บันทึกข้อความ

ส่วนราชการ สสพ. โทร ๐๒-๒๔๑๐๗๗๗ ต่อ ๑๖

ที่ ๑๙๖ / ๒๕๖๖ **วันที่** ๙ สิงหาคม ๒๕๖๖

เรื่อง ผลการทบทวนแผนการดำเนินงานตามตัวชี้วัด ที่ ๒ (ข้อย่อย ๒.๒ และ ๒.๓) ๓ และ ๔

เรียน หัวหน้าฝ่ายอำนวยการ

ตามเกณฑ์การประเมินรัฐวิสาหกิจทางด้านการพัฒนาเทคโนโลยีดิจิทัล ที่กำหนดโดยสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) และบริษัท ทริส คอร์ปอเรชั่น จำกัด กำหนดตัวชี้วัดเป็น ๘ ข้อ พร้อมกำหนดเกณฑ์น้ำหนักแต่ละหัวข้อไว้ดังนี้

หัวข้อ	น้ำหนัก (ร้อยละ)
๑. การกำกับดูแลด้านเทคโนโลยีดิจิทัลและแผนปฏิบัติการดิจิทัลขององค์กร (Digital Governance and Roadmap)	๒๕
๒. การนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร (Digital Transformation)	๒๕
๓. การบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันระหว่างหน่วยงาน (Government Integration)	๑๐
๔. การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management)	๑๐
๕. การบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management)	๑๐
๖. การบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบ (Business Continuity and Availability Management)	๑๐
๗. การดำเนินการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม (Resource Optimization Management)	๑๐
รวม	**๑๐๐**

โดยในเดือน กรกฎาคม ส่วนสารสนเทศได้ดำเนินการทบทวนแผนการดำเนินงานตามตัวชี้วัดข้อ ๒ การนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร (Digital Transformation) ข้อย่อย ๒.๒ การบริหารโครงการและการดำเนินงินด้านเทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (Project Management) และข้อย่อย ๒.๓ การจัดการด้านคุณภาพ (Quality Management) ข้อ ๓ การบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันระหว่างหน่วยงาน (Government Integration) ตัวชี้วัดที่ ๔ การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management) ตามกระบวน และแนวทางปฏิบัติอย่างเป็นระบบที่สามารถทำซ้ำได้ (Repeatable Practice) และเป็นมาตรฐาน (Standardized Practice) ครบถ้วนเรียบร้อย สมบูรณ์แล้ว

จึงเรียนมาเพื่อโปรดเสนอผู้อำนวยการพิจารณาเห็นชอบและแจ้งเวียนผู้เกี่ยวข้องต่อไป

เรียน ผู้อำนวยการ
เพื่อโปรดพิจารณาเห็นชอบ
และแจ้งเวียนผู้เกี่ยวข้องต่อไป

(นางสาววิมลรัตน์ บุญโยดม)
หัวหน้าฝ่ายอำนวยการ

ปชาดา บุตรครุธ
(นางสาวปชาดา บุตรครุธ)
หัวหน้าส่วนสารสนเทศและพัฒนาระบบ

100866

- เห็นชอบผลการชดชายแผนฯ
- แจ้งเวียนผู้เกี่ยวข้อง

พันโท
(นราวิทย์ เปาอินทร์)
ผู้อำนวยการโรงงานไพ่
๑๐ ส.ค. ๒๕๖๖

KPI4 การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management)

เอกสารโดย

ส่วนสารสนเทศและพัฒนาระบบ โรงงานไพ่ กรมสรรพสามิต

รหัสเอกสาร IT-DOC-KPI4-001
ปรับปรุงล่าสุด 7 สิงหาคม 2566

บทสรุปผู้บริหาร (EXECUTIVE SUMMARY)

ข้อมูลจัดเป็นทรัพย์สินที่สำคัญในการดำเนินงานของหน่วยงาน ภาครัฐจึงได้ให้ความสำคัญกับการนำข้อมูลมาใช้สนับสนุนการขับเคลื่อนนโยบายเศรษฐกิจและสังคมดิจิทัลให้กับทุกภาคส่วน แต่ในปัจจุบันหน่วยงานภาครัฐยังประสบกับปัญหาและอุปสรรคในการดำเนินงานในด้านต่าง ๆ ที่เกี่ยวข้องกับข้อมูล ซึ่งเป็นประเด็นปัญหาเชิงนโยบายและปฏิบัติ ทั้งในเรื่องความซ้ำซ้อนของข้อมูล ความมั่นคงปลอดภัยของข้อมูล (เช่น การรักษาความลับ การเข้าถึงข้อมูล การรักษาความเป็นส่วนบุคคล) คุณภาพของข้อมูล (เช่น ความถูกต้อง ความครบถ้วน ความเป็นปัจจุบัน) การเปิดเผยข้อมูล (เช่น หน่วยงานเจ้าของข้อมูลไม่อนุญาตให้เข้าถึงข้อมูล กระบวนการขอใช้ข้อมูลซับซ้อนและใช้เวลานาน ข้อมูลไม่อยู่ในรูปแบบที่ใช้งานต่อได้ง่าย) และยังไม่มีการนำข้อมูลไปใช้ประโยชน์อย่างเป็นรูปธรรม ประเด็นปัญหาและอุปสรรคเหล่านี้อาจเป็นผลมาจากการบริหารจัดการข้อมูลที่ไม่ครอบคลุมและไม่ชัดเจนของหน่วยงาน ดังนั้นจึงจำเป็นต้องให้หน่วยงานมีมาตรการและแนวปฏิบัติในธรรมาภิบาลข้อมูลและบริหารจัดการข้อมูลที่มีประสิทธิภาพและประสิทธิผลจากการศึกษาเกี่ยวกับธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล (Data Governance) พบว่า ธรรมาภิบาลข้อมูลภาครัฐถือเป็นหัวใจสำคัญในการบริหารจัดการข้อมูล (Data Management) กล่าวคือ ธรรมาภิบาลข้อมูลภาครัฐเป็นกลไกในการกำหนดทิศทาง ควบคุม และทวนสอบการบริหารจัดการข้อมูล เพื่อให้หน่วยงานได้ดำเนินการบริหารจัดการข้อมูลตามนโยบาย กฎระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ ธรรมาภิบาลข้อมูลภาครัฐที่ดีก่อให้เกิดการบริหารจัดการข้อมูลที่ดี ส่งผลให้ข้อมูลมีความมั่นคงปลอดภัย มีคุณภาพ มีคุณค่าทางเศรษฐกิจและสังคม และมีความคุ้มทุนต่อการดำเนินงาน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงานภาครัฐ ถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัยได้จริง ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) ในเอกสารฉบับนี้จึงถูกจัดทำขึ้น เพื่อกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูล โดยประกอบด้วย สภาพแวดล้อมของธรรมาภิบาลข้อมูลภาครัฐ กฎเกณฑ์หรือนโยบายที่เกี่ยวข้องกับการดำเนินงานกับข้อมูล บทบาทและความรับผิดชอบในธรรมาภิบาลข้อมูลภาครัฐ กระบวนการธรรมาภิบาลข้อมูลภาครัฐ และการวัดการดำเนินการและความสำเร็จของธรรมาภิบาล กล่าวคือ บุคคลที่ได้รับบทบาทในธรรมาภิบาลจะมีหน้าที่ในการกำหนดขอบเขต กฎเกณฑ์ และนโยบายข้อมูลที่ใช้ในกระบวนการธรรมาภิบาล เพื่อควบคุมและตรวจสอบการดำเนินงานที่เกี่ยวข้องกับข้อมูล ตั้งแต่การสร้าง การจัดเก็บ การประมวลผล การใช้ การเผยแพร่ จนถึงการทำลาย โดยกฎเกณฑ์และนโยบายข้อมูลต้องสอดคล้องกับสภาพแวดล้อมและวัฒนธรรมองค์กรของแต่ละหน่วยงาน การวัดผลการดำเนินการช่วยให้เห็นระดับการดำเนินการของธรรมาภิบาลข้อมูลภาครัฐ ซึ่งส่งผลต่อความสำเร็จของการดำเนินการหรือคุณภาพของข้อมูล ธรรมาภิบาลข้อมูลภาครัฐจะเป็นแนวทางให้หน่วยงานภาครัฐ ทั้งส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานของรัฐรูปแบบใหม่ นำไปปรับใช้ให้เข้ากับลักษณะเฉพาะของแต่ละหน่วยงานเพื่อให้สามารถปรับตัวตามบริบทที่เปลี่ยนแปลงอย่างต่อเนื่อง

สารบัญ

สารบัญ

บทที่ 1
บทนำ (INTRODUCTION)

1.1 ความเป็นมา

ข้อมูลจัดเป็นหนึ่งในทรัพย์สินที่สำคัญและเป็นกลไกในการขับเคลื่อนการดำเนินงานของหน่วยงานเพื่อนำไปสู่เป้าหมายที่ได้กำหนดไว้ อย่างไรก็ตามสถานการณ์ด้านการบริหารจัดการข้อมูลและการใช้ประโยชน์จากข้อมูลของหน่วยงานภาครัฐในปัจจุบันนั้นยังมีอุปสรรคในด้านต่างๆ ทั้งในด้านการจัดเก็บข้อมูล (เช่น ข้อมูลเดียวกันแต่จัดเก็บกระจายไปในหลายระบบ หลายส่วนงาน หลายรูปแบบ) ด้านการเปิดเผยข้อมูล (เช่น หน่วยงานเจ้าของข้อมูลไม่อนุญาตให้เข้าถึงข้อมูล กระบวนการขอใช้ข้อมูลซับซ้อนและใช้เวลานาน ข้อมูลไม่อยู่ในรูปแบบที่ใช้งานต่อได้ง่าย) ด้านความมั่นคงปลอดภัยของข้อมูล (เช่น การรักษาความลับ การเข้าถึง ความเป็นส่วนบุคคล) และด้านคุณภาพของข้อมูล (เช่น ความถูกต้อง ความสมบูรณ์ ความต้องกัน ความเป็นปัจจุบัน ตรงตามความต้องการใช้งาน ความพร้อมใช้) สาเหตุของปัญหานั้นมาจากการขาดการวางแผนในการบริหารจัดการข้อมูลทั้งระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูล (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 จะต้องอาศัยธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) ที่เอื้อให้หน่วยงานภาครัฐต่างๆ สามารถนำไปใช้ธรรมาภิบาลและบริหารจัดการข้อมูลของหน่วยงานภาครัฐทุกขั้นตอนอย่างเป็นระบบและมีความชัดเจนมากยิ่งขึ้น

1.2 วัตถุประสงค์

การจัดทำธรรมาภิบาลข้อมูลภาครัฐ เพื่อให้หน่วยงานภาครัฐสามารถนำไปผลักดัน และดำเนินการในธรรมาภิบาลข้อมูลภาครัฐ รวมถึงติดตามการบริหารจัดการข้อมูลให้มีความโปร่งใส ตรวจสอบได้ ส่งผลต่อคุณภาพ ความมั่นคงปลอดภัย และบูรณาการข้อมูลได้อย่างครบถ้วน ถูกต้อง และข้อมูลเป็นปัจจุบัน

1.3 หน่วยงานภาครัฐที่นำไปใช้

ธรรมาภิบาลข้อมูลภาครัฐนี้ครอบคลุมถึงธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูลภายในหน่วยงานภาครัฐทั้ง 4 ประเภท คือ ส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานของรัฐรูปแบบใหม่ ดังนี้

1) ส่วนราชการ หมายถึง หน่วยงานที่รับผิดชอบการให้บริการสาธารณะทางปกครอง ซึ่งเป็นภารกิจหลักของรัฐ ให้บริการเป็นการทั่วไปและไม่มุ่งกำไร และมีความสัมพันธ์กับรัฐ

2) รัฐวิสาหกิจ หมายถึง หน่วยงานที่รับผิดชอบบริการสาธารณะทางอุตสาหกรรมและพาณิชยกรรม มีวัตถุประสงค์เพื่อการแสวงหารายได้ ต้องสามารถเลี้ยงตัวเองจากการดำเนินงานเชิงพาณิชย์ แต่สามารถรับเงินงบประมาณสนับสนุนเป็นครั้งคราวหรือบางส่วนในบางกรณี

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

4) หน่วยงานของรัฐรูปแบบใหม่ หมายถึง

- องค์การของรัฐที่เป็นอิสระ (Independent Administrative Organization) ซึ่งเป็นหน่วยงานรูปแบบใหม่ที่จัดตั้งขึ้น เพื่อทำหน้าที่ในการควบคุมกำกับดูแลกิจกรรมของรัฐ ตามนโยบายสำคัญที่ต้องการความเป็นกลางอย่างเคร่งครัด

- กองทุนที่เป็นนิติบุคคล ซึ่งเป็นเครื่องมือทางเศรษฐกิจของรัฐ หมายถึง นิติบุคคลที่จัดตั้งขึ้นโดยตราเป็นพระราชบัญญัติ เนื่องจากต้องการอำนาจรัฐในการบังคับฝ่ายเดียวต่อภาคเอกชน หรือประชาชนในการสมทบเงินเข้ากองทุน

ธรรมาภิบาลข้อมูลภาครัฐในพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล ได้กำหนดหน่วยงานของรัฐ หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์การมหาชน รัฐสภา ศาล (ครอบคลุมเพียงหน่วยงานของศาลในส่วนที่ไม่เกี่ยวกับการพิจารณาอรรถคดี) องค์การอิสระตามรัฐธรรมนูญ องค์การอัยการ สถาบันอุดมศึกษาของรัฐ และหน่วยงานอิสระของรัฐ

1.4 ขอบเขตของเนื้อหาภายในธรรมาภิบาลข้อมูลภาครัฐ

ขอบเขตของธรรมาภิบาลข้อมูลภาครัฐในเอกสารฉบับนี้ ประกอบด้วย บทที่ 2 อธิบายถึงแนวคิดธรรมาภิบาลข้อมูลภาครัฐ ประกอบด้วย นิยามของธรรมาภิบาลข้อมูลภาครัฐ ความหมายและประเภทข้อมูลการบริหารจัดการข้อมูล ความสัมพันธ์ระหว่างธรรมาภิบาลข้อมูลภาครัฐกับการบริหารจัดการข้อมูล บทที่ 3 กล่าวถึงกรอบธรรมาภิบาลข้อมูลภาครัฐ ประกอบด้วย โครงสร้างของธรรมาภิบาลข้อมูลภาครัฐ กระบวนการธรรมาภิบาลข้อมูลภาครัฐ สภาพแวดล้อมของธรรมาภิบาลข้อมูลภาครัฐ การนิยามข้อมูล กฎเกณฑ์ข้อมูล และการวัดการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูลภาครัฐ

บทที่ 2
แนวคิดธรรมาภิบาลข้อมูลภาครัฐ
(DATA GOVERNANCE FOR GOVERNMENT CONCEPT)

2.1 นิยามของธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government Definition)

ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) ได้มีผู้เชี่ยวชาญจากหน่วยงานต่าง ๆ ให้คำนิยามไว้ ดังนี้

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

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

“การกำหนดสิทธิและการควบคุม (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 ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) คือ “การกำหนดสิทธิในการตัดสินใจและความรับผิดชอบ ในการส่งเสริมให้เกิดกระบวนการจัดทำ การใช้งาน และการบริหารจัดการข้อมูล รวมถึงกระบวนการที่กำหนดบทบาท นโยบาย และมาตรฐานที่ช่วยสนับสนุนให้การดำเนินงานเกี่ยวกับข้อมูลมีประสิทธิภาพมากยิ่งขึ้น ซึ่งส่งผลให้หน่วยงานสามารถบรรลุเป้าหมายได้”

ในมุมมองของภาครัฐ ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) หมายถึง “การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย โดยใช้ข้อมูลเป็นหลักในการขับเคลื่อนประเทศ เช่น การใช้ข้อมูลในการวิเคราะห์การตัดสินใจเชิงนโยบายและการบริหารราชการแผ่นดิน การเพิ่มประสิทธิภาพในการบริการประชาชน การเสริมสร้างและผลักดันธุรกิจที่เกิดจากการใช้นวัตกรรมข้อมูล” ทั้งนี้ Intra-governmental Group on Geographic Information (IGGI, 2005) ให้องค์ประกอบหลักของธรรมาภิบาลข้อมูลภาครัฐที่ดี ประกอบไปด้วย

1) มีความมั่นคงปลอดภัยและรักษาความเป็นส่วนบุคคล โดยมีมาตรการในการรักษาความมั่นคงปลอดภัย
และความเป็นส่วนบุคคล ซึ่งช่วยป้องกันความเสียหายที่จะเกิดขึ้นกับข้อมูลและการละเมิดสิทธิส่วนบุคคล

2) มีมาตรการควบคุมและจัดการระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูล ซึ่งประกอบด้วย การประเมินธุรกิจ การกำหนดประเภทและแนวทางการแบ่งประเภทของชุดข้อมูล มีการตรวจสอบอย่างต่อเนื่อง ทั้งการเก็บข้อมูลและการทำลายข้อมูล

3) มีนโยบายการใช้ข้อมูลที่ชัดเจน โดยกำหนดนโยบายและกฎเกณฑ์ของข้อมูลเป็นสำหรับธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล

4) มีการกำหนดบทบาทหน้าที่ของเจ้าของข้อมูล โดยกำหนดวิธีการที่ผู้ดูแลข้อมูลหรือเจ้าของข้อมูลสามารถจัดการ เปลี่ยนแปลง หรือส่งผ่านข้อมูลให้ชัดเจน เพื่อไม่ให้เกิดปัญหาในกรณีที่ชุดข้อมูลหรือฐานข้อมูลบางแหล่งอาจจะมีผู้ดูแล ผู้ใช้งาน หรือเจ้าของข้อมูลหลายคนหรือหลายหน่วยงาน

5) ข้อมูลมีMetadata โดยMetadataจะช่วยให้ผู้ใช้งานเข้าใจว่าข้อมูลชุดนี้คือข้อมูลที่เกี่ยวข้องกับอะไรสามารถนำไปใช้งานอย่างไร และมีข้อจำกัดอะไร โดยมีมาตรฐานของMetadataที่เหมาะสมกับการใช้งาน

6) ข้อมูลมีคุณภาพ โดยมีมาตรการในการควบคุมคุณภาพของข้อมูลให้มีคุณภาพสูง ซึ่งจะสนับสนุนให้การดำเนินงานของหน่วยงานเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

ดังนั้น สรุปได้ว่า ธรรมาภิบาลข้อมูลภาครัฐ หมายความว่า การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลภาครัฐทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลของหน่วยงานของรัฐไปใช้อย่างถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงแลกเปลี่ยน และบูรณาการระหว่างกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย โดยใช้ข้อมูลเป็นหลักในการบริหารงานภาครัฐและการบริการสาธารณะ

2.2 ข้อมูล (Data)

ข้อมูล คือ “ข้อเท็จจริงซึ่งใช้เป็นพื้นฐานสำหรับการอธิบายเหตุผล การสนทนา หรือการคำนวณ” (Australian Institute of Health and Welfare, 2014) ข้อมูลจัดเป็นองค์ประกอบหลักในการขับเคลื่อนหน่วยงาน ซึ่งมีความสัมพันธ์กับกระบวนการปฏิบัติงาน เทคโนโลยีสารสนเทศ สถานที่ รวมถึงบุคลากรข้อมูลจึงเปรียบเสมือนทรัพย์สินที่มีความสำคัญเช่นเดียวกับทรัพย์สินประเภทอื่น ดังนั้นหน่วยงานจึงจำเป็นต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล เช่น การรักษาความลับของข้อมูล (Confidentiality) การป้องกันไม่ให้เกิดเหตุการณ์ที่ทำให้ไม่สามารถใช้งานข้อมูลได้ (Loss of Availability) การรักษาความถูกต้องครบถ้วนของข้อมูล (Integrity) การทำให้ข้อมูลเป็นปัจจุบันอยู่เสมอ (Timeliness) ทั้งนี้เพื่อตอบสนองต่อการตัดสินใจทั้งในระดับปฏิบัติการและระดับยุทธศาสตร์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

2.2.1 ประเภทข้อมูล (Types of Data)

ข้อมูลถูกจัดแบ่งออกได้เป็น 3 ประเภท ดังนี้

รูปที่ 1 ประเภทข้อมูล

1) ข้อมูลที่มีโครงสร้าง (Structured Data) เป็นข้อมูลที่มีการนิยามโครงสร้างของข้อมูลไว้ โดยนิยามความหมายและคุณสมบัติของแต่ละฟิลด์ข้อมูล โครงสร้างมีชั้นเดียวทำให้ง่ายต่อการค้นหา เช่น ตารางข้อมูลในฐานข้อมูล Comma-Separated Values – CSV ดังแสดงในตารางที่ 1

2) ข้อมูลกึ่งโครงสร้าง (Semi-structured Data) เป็นข้อมูลที่มีการนิยามโครงสร้างของข้อมูลไว้แต่โครงสร้างเป็นแบบลำดับขั้น (Hierarchy) เช่น Extensible Markup Language – XML JavaScript Object Notation - JSON

3) ข้อมูลที่ไม่มีโครงสร้าง (Unstructured Data) เป็นข้อมูลที่ไม่ได้มีการนิยามโครงสร้างของข้อมูลไว้ มักจะอยู่ในรูปแบบ เช่น ข้อความ รูปภาพ เสียง วีดิทัศน์

2.2.2 ชุดข้อมูล (Datasets)

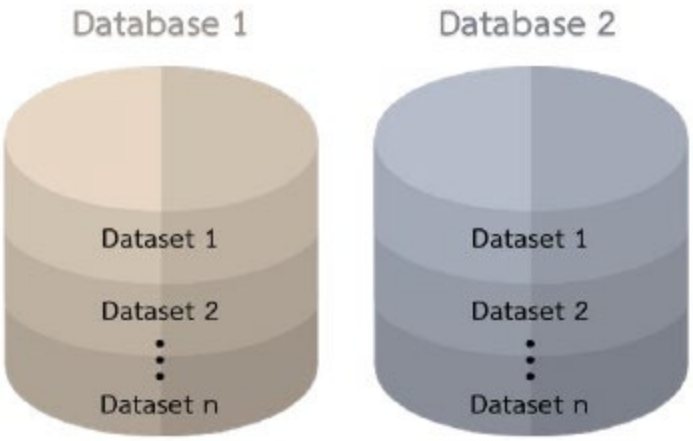
ชุดข้อมูล คือ “ข้อมูลที่มีการรวบรวมไว้ โดยปกติอยู่ในรูปแบบของตารางข้อมูล” (Askham et al., 2013) ซึ่งการรวบรวมข้อมูลนี้มาจากหลายแหล่ง และนำข้อมูลมาจัดเป็นชุดให้ถูกต้องตามลักษณะโครงสร้างข้อมูลที่กำหนดไว้ ดังตารางที่ 1 แสดงตัวอย่างชุดข้อมูลพนักงานในรูปแบบตารางข้อมูลหรือข้อมูลที่มีโครงสร้าง (Structured Data) มีทั้งหมด 3 แถว 5 ฟิลด์ (Data Field/Element/Attribute) ได้แก่ ชื่อ นามสกุล เพศ อายุ และระดับการศึกษา

ตารางที่ 1 ตัวอย่างชุดข้อมูลพนักงาน

ชื่อ	นามสกุล	เพศ	อายุ	ระดับการศึกษา
สุระเดช	ชัยสงค์	ชาย	41	ปริญญาโท
วิภาดา	ธรรมรงค์	หญิง	36	ปริญญาตรี
ณรงค์	นาเย็น	ชาย	32	ปริญญาตรี

2.2.3 ฐานข้อมูล (Database)

ฐานข้อมูล คือ “กลุ่มข้อมูลที่มีความสัมพันธ์กันได้ถูกรวบรวมเข้าไว้ด้วยกัน ซึ่งสนับสนุนกิจกรรมของหน่วยงาน” (Malinowski, E. & Zimányi, E., 2009) หรือกล่าวได้ว่า แต่ละฐานข้อมูลจะประกอบไปด้วยหลายๆ ชุดข้อมูลที่มีความสัมพันธ์กันดังแสดงในรูปที่ 2



รูปที่ 2 ความสัมพันธ์ระหว่างฐานข้อมูลกับชุดข้อมูล

2.3 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 ซึ่งแต่ละหน่วยงานต้องตระหนักว่าข้อมูลที่มีอยู่เป็นทรัพย์สินที่มีค่า และจากการเกิดขึ้นของข้อมูลที่มีปริมาณมหาศาล ไม่ว่าจะเป็นข้อมูลที่รวบรวมมาโดยอัตโนมัติจากระบบหรืออุปกรณ์ต่าง ๆ หรือข้อมูลที่เกิดขึ้นจากการป้อนข้อมูลหรือโต้ตอบกับผู้ใช้งาน เพื่อให้หน่วยงานสามารถนำข้อมูลเหล่านี้ไปประมวลผลหรือใช้ในการตัดสินใจได้อย่างแม่นยำ จึงต้องได้รับการบริหารจัดการอย่างถูกต้อง เหมาะสม และสอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูลของหน่วยงาน เช่น

1) เพื่อการจัดเก็บ นำมาใช้งาน และประมวลผลข้อมูลตามที่หน่วยงานต้องการ

2) เพื่อควบคุม ตรวจสอบ และป้องกัน โดยใช้กระบวนการธรรมาภิบาลข้อมูลภาครัฐและความปลอดภัยของข้อมูล

3) เพื่อจัดหมวดหมู่ และกำหนดมาตรฐานของข้อมูล โดยใช้การจำแนกข้อมูล และกำหนดกรอบการทำงานที่เป็นที่รู้จักแพร่หลาย

4) เพื่อให้สามารถนำข้อมูลกลับมาใช้ได้ในภายหลัง โดยกำหนดข้อมูลให้อยู่ในรูปแบบที่เรียกใช้ได้อย่างมีประสิทธิภาพ

5) เพื่อการปรับปรุงข้อมูลให้เป็นปัจจุบัน และมีความถูกต้องสมบูรณ์อยู่เสมอ

6) เพื่อการปกป้องข้อมูลจากการลักลอบใช้งานหรือแก้ไขโดยมิชอบ รวมถึงจากเหตุการณ์ที่อาจเกิดจากภัยธรรมชาติหรือความบกพร่องภายในระบบคอมพิวเตอร์

ซึ่งในการบริหารจัดการข้อมูลนั้น มีองค์ประกอบในการบริหารจัดการตลอดทั้งระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล ดังรูปที่ 3

รูปที่ 3 ระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูลและองค์ประกอบในการบริหารจัดการข้อมูล

2.3.1 ระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล (Data Life Cycle)

ระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล คือ “ลำดับขั้นตอนของข้อมูล ตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล” ประกอบด้วย 6 ขั้นตอน ดังนี้

1) กระบวนการสร้างข้อมูล (Create) เป็นการสร้างข้อมูลขึ้นมาใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์ตรวจจับสัญญาณ (Sensor) รวมถึงการซื้อข้อมูล หรือการรับข้อมูลจากหน่วยงานอื่น เพื่อนำมาจัดเก็บในภายหลัง

2) กระบวนการจัดเก็บข้อมูล (Store) เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้าง หรือข้อมูลที่ได้จากการแลกเปลี่ยนกับหน่วยงานอื่น เพื่อให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหาย หรือถูกทำลาย และให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS)

3) กระบวนการใช้ข้อมูล (Use) เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูลการเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ รวมถึงการสำรอง (Backup) ข้อมูล โดยการคัดลอกข้อมูลที่ใช้งานอยู่ในปัจจุบัน เพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)

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

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

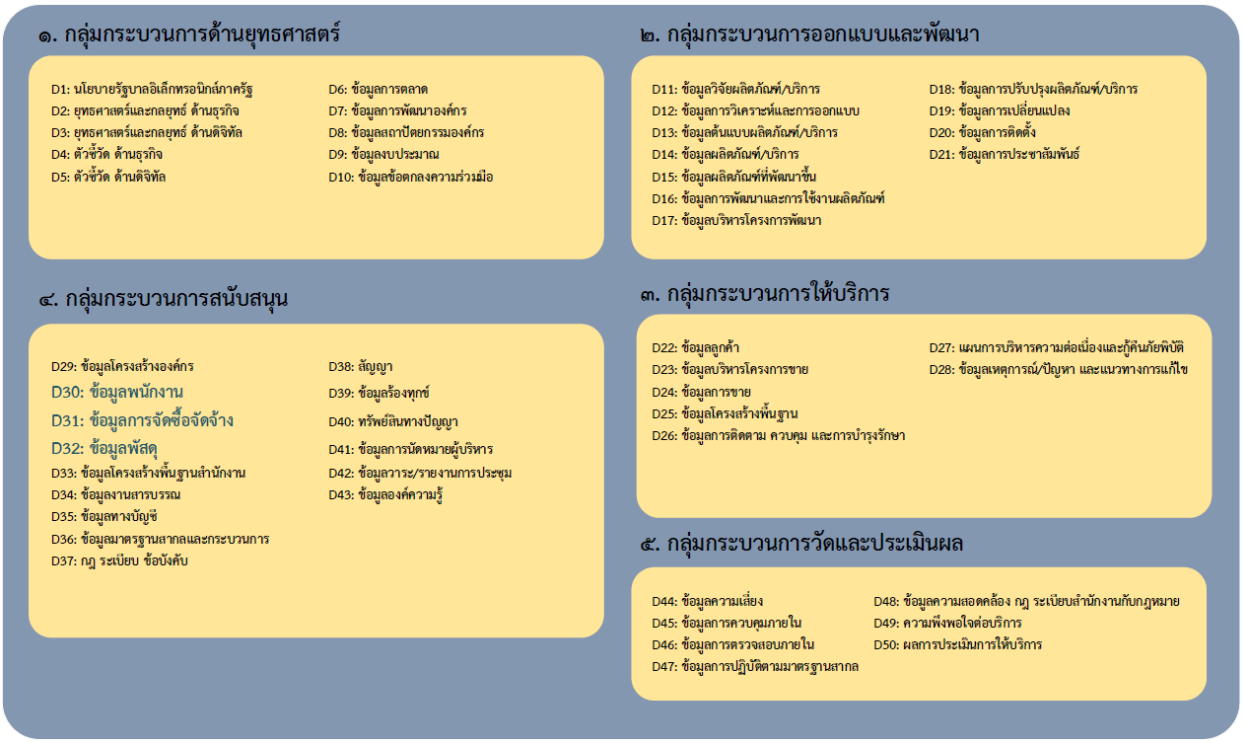
6) กระบวนการทำลายข้อมูล (Destroy) เป็นการทำลายข้อมูล ซึ่งปกติจะเป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด

2.3.2 องค์ประกอบในการบริหารจัดการข้อมูล (Data Management Component)

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

2.3.2.1 สถาปัตยกรรมข้อมูล (Data Architecture)

สถาปัตยกรรมข้อมูล (Data Architecture) เป็นส่วนหนึ่งของการพัฒนาสถาปัตยกรรมองค์กร (Enterprise Architecture) เป็นการอธิบายเกี่ยวกับกลุ่มของข้อมูลทั้งหมดที่มีในหน่วยงาน ความสัมพันธ์ระหว่างข้อมูลกับกระบวนการปฏิบัติงาน ความสัมพันธ์ระหว่างข้อมูลกับแอปพลิเคชัน สถาปัตยกรรมเทคโนโลยีข้อมูล สถาปัตยกรรมการบูรณาการข้อมูล สถาปัตยกรรมMetadata เป็นต้น สถาปัตยกรรมข้อมูลจะอยู่ในรูปแบบของแบบจำลองข้อมูลที่มองเห็นภาพรวม ความเชื่อมโยง และการไหลของข้อมูลในระดับต่างๆ ทั้งหมดของหน่วยงาน ทั้งที่เป็นหน่วยงานต้นน้ำ กลางน้ำ หรือปลายน้ำ สามารถอธิบายสถานะที่มีอยู่ในปัจจุบันและกำหนดความต้องการสำหรับอนาคต เพื่อให้หน่วยงานเกิดความเข้าใจ และเห็นเป็นภาพเดียวกัน ดังนั้นจึงเป็นพื้นฐานที่สำคัญในการวางแผนบริหารจัดการข้อมูล



รูปที่ 4 ตัวอย่างความสัมพันธ์ระหว่างกลุ่มข้อมูลกับกลุ่มกระบวนการปฏิบัติงาน

จากรูปที่ 4 ตัวอย่างความสัมพันธ์ระหว่างกลุ่มข้อมูลกับกลุ่มกระบวนการปฏิบัติงาน ซึ่งชี้ให้เห็นถึงภาพรวมของข้อมูลทั้งหมดที่มีการดำเนินการในแต่ละกลุ่มกระบวนการปฏิบัติงานกอง หรือส่วนงานภายในหน่วยงาน ความสัมพันธ์นี้สามารถใช้เป็นจุดเริ่มต้นในการจัดลำดับความสำคัญของข้อมูล กำหนดขอบเขต กำหนดอัตรากำลังคน และจัดสรรงบประมาณสำหรับธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล จากตารางที่ 2 แสดงความสัมพันธ์ระหว่างข้อมูลกับแอปพลิเคชันในงานบริหารจัดการพัสดุ ซึ่งชี้ให้เห็นว่าข้อมูลเดียวกันอาจจะมีการใช้งานหรือเก็บซ้ำซ้อนกันในหลายๆ แอปพลิเคชัน

ดังนั้นความสัมพันธ์ระหว่างข้อมูลกับแอปพลิเคชันสามารถสนับสนุนการบูรณาการข้อมูล (Data Integration) ได้จากการที่ข้อมูลกระจายอยู่ตามแอปพลิเคชันต่างๆ ตัวอย่างสถาปัตยกรรมการบูรณาการข้อมูล ซึ่งแสดงความสัมพันธ์ระหว่างคลังข้อมูล ดาต้าเลค ระบบรายงานอัจฉริยะ และดาต้าอนาไลติกส์

ตารางที่ 2 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

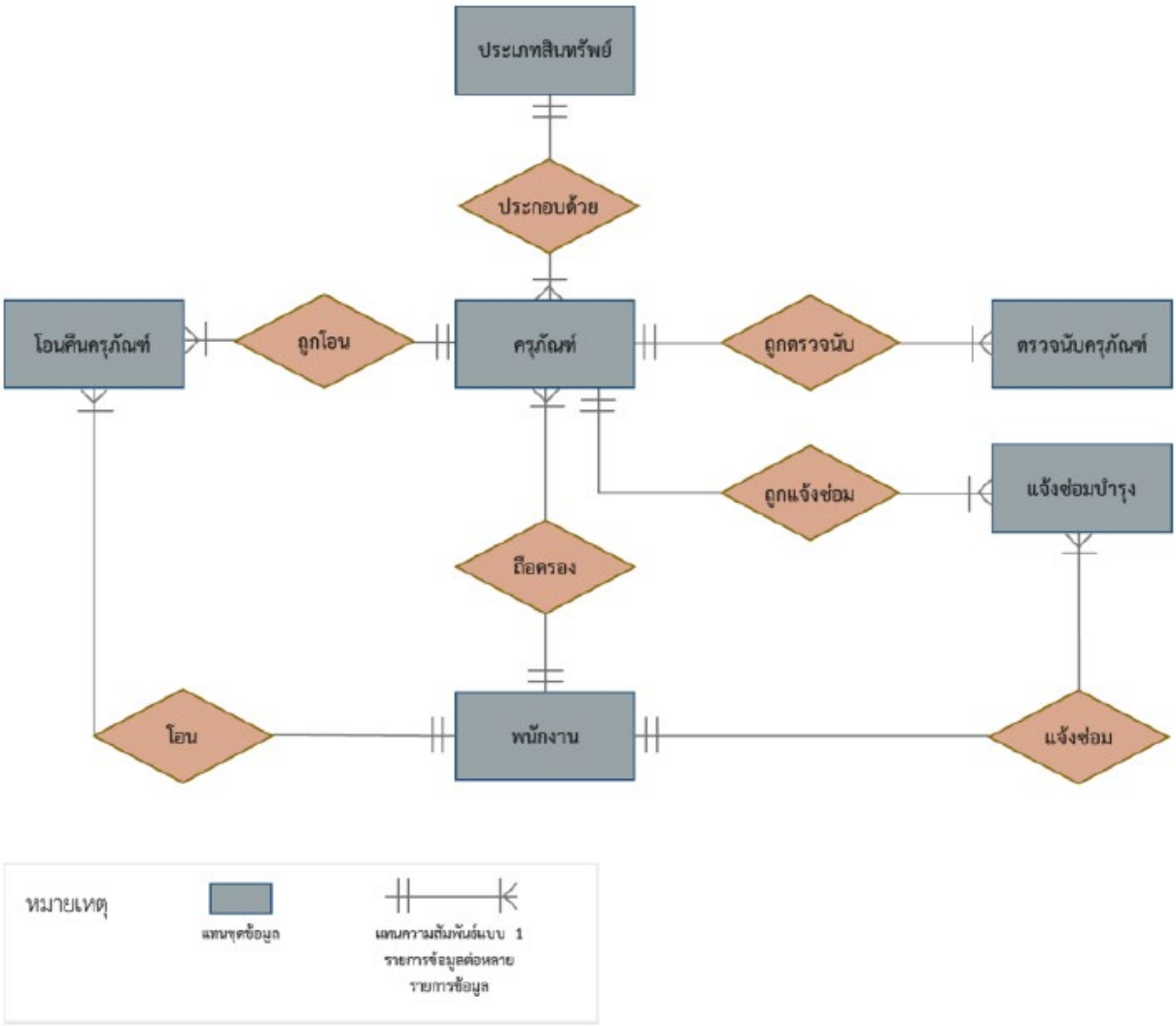
ตารางที่ 3 สรุปการบริหารจัดการสถาปตยกรรมข้อมูล

การบริหารจัดการสถาปัตยกรรมข้อมูล	
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)

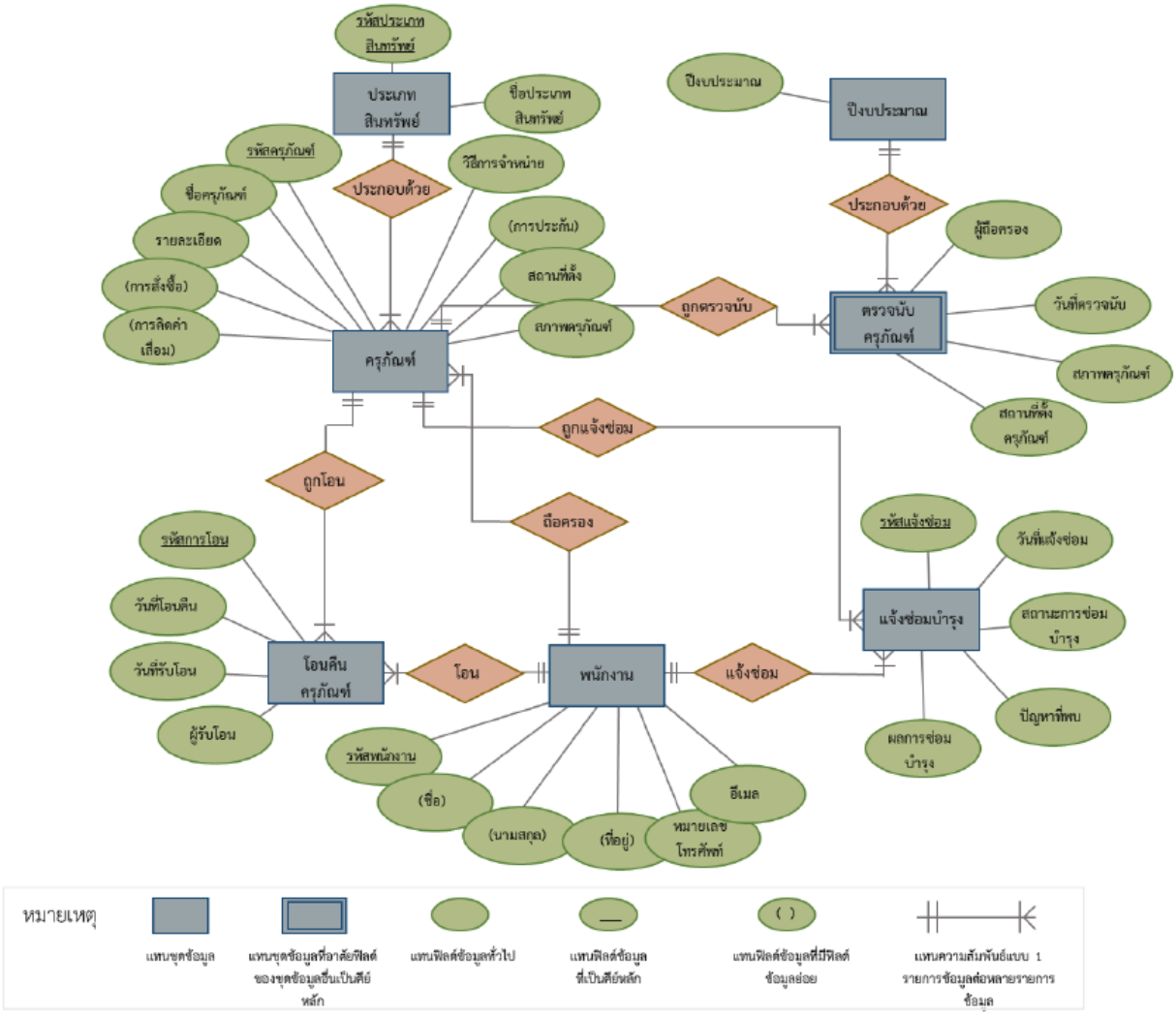
2.3.2.2 การจำลองและการออกแบบข้อมูล (Data Modeling and Design)

การจำลองและการออกแบบข้อมูล (Data Modeling and Design) เป็นวิธีการวิเคราะห์ความต้องการของผู้ใช้งาน รวมถึงระบุข้อกำหนดและการแก้ปัญหาต่าง ๆ ที่เกี่ยวข้อง แบบจำลองข้อมูลแสดงในรูปแบบของไดอะแกรม (Diagram)ที่มีการออกแบบลักษณะโครงสร้างของข้อมูล เพื่อใช้ในการสื่อสารภายในหน่วยงานให้เข้าใจตรงกัน แบบจำลองข้อมูลจะแสดงถึงความสัมพันธ์ระหว่างข้อมูลที่เกี่ยวข้องกันพร้อมทั้งรายละเอียดของโครงสร้างของข้อมูล โดยแบ่งออกเป็น 3 ระดับ ได้แก่ (1) แบบจำลองข้อมูลเชิงความคิด (Conceptual Data Model) (2) แบบจำลองข้อมูลเชิงตรรกะ (Logical Data Model) และ (3) แบบจำลองข้อมูลเชิงกายภาพ (Physical Data Model)

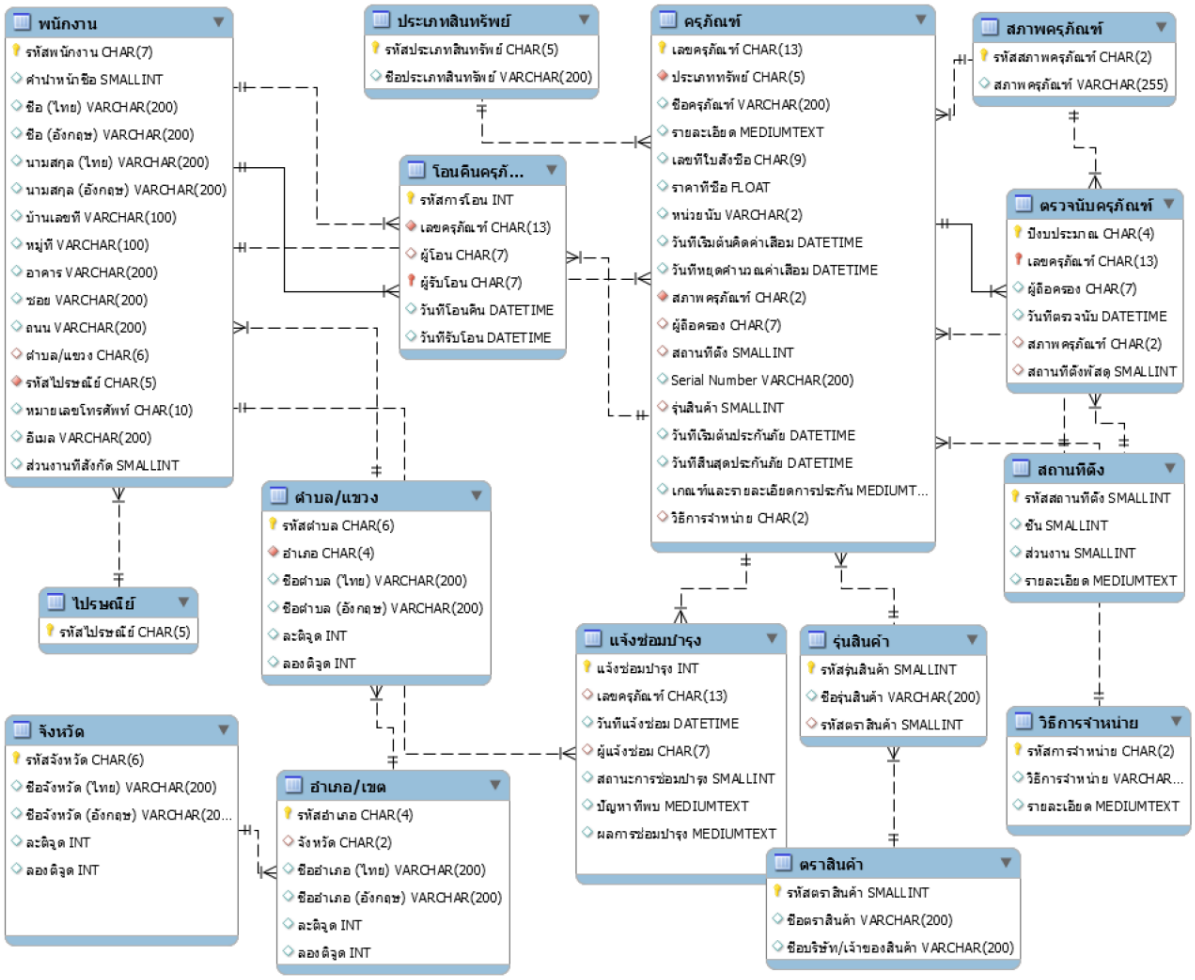
ขั้นตอนในการสร้างแบบจำลองและการออกแบบข้อมูล เริ่มตั้งแต่การวิเคราะห์ความต้องการของผู้ใช้เพื่อกำหนดเป็นแบบจำลองข้อมูลเชิงความคิดของข้อมูลขึ้นมา เป็นขั้นตอนของการกำหนดเค้าโครงในระดับเบื้องต้น สามารถมองเห็นถึงความสัมพันธ์ของข้อมูล แต่ยังไม่สามารถนำไปใช้งานได้จริงเพราะเป็นเพียงแนวคิดเท่านั้น หลังจากนั้นทำการออกแบบข้อมูลให้มีความชัดเจนมากขึ้นโดยกำหนดเป็นแบบจำลองข้อมู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



รูปที่ 5 ตัวอย่างแบบจำลองข้อมูลเชิงความคิด (Conceptual Data Model) สำหรับงานบริหารจัดการพัสดุ



รูปที่ 6 ตัวอย่างแบบจำลองข้อมูลเชิงตรรกะ (Logical Data Model) สำหรับงานบริหารจัดการพัสดุ



รูปที่ 7 ตัวอย่างแบบจำลองข้อมูลเชิงกายภาพ (Physical Data Model) สำหรับงานบริหารจัดการพัสดุ

จากรูปที่ 6 แสดงตัวอย่างแบบจำลองข้อมูลเชิงความคิดสำหรับงานบริหารจัดการพัสดุ ซึ่งแสดงให้เห็นว่า ประเภทสินทรัพย์หนึ่งประเภท ประกอบด้วยครุภัณฑ์หลายรายการ พนักงานหนึ่งราย ถือครองครุภัณฑ์ได้หลายรายการ และแจ้งซ่อมได้หลายครั้ง ครุภัณฑ์หนึ่งรายการ สามารถโอน ตรวจนับ และแจ้งซ่อมได้ หลายครั้ง สำหรับฟิลด์ข้อมูลของแต่ละชุดข้อมูลแสดงในแบบจำลองเชิงตรรกะตามรูปที่ 7 ทั้งนี้รายละเอียดด้านเทคนิคอธิบายไว้ในรูปที่ 7 ประกอบด้วย คีย์หลัก ประเภทข้อมูล และความกว้างของฟิลด์ข้อมูล

ตารางที่ 4 สรุปการบริหารจัดการการจำลองและการออกแบบข้อมูล

การบริหารจัดการการจำลองและการออกแบบข้อมูล	
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)

2.3.2.3 การจัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operations)

การจัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operations) เป็นการจัดเก็บข้อมูลที่มีโครงสร้าง โดยจัดเก็บในรูปแบบของฐานข้อมูล ส่วนการดำเนินการกับข้อมูลจะเกี่ยวข้องตั้งแต่การวางแผนการใช้งาน การสำรองข้อมูล (Backup) การกู้คืนข้อมูล (Restore) การจัดเก็บข้อมูลถาวร (Archive)กระบวนการที่เกี่ยวข้องกับข้อมูล (Create Read Update Delete – CRUD) ตลอดทั้งระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล การโอนย้ายข้อมูล (Migration) รวมถึงการปรับปรุงