสารให้กับเจ้าหน้าที่และผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงานเพื่อดำเนินการต่อไป
๕. **การปฏิบัติงานต่าง ๆ ที่เกี่ยวข้องกับการกำกับดูแลข้อมูล** กลุ่มคนที่ได้กำหนดไว้ในการกำกับดูแลข้อมูลตามที่ระบุในข้อที่ ๒ มีหน้าที่ในการดำเนินงานที่แตกต่างกันออกไป โดยเริ่มตั้งแต่การวางแผน การลงมือปฏิบัติ การตรวจสอบ และปรับปรุง ตามลำดับ องค์ประกอบอย่างน้อยที่หน่วยงานจะต้องดำเนินการได้แก่

- สร้างการรับรู้ให้กับคนภายในหน่วยงาน
- ดำเนินการตามนโยบาย กฎเกณฑ์ของข้อมูล
- บริหารจัดการข้อมูล
- ส่งเสริมและสนับสนุนการแลกเปลี่ยนตลอดจนการเชื่อมโยงข้อมูลระหว่างหน่วยงาน

๖. **ตรวจสอบเพื่อการประเมินผล** การทำงานในภาพรวมเพื่อเป็นข้อมูลที่ใช้สำหรับการตัดสินใจ เพื่อการปรับปรุงหรือพัฒนาในอนาคตและบรรลุตามเป้าหมายที่วางไว้ตลอดจนเป็นแนวทางในการบริหารจัดการต่อไป

ในการกำกับดูแลข้อมูลนั้นจะต้องจัดทำอย่างสม่ำเสมอและต่อเนื่อง ดังนั้นหน่วยงานควรต้องดำเนินการและวัดผล ปรับปรุงประสิทธิภาพอยู่เสมอเพื่อยกระดับการดำเนินงานให้มีการกำกับดูแลข้อมูลที่มีให้ดียิ่งๆขึ้น เพื่อประโยชน์ในการดำเนินงาน เพิ่มศักยภาพ ส่งผลดีทั้งต่อประชาชนและประเทศชาติต่อไป

ภาคผนวก

ภาคผนวก ก แบบฟอร์มการจัดทำเมทาดาตา

ตารางที่ ๑๙ แบบฟอร์มการจัดทำเมทาดาตา

ชื่อรายการ	คำอธิบาย	โปรดระบุ
๑) ชื่อข้อมูล	ชื่อของข้อมูลที่กำหนดโดยหน่วยงานเจ้าของเรื่อง	
๒) เจ้าของข้อมูล	ชื่อบุคคล ชื่อส่วนงาน หรือชื่อหน่วยงานที่รับผิดชอบข้อมูล และที่อยู่ที่สามารถติดต่อได้	
๓) คำสำคัญ	หัวข้อ คำ หรือวลี ที่ใช้สำหรับการค้นเรื่องที่ต้องการได้	
๔) คำอธิบายอย่างย่อ	บทคัดย่อของข้อมูลหรือ Abstract ที่บ่งบอกถึงเนื้อความในข้อมูลอย่างสั้น	
๕) หน่วยงานที่ให้ข้อมูล	ชื่อบุคคลหรือชื่อหน่วยงานที่ให้ข้อมูล และที่อยู่ที่สามารถติดต่อได้	
๖) ผู้สนับสนุนหรือผู้ร่วมดำเนินการ	บุคคลหรือหน่วยงานนอกเหนือจากผู้รับผิดชอบข้อมูลที่สนับสนุนหรือร่วมดำเนินการ	
๗) วันที่เริ่มต้น	วัน เดือน ปี ที่เริ่มต้นใช้ข้อมูล (รูปแบบ YYYY-MM-DD เช่น 2015-02-25)	
๘) วันที่ทำการเปลี่ยนแปลงข้อมูลล่าสุด	วัน เดือน ปี ล่าสุดที่มีการปรับปรุงข้อมูล (รูปแบบ YYYY-MM-DD เช่น 2015-02-25)	
๙) แหล่งที่มา	แหล่งที่มาของข้อมูล เช่น จากโครงการสำรวจ	

ชื่อรายการ	คำอธิบาย	โปรดระบุ
๑๐) วิธีการได้มา	วิธีการที่ได้ซึ่งข้อมูล เช่น การรายงานจากระบบทะเบียน การสำรวจข้อมูล การวิจัย	☐ การรายงานจากระบบทะเบียน ☐ การสำรวจข้อมูล ☐ การวิจัย ☐ อื่น ๆ.....
๑๑) หน่วยย่อยที่สุดที่มีข้อมูล	หน่วยย่อยหรือขอบเขตที่ย่อยที่สุดที่มีข้อมูล เช่น หมู่บ้าน จังหวัด ภาค ประเทศ	☐ บุคคล ☐ สถานประกอบการ ☐ ครัวเรือน ☐ หมู่บ้าน ☐ ตำบล ☐ อำเภอ ☐ จังหวัด ☐ ภาค ☐ ประเทศ ☐ อื่น ๆ.....
๑๒) หน่วยของการจัดเก็บข้อมูล	หน่วยย่อยหรือขอบเขตที่ย่อยที่สุดที่มีการจัดเก็บข้อมูล เช่น หมู่บ้าน จังหวัด ภาค ประเทศ	☐ บุคคล ☐ สถานประกอบการ ☐ ครัวเรือน ☐ หมู่บ้าน ☐ ตำบล ☐ อำเภอ ☐ จังหวัด ☐ ภาค ☐ ประเทศ ☐ อื่น ๆ.....
๑๓) รูปแบบการเก็บข้อมูลปฐมภูมิ	รูปแบบที่บันทึกข้อมูลปฐมภูมิ เช่น text/html XML ฐานข้อมูล รูปภาพ	☐ Text/html ☐ XML ☐ ฐานข้อมูล ☐ รูปภาพ ☐ อื่น ๆ.....
๑๔) รูปแบบการเก็บข้อมูลทุติยภูมิ	รูปแบบที่บันทึกข้อมูลทุติยภูมิ เช่น text/html ASCII ฐานข้อมูล รูปภาพ	☐ Text/html ☐ XML ☐ ฐานข้อมูล ☐ รูปภาพ ☐ อื่น ๆ.....

ชื่อรายการ	คำอธิบาย	โปรดระบุ
๑๕) ประเภทการนำเสนอ	ประเภทการนำเสนอข้อมูล เช่น เว็บไซต์ รายงานวิชาการ ตาราง สถิติ ผลงานวิจัย	☐ เว็บไซต์ ☐ รายงานวิชาการ ☐ ตารางสถิติ ☐ ผลงานวิจัย ☐ อื่น ๆ.....
๑๖) ภาษาที่ใช้	ภาษาที่ใช้ เช่น ภาษาไทย ภาษาอังกฤษ ภาษาจีน ภาษาญี่ปุ่น	☐ ภาษาไทย ☐ ภาษาอังกฤษ ☐ จีน ☐ ญี่ปุ่น ☐ อื่น ๆ.....
๑๗) รหัสอ้างอิงเพื่อการเข้าถึงข้อมูล	สัญลักษณ์ เลขที่ หรือรหัสอ้างอิงที่ระบุว่าเป็นข้อมูลนั้น ๆ เช่น Uniform Resource Locator – URL	
๑๘) เรื่องที่เกี่ยวข้อง	ระบุ URL เรื่องอื่นๆ ที่เกี่ยวข้อง	
๑๙) ขอบเขตที่เผยแพร่ข้อมูล	ขอบเขตหรือพื้นที่ในการนำเสนอข้อมูล เช่น กรุงเทพมหานคร ปริมณฑล ประเทศไทย ทุกประเทศ	☐ กรุงเทพมหานคร ☐ ปริมณฑล ☐ ประเทศไทย ☐ ทุกประเทศ ☐ อื่น ๆ.....
๒๐) สิทธิ์ในการเข้าถึงข้อมูล	สิทธิ์ในการเข้าถึงข้อมูล ซึ่งอธิบายระดับการเข้าถึงข้อมูล เช่น ผู้มีสิทธิเข้าถึง ฟิลด์ที่สามารถเข้าถึง รายการที่สามารถเข้าถึง	
๒๑) สิทธิ์ในการใช้ข้อมูล	สิทธิ์ สัญญา หรือข้อตกลงในการใช้ชุดข้อมูล เช่น สัญญาอนุญาตสำหรับข้อมูลเปิดภาครัฐ (License for Open Government Data	

ภาคผนวก ข บทบาท และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียกับข้อมูล

เพื่อให้หน่วยงานสามารถดำเนินการบริหารจัดการและกำกับดูแลข้อมูลได้อย่างมีประสิทธิภาพ และสร้างประโยชน์สูงสุด จึงมีการกำหนดบทบาท และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียกับข้อมูลในแต่ละด้าน ดังต่อไปนี้

ตารางที่ ๒๐ บทบาท และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียกับข้อมูล

บทบาท	ความรับผิดชอบ
ด้านการบริหารจัดการข้อมูล	
สถาปนิกข้อมูล (Data Architect)	● กำหนดโครงสร้างและความสัมพันธ์ของข้อมูล โดยพิจารณาจากความต้องการข้อมูล และวัตถุประสงค์ของหน่วยงาน ● พัฒนาสถาปัตยกรรมข้อมูลในภาพรวมของทั้งหน่วยงาน โดยประเมินสถานะในปัจจุบัน และออกแบบเพื่อปรับปรุงสำหรับอนาคต ● สร้างพิมพ์เขียว (Blueprint) สำหรับการบริหารจัดการข้อมูลต่าง ๆ เช่น การบูรณาการข้อมูล การไหลของข้อมูลตั้งแต่ต้นทางจนถึงปลายทาง
ผู้บริหารจัดการฐานข้อมูล (Database Administrator)	● บริหารจัดการ และควบคุมเกี่ยวกับระบบฐานข้อมูลภายในหน่วยงาน ● กำหนดนโยบาย มาตรการ และมาตรฐานของระบบฐานข้อมูลทั้งหมดภายในหน่วยงาน ตัวอย่างเช่น รายละเอียดและวิธีการจัดเก็บข้อมูล การใช้งานฐานข้อมูล การรักษาความปลอดภัยของข้อมูล การสำรองข้อมูล การกู้คืนข้อมูล
วิศวกรข้อมูล (Data Engineer)	● ออกแบบวิธีการจัดเก็บ และเรียกใช้งานข้อมูล ● จัดการเกี่ยวกับข้อมูลทั้งหมด ตั้งแต่ระบุชนิดของข้อมูล วางโครงสร้างของการเข้าและการออกของข้อมูล เพื่อให้ข้อมูลไหลได้อย่างไม่สะดุด
นักวิเคราะห์ข้อมูล (Data Analyst)	● นำข้อมูลมาวิเคราะห์แนวโน้มในเชิงธุรกิจ หรือแก้ปัญหาจากสิ่งที่ผิดแปลกไปจากแนวโน้มเดิม โดยใช้ประสบการณ์ และหลักสถิติ ● ใช้โมเดลหรือเครื่องมือในการทำรายงาน เพื่อสรุปข้อมูลสำหรับใช้ในการตัดสินใจ
นักวิทยาการข้อมูล (Data Scientist)	● นำข้อมูลจากหลาย ๆ แหล่ง และแปลงข้อมูล เพื่อหารูปแบบและความสัมพันธ์ของข้อมูล

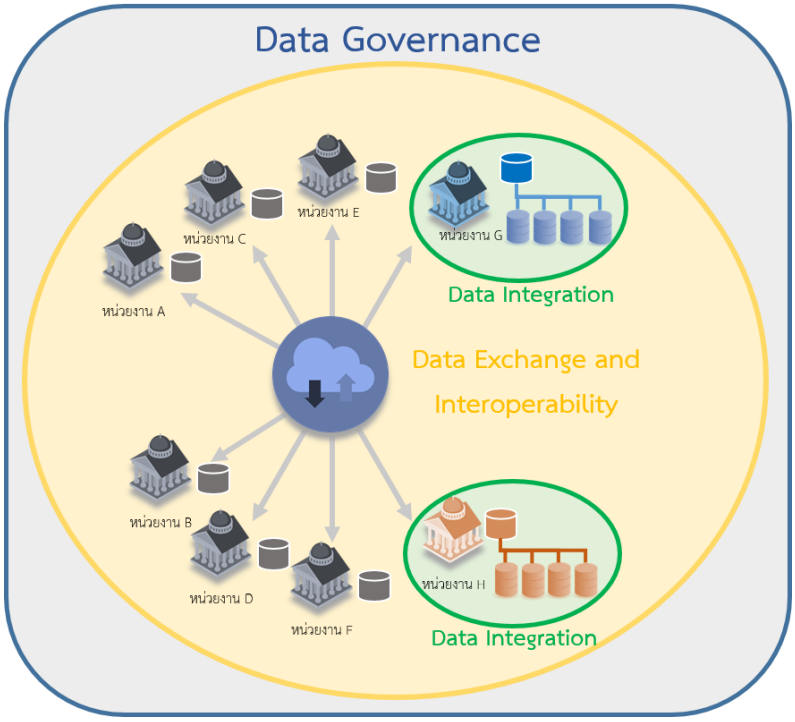
บทบาท	ความรับผิดชอบ
	• สร้างแบบจำลอง และดำเนินการกับข้อมูลด้วยวิธีการต่าง ๆ เช่น Machine Learning หรือเขียนโปรแกรม เพื่อทำนายมุมมอง และคำตอบใหม่ ๆ
นักวิเคราะห์ระบบ (System Analyst)	• วิเคราะห์และออกแบบระบบ โดยศึกษาเกี่ยวกับปัญหา รวบรวมความต้องการของผู้ใช้งานระบบ วิเคราะห์ระบบงานภายในหน่วยงาน
นักวิเคราะห์ธุรกิจ (Business Analyst)	• ศึกษาและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับเทคโนโลยี กลยุทธ์ กลุ่มเป้าหมาย และหน่วยงานที่เกี่ยวข้อง • ทำความเข้าใจเป้าหมายและปัญหาของหน่วยงาน วิเคราะห์ความต้องการและหาคำตอบ เพื่อวางแผนด้านกลยุทธ์ เพื่อผลักดันให้เกิดการเปลี่ยนแปลง
นักออกแบบจำลองข้อมูล (Data Modeler)	• ออกแบบจำลองข้อมูล เช่น Entity Relationship Diagram และ Data Flow Diagram • ออกแบบและพัฒนาแบบจำลองข้อมูล (Data Model) เพื่ออธิบายลักษณะโครงสร้างและการทำงานของข้อมูลให้เห็นภาพได้มากขึ้น
ด้านการกำกับดูแลข้อมูล	
ผู้บริหารข้อมูลระดับสูง (Chief Data Officer)	• นำข้อมูลและวิเคราะห์ข้อมูล เพื่อสร้างและส่งมอบเทคโนโลยี เครื่องมือ แนวทาง และวิธีการในการทำให้ข้อมูลของหน่วยงานมีคุณค่า และเกิดประโยชน์สูงสุดต่อหน่วยงาน • วิเคราะห์และร่วมกับผู้บริหารส่วนอื่น ๆ เพื่อจัดทำยุทธศาสตร์และดำเนินการกำกับดูแลข้อมูลคุณภาพและการควบคุมอื่น ๆ เพื่อรักษาความสมบูรณ์ของข้อมูล • นำแนวปฏิบัติและมาตรฐานของหน่วยงานไปปรับปรุงข้อมูลและยุทธศาสตร์ของประเทศ • เป็นตัวกลางระหว่างหน่วยงานภาครัฐในการแลกเปลี่ยน เชื่อมโยงข้อมูล รวมไปถึงการจัดการความเสี่ยงที่อาจเกิดจากข้อมูลของหน่วยงานภาครัฐ • ส่งเสริมนวัตกรรมที่ใช้ประโยชน์จากข้อมูลในการวิเคราะห์ปัญหา • วิเคราะห์หาเทคโนโลยีใหม่ ๆ มาใช้ในการวิเคราะห์ข้อมูล

บทบาท	ความรับผิดชอบ
บริกรข้อมูลด้านธุรกิจ (Business Data Stewards)	• นิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัย • นิยามเมทาดาตา • ร่างนโยบายข้อมูล มาตรฐาน และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับข้อมูล • ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ
บริกรข้อมูลด้านเทคนิค (Technical Data Stewards)	• ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูล • รักษา และดูแลข้อมูลที่อยู่บนระบบเทคโนโลยีสารสนเทศต่าง ๆ ในหน่วยงาน
บริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards)	• ดำเนินการในเรื่องคุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูล และการวิเคราะห์คุณภาพข้อมูล
เจ้าของข้อมูล (Data Owner)	• ตรวจสอบ ดูแล และรักษาคุณภาพของข้อมูล • ทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล
ผู้สร้างข้อมูล (Data Creator)	• บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ • ทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความปลอดภัยของข้อมูล
ผู้ใช้ข้อมูล (Data User)	• นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร • สนับสนุนการกำกับดูแลข้อมูล • รายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูล

ภาคผนวก ค แนวนโยบายและแนวปฏิบัติในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

การแลกเปลี่ยนข้อมูลเป็นกระบวนการของการรับส่งข้อมูลหรือแบ่งปันข้อมูลภายในหน่วยงานหรือระหว่างหน่วยงาน ตัวอย่างการแลกเปลี่ยนข้อมูลภาครัฐ เช่น การแลกเปลี่ยนข้อมูลกระบวนการยุติธรรม ข้อมูลการนำเข้า/ส่งออกสินค้าระหว่างประเทศ ข้อมูลภูมิสารสนเทศ ข้อมูลการบริหารจัดการน้ำ ข้อมูลเกษตรกรผู้มีรายได้น้อย ข้อมูลความมั่นคงประเทศ ทั้งนี้ ข้อมูลที่มีการแลกเปลี่ยนต้องไม่เป็นข้อมูลเปิด (Open Data) หรือข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ

การกำกับดูแลข้อมูลถือเป็นส่วนสำคัญที่จะช่วยให้การแลกเปลี่ยนข้อมูลมีประสิทธิภาพและประสิทธิผล ซึ่งส่งผลให้เกิดประโยชน์ต่อภาคประชาชน ภาครัฐ ตลอดจนภาคเอกชน อันจะส่งผลต่อความเจริญก้าวหน้าของประเทศ สอดคล้องกับรูปที่ ๑๘ ซึ่งชี้ให้เห็นถึงการกำกับดูแลข้อมูลเข้ามาควบคุมการบูรณาการข้อมูล (Data Integration) และการแลกเปลี่ยนข้อมูล (Data Exchange) เพื่อให้เกิดการเชื่อมโยงข้อมูลระหว่างหน่วยงาน (Interoperability) อย่างแท้จริง



รูปที่ ๑๘ ความสัมพันธ์ระหว่างการกำกับดูแลข้อมูลและการแลกเปลี่ยนข้อมูล

โดยกิจกรรมของการกำกับดูแลข้อมูลที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลควรประกอบไปด้วย ๑) กำหนดบทบาทหน้าที่ของบุคคลที่เกี่ยวข้อง ๒) กำหนดนโยบายการแลกเปลี่ยนข้อมูล และ ๓) กำหนดแนวปฏิบัติในการแลกเปลี่ยนข้อมูล ดังรายละเอียดต่อไปนี้

๑) กำหนดบทบาทหน้าที่ที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูล

๑.๑) กำหนดบุคคลหรือกลุ่มบุคคลที่มีสิทธิ์ตัดสินใจในการสนับสนุนข้อมูลให้หน่วยงานอื่น เช่น คณะกรรมการกำกับดูแลข้อมูล (Data Governance Council) หรือคณะทำงาน

๑.๒) กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการแลกเปลี่ยนข้อมูล เช่น บุคคลที่ทำหน้าที่ออกแบบกระบวนการและเทคโนโลยีในการแลกเปลี่ยนข้อมูล (Data

Integration Architect) บุคคลที่ทำหน้าที่ดำเนินการแลกเปลี่ยนข้อมูลให้สอดคล้องกับที่ได้ออกแบบไว้ (Data Integration Specialist)

๑.๓) กำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่องและแก้ไขปัญหาเบื้องต้นในการแลกเปลี่ยนหรือขอใช้ข้อมูล เช่น ศูนย์ติดต่อ (Contact Center)

๒) กำหนดนโยบายการแลกเปลี่ยนข้อมูล

ในหัวข้อ ๓.๓.๑ ได้แสดงกรอบนโยบายข้อมูลในหมวดการแลกเปลี่ยนและเชื่อมโยงข้อมูล ดังต่อไปนี้

๒.๑) กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)

๒.๒) กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลให้ชัดเจนเริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ

๒.๓) กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการแลกเปลี่ยนที่จำเป็นให้ครบถ้วน

๒.๔) ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

๒.๕) กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล

๒.๖) บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้

๒.๗) สามารถตรวจสอบได้ว่าการแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติ กระบวนการแลกเปลี่ยน และมาตรฐานตามที่กำหนด

๓) กำหนดแนวปฏิบัติการแลกเปลี่ยนข้อมูล

แนวปฏิบัติการแลกเปลี่ยนข้อมูลเป็นไปตามขั้นตอนต่อไปนี้

๓.๑) ตรวจสอบชั้นความลับของข้อมูล (Data Classification) ว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ นั่นคือ ต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนบุคคล พร้อมทั้งตรวจสอบสิทธิ์ของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ

๓.๒) จัดทำเมทาดาตา (Metadata) ของชุดข้อมูลที่ร้องขอ ตัวอย่างองค์ประกอบของเมทาดาตา เช่น ชื่อข้อมูล คำอธิบายข้อมูล คำสำคัญ วันที่ทำการเปลี่ยนแปลงข้อมูลล่าสุด ชื่อหน่วยงานเจ้าของข้อมูล ฟิลด์ข้อมูล ทั้งนี้ต้องตรวจสอบให้แน่ใจได้ว่าเมทาดาตามีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ข้อมูล

๓.๓) จัดทำสัญญาอนุญาตหรือเงื่อนไขในการแลกเปลี่ยนและการนำข้อมูลไปใช้ ตัวอย่างส่วนประกอบของสัญญา เช่น วัตถุประสงค์ในการนำไปใช้ ขอบเขตในการนำไปใช้ ช่วงวันที่ในการเข้าถึง ความถี่ในการเข้าถึง ระดับการให้บริการ (Service Level Agreement-SLA) ช่วงเวลาในการนำไปใช้ ฟิลด์ที่สามารถเข้าถึง รายการข้อมูลที่สามารถเข้าถึง ในกรณีขอข้อมูลส่วนบุคคลเป็นรายคน ต้องจัดทำหนังสือแสดงความยินยอม (Consent Letter) เพื่อรับการยินยอมจากบุคคลนั้น ๆ ยกเว้นหน่วยงานที่ขอใช้ข้อมูลมีอำนาจตามกฎหมายโดยชอบธรรม พร้อมทั้งกำหนดเทคโนโลยีและ

มาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล เช่น Representational State Transfer (REST) Simple Object Access Protocol (SOAP)

๓.๔) ทำการแปลงข้อมูล (Anonimization) ในกรณีที่หน่วยงานที่ขอข้อมูลไม่มีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลแต่ต้องการใช้ข้อมูลเพื่อทำการศึกษาหรือวิจัย ซึ่งสามารถอ้างอิง “แนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคลได้ (Guideline to protect the Personally Identifiable Information)” พร้อมทั้งตรวจสอบและปรับปรุงคุณภาพของข้อมูล (Data Quality) ให้อยู่ในเกณฑ์มาตรฐานก่อนการแลกเปลี่ยน

๓.๕) ดำเนินการแลกเปลี่ยนข้อมูลตามเงื่อนไขและมาตรฐานการแลกเปลี่ยนที่กำหนดไว้

๓.๖) ติดตามและควบคุมประสิทธิภาพระหว่างการแลกเปลี่ยนข้อมูล เพื่อรักษาไว้ซึ่งความปลอดภัยของข้อมูล คุณภาพข้อมูล และสอดคล้องกับระดับการให้บริการ

ภาคผนวก ง แนวนโยบายและแนวปฏิบัติในการเปิดเผยข้อมูลและการขอใช้ข้อมูล

ข้อมูลเปิด (Open Data) คือ “ข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ สามารถนำกลับมาใช้ใหม่และแจกจ่ายได้โดยใครก็ตาม แต่ต้องระบุแหล่งที่มาหรือเจ้าของงานและต้องใช้สัญญาอนุญาต หรือเงื่อนไขเดียวกันกับที่มาหรือตามเจ้าของงานกำหนด”[4] ข้อมูลจากหน่วยงานภาครัฐที่สามารถเปิดเผยได้ จะอยู่ในรูปแบบที่เป็นมาตรฐานเปิด (Open Format) และไม่ใช่รูปแบบมาตรฐานเฉพาะ (Non-proprietary Format) ที่คนและเครื่องคอมพิวเตอร์สามารถอ่านและนำไปใช้ต่อยอดในการพัฒนาบริการในรูปแบบต่าง ๆ ได้ ข้อมูลเปิดถูกใช้เป็นเครื่องมือในการตรวจสอบความโปร่งใสในการดำเนินการของภาครัฐและความสามารถในการพัฒนาประเทศ ซึ่งสามารถวัดอันดับการเปิดเผยข้อมูลภาครัฐได้จากมาตรฐานตัวชี้วัด เช่น Open Data Index และ Open Data Barometer เพื่อให้อันดับการเปิดเผยข้อมูลภาครัฐสูงขึ้น หน่วยงานรัฐควรดำเนินการเปิดเผยตามหลักการเปิดเผยข้อมูล ๘ ด้าน ดังต่อไปนี้

๑) สมบูรณ์ (Completeness) ข้อมูลภาครัฐทั้งหมดที่ไม่เกี่ยวข้องกับข้อมูลส่วนบุคคลหรือความมั่นคงจะต้องถูกเปิดเผยโดยข้อมูลดังกล่าวจะไม่ขัดกับข้อกำหนดในเรื่องความเป็นส่วนตัว ความมั่นคง และเอกสิทธิ์ที่ชอบด้วยเหตุผล

๒) ข้อมูลปฐมภูมิ (Primary) ข้อมูลควรจะถูกเผยแพร่จากแหล่งที่เก็บข้อมูลโดยตรงด้วยระดับความละเอียดสูง ไม่มีการปรับแต่งหรือทำให้อยู่ในรูปแบบข้อมูลสรุป (Summary Data)

๓) ทันเวลา (Timeliness) คือ ข้อมูลควรจะเป็นปัจจุบันและหากเป็นไปได้อาจจะเป็นลักษณะ Real-time feed ซึ่งอาจจะพิจารณาตามความเหมาะสมในการเพิ่มอรรถประโยชน์ของข้อมูลนั้น ๆ ชุดข้อมูลควรจะมีการบันทึกเวลา (Timestamps) หรือข้อมูลอื่น ๆ ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน

๔) สามารถเข้าถึงได้ (Accessibility) ข้อมูลถูกเปิดเพื่อให้ผู้ใช้ที่หลากหลายและมีจุดประสงค์ต่างกัน ซึ่งข้อมูลดังกล่าวจะต้องมีการเผยแพร่อยู่บนอินเทอร์เน็ตโดยทุกคนจะต้องสามารถเข้าถึงข้อมูลเหล่านั้นได้และข้อมูลจะต้องรองรับการใช้งานจากทุกแพลตฟอร์ม

๕) เครื่องสามารถอ่านได้ (Machine Readability) ข้อมูลจะต้องอยู่ในรูปแบบที่นำไปประมวลผลได้โดยอัตโนมัติ

๖) การไม่เลือกปฏิบัติ (Non-discriminatory) ทุกคนสามารถนำข้อมูลไปใช้ได้โดยไม่ต้องมีการลงทะเบียนผู้ใช้

๗) ปลอดกรรมสิทธิ์ (Non-proprietary) ข้อมูลที่เผยแพร่จะต้องอยู่ในรูปแบบมาตรฐานเปิดไม่ใช่รูปแบบมาตรฐานเฉพาะและไม่มีองค์กรใดมีสิทธิขาดในการเป็นเจ้าของแต่ผู้เดียว

๘) ใช้งานฟรี (License-free) ข้อมูลจะต้องไม่มีปัญหาเรื่องลิขสิทธิ์ในการใช้งานสามารถใช้งานโดยไม่เสียค่าใช้จ่ายเพื่อเป็นการส่งเสริมการใช้งานอย่างแพร่หลายทำให้เกิดเป็นนวัตกรรมและบรรลุเป้าหมายที่หน่วยงานตั้งไว้รวมทั้งเป็นการเพิ่มความโปร่งใสให้แก่หน่วยงานภาครัฐ ควรจะหลีกเลี่ยงข้อจำกัดในการใช้งานข้อมูล

โดยกิจกรรมของการกำกับดูแลข้อมูลที่เกี่ยวข้องกับการเปิดเผยข้อมูลควรประกอบไปด้วย ๑) กำหนดบทบาทหน้าที่ของบุคคลที่เกี่ยวข้อง ๒) กำหนดนโยบายการเปิดเผยข้อมูล และ ๓) กำหนดแนวปฏิบัติในการเปิดเผยข้อมูล ดังรายละเอียดต่อไปนี้

๑) กำหนดบทบาทหน้าที่ ที่เกี่ยวข้องกับการเปิดเผยข้อมูล

๑.๑) กำหนดบุคคลหรือกลุ่มบุคคลที่มีสิทธิ์ตัดสินใจในการเปิดเผยข้อมูล เช่น คณะกรรมการกำกับดูแลข้อมูล (Data Governance Council) หรือคณะทำงานเปิดเผยข้อมูล

๑.๒) กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการและปรับปรุงการเปิดเผยข้อมูล

๑.๓) กำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่องและแก้ไขปัญหาเบื้องต้นในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้ เช่น ศูนย์ติดต่อ (Contact Center)

๒) กำหนดนโยบายการเปิดเผยข้อมูล

ในหัวข้อ ๓.๓.๑ ได้แสดงกรอบนโยบายข้อมูลในหมวดการเปิดเผยข้อมูล ดังต่อไปนี้

๒.๑) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

๒.๒) ต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล

๒.๓) ควรมีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

๒.๔) ควรมีการเปิดเผยเมทาดาตาควบคู่ไปกับข้อมูลที่เปิดเผย

๒.๕) สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล

๓) กำหนดแนวปฏิบัติการเปิดเผยข้อมูล

แนวปฏิบัติการเปิดเผยข้อมูลเป็นไปตามขั้นตอนต่อไปนี้

๓.๑) คัดเลือกชุดข้อมูลที่ต้องการเผยแพร่ ทั้งนี้ควรจะต้องพิจารณาชุดข้อมูลที่มีคุณภาพและเป็นที่ต้องการของทุกภาคส่วน เพื่อส่งเสริมให้เกิดการนำไปใช้อย่างแพร่หลายและเกิดประโยชน์สูงสุด

๓.๒) พิจารณาชุดข้อมูลที่คัดเลือก ชุดข้อมูลที่คัดเลือกสำหรับเผยแพร่นั้นต้องอยู่ในชั้นความลับที่สามารถเผยแพร่ได้ นั่นคือ ต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนตัว

๓.๓) จัดเตรียมข้อมูลให้อยู่ในรูปแบบที่ง่ายต่อการนำไปใช้ นั่นคือ ข้อมูลควรอยู่ในรูปแบบที่คอมพิวเตอร์สามารถอ่านได้ง่าย (Machine-Readable) หรือระดับการเปิดเผยข้อมูลระดับ ๒ ขึ้นไป เช่น รูปแบบของ Comma-Separated Values – CSV Application Programming Interface - API รวมถึงการจัดทำคำอธิบายชุดข้อมูล (Metadata) เพื่อให้ผู้ใช้ข้อมูลสามารถเข้าใจเกี่ยวกับบริบทของข้อมูล เช่น เจ้าของข้อมูล วัตถุประสงค์ ขอบเขต วันที่เผยแพร่ ความถี่ในการปรับปรุง ความถี่ในการเผยแพร่ แหล่งที่มาของข้อมูล

๓.๔) นำชุดข้อมูลขึ้นเผยแพร่ หน่วยงานจะต้องกำหนดผู้รับผิดชอบหลัก เพื่อนำชุดข้อมูลขึ้นเผยแพร่สู่สาธารณะ ซึ่งสามารถดำเนินการได้ ดังนี้

- เผยแพร่ผ่านเว็บไซต์หรือ Universal Resource Identifier - URI ของหน่วยงานพร้อมคำอธิบายชุดข้อมูล
- เผยแพร่ผ่านศูนย์กลางข้อมูลเปิดภาครัฐ โดยปฏิบัติตามเอกสาร คู่มือการนำข้อมูลขึ้นเผยแพร่บน data.go.th

- ผู้ใช้ข้อมูลถือได้ว่าเป็นผู้ที่มีส่วนร่วมในกระบวนการปรับปรุงคุณภาพของข้อมูลที่หน่วยงานได้เผยแพร่ผ่านช่องทางในการแสดงความคิดเห็นและการร้องขอข้อมูลที่ต้องการได้ ซึ่งการเปิดเผยข้อมูลที่มีคุณภาพและตรงกับความต้องการของผู้บริโภคนั้น จะช่วยให้เกิดการสร้างนวัตกรรมและยกระดับคุณภาพชีวิตของประชาชน

ภาคผนวก จ แนวนโยบายและแนวปฏิบัติอื่น ๆ

ในส่วนนี้กล่าวถึงแผนการจัดทำนโยบาย มาตรฐาน และแนวปฏิบัติ เพื่อใช้ในการกำกับดูแลข้อมูลและบริหารจัดการข้อมูลภายในหน่วยงานให้เป็นรูปธรรม มีรายละเอียดดังนี้

๑) **นโยบายข้อมูล (Data Policy)** อธิบายถึงบทบาทหน้าที่ ข้อควรปฏิบัติ และข้อห้ามปฏิบัติในการบริหารจัดการข้อมูล นโยบายข้อมูลอาจจะประกอบไปด้วย นโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policy นโยบายคุณภาพข้อมูล (Data Quality Policy) นโยบายการแลกเปลี่ยนและเชื่อมโยงข้อมูล (Data Exchange and Integration Policy) และนโยบายการเปิดเผยข้อมูล (Data Disclosure Policy)

๒) **มาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard)** อธิบายถึงรูปแบบและวิธีการจัดชั้นความลับของข้อมูลให้สอดคล้องกับผลกระทบหรือความเสียหายในด้านต่าง ๆ ได้แก่ เงิน ชื่อเสียง และความมั่นคงทั้งในระดับบุคคล ระดับหน่วยงาน และระดับประเทศ ซึ่งจะเป็นประโยชน์ในการกำหนดมาตรการรักษาความปลอดภัยของข้อมูล รวมถึงการอนุญาตให้สามารถทำการแลกเปลี่ยนหรือเปิดเผยข้อมูลได้

๓) **มาตรฐานการแลกเปลี่ยนและเชื่อมโยงข้อมูล (Data Exchange and Integration Standard)** เป็นการกำหนดรูปแบบ วิธีการ และเทคโนโลยีในการแลกเปลี่ยนและเชื่อมโยงข้อมูล เช่น มาตรฐานชุดข้อมูลอ้างอิงพื้นฐานสำหรับการแลกเปลี่ยนข้อมูล (Core Vocabulary) มาตรฐานชุดข้อมูลที่ควรเปิดเผยของประเทศ (National Open Datasets Standard)

๔) **แนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคลได้ (Guideline to protect the Personally Identifiable Information)** ให้แนวทางสำหรับหน่วยงานที่จัดเก็บข้อมูลส่วนบุคคล ได้เตรียมข้อมูลให้เหมาะสมต่อการบูรณาการข้อมูลเข้าด้วยกัน เพื่อป้องกันไม่ให้หน่วยงานปลายทางทราบได้ว่าข้อมูลที่ได้รับเป็นของบุคคลใด

๕) **แนวปฏิบัติในด้านความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Guideline)** ให้แนวทางในการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลและความเป็นส่วนบุคคล ซึ่งจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล เช่น การจัดทำสถาปัตยกรรมความมั่นคงปลอดภัยของข้อมูล (Data Security Architecture) การควบคุมการเข้าถึงข้อมูล (Data Access Control) การตรวจสอบความมั่นคงปลอดภัยของข้อมูล (Data Security Audit) การประเมินความปลอดภัยของข้อมูล (Data Security Assessment) การกำหนดเครื่องมือและเทคโนโลยีความมั่นคงปลอดภัยของข้อมูล (Data Security Tool/Technology)

๖) **แนวปฏิบัติในด้านคุณภาพข้อมูล (Data Quality Guideline)** ให้แนวทางในการวิเคราะห์คุณภาพข้อมูล (Data Profiling) และแนวปฏิบัติในการจัดเตรียมข้อมูลและปรับปรุงข้อมูล (Data Preparation and Data Cleansing) เพื่อให้ข้อมูลอยู่ในรูปแบบที่เหมาะสมสำหรับการวิเคราะห์ข้อมูลและการนำไปใช้ตัดสินใจ

๗) **แนวปฏิบัติในการเปิดเผยข้อมูล** เพื่อสร้างความรู้ ความเข้าใจให้แก่หน่วยงาน ภาคเอกชน และผู้ที่ต้องการศึกษาเกี่ยวกับข้อมูลเปิด (Open Data) ประกอบด้วย คู่มือการเปิดเผยข้อมูล (Open Data Handbook) Version 2 และแนวปฏิบัติในการเปิดเผยข้อมูลในรูปแบบ Public API

๘) **แนวปฏิบัติในการออกแบบความคิดเชิงนวัตกรรมด้านข้อมูล (Data Innovation Guideline)** เป็นแนวปฏิบัติในการออกแบบความคิดเชิงนวัตกรรม (Guidelines for Data Innovation) เป็นคู่มือที่ช่วยให้เข้าใจปัญหาที่แท้จริง และสามารถออกแบบแนวทางแก้ไขปัญหาที่เป็นแนวคิดเชิงนวัตกรรมตลอดจนสามารถเข้าถึงชุดข้อมูล (Datasets) ต่าง ๆ เพื่อให้ได้มาซึ่งแนวทางในการแก้ปัญหา นอกจากนั้นผู้ที่ต้องการศึกษากระบวนการออกแบบนวัตกรรมสามารถนำไปประยุกต์หรือปรับใช้กับหน่วยงานได้

๙) **แนวปฏิบัติในการประเมินผลการกำกับดูแลข้อมูล (Data Governance Assessment Guideline)** ให้แนวทางในการประเมินผลการกำกับดูแลข้อมูล ประกอบด้วย การประเมินความพร้อมของการกำกับดูแลข้อมูล (Data Governance Readiness Assessment) การประเมินคุณภาพของข้อมูล (Data Quality Assessment) และการประเมินความมั่นคงปลอดภัยของข้อมูล (Data Security Assessment)

บรรณานุกรม

Askham, N. (2016). Squaring the circle: Using a data governance framework to support data quality. Experian Information Solutions, Inc.

Askham, N., Cook, D., Doyle, M., Fereday, H., Gibson, M., Landbeck, U., Lee, R., Maynard, C., Palmer, G., & Schwarzenbach, J. (2013). THE SIX PRIMARY DIMENSIONS FOR DATA QUALITY ASSESSMENT: Defining Data Quality Dimensions. em360tech. [Online] 2013.

Australian Institute of Health and Welfare. (2014). Data Governance Framework. Retrieved from https://www.aihw.gov.au/getmedia/0d59ee71-9abe-4806-8e87-ce9de81974d3/AIHW-data-governance-framework.pdf.aspx

Cupola, P., Earley, S., & Henderson, D. (2014). DAMA-DMBOK2 Framework.

Henderson, D., Earley, S., Sebastian-Coleman, L., Sykora, E., & Smith, E. (2017). *DAMA guide to the data management body of knowledge.* Second Edition. Technics Publications.

Intra-governmental Group on Geographic Information (IGGI). (2005). The Principles of Good Data Management. The Office of the Deputy Prime Minister.

Kim, H. Y., & Cho, J. S. (2017, June). Data Governance Framework for Big Data Implementation with a Case of Korea. *In Big Data (BigData Congress), 2017 IEEE International Congress on* (pp. 384-391). IEEE.

Malinowski, E., & Zimányi, E. (2009). Advanced Data Warehouse Design. Springer Berlin Heidelberg.

Thomas, G. (2009). How to use the DGI data governance framework to configure your program. *Data Governance Institute, 17.*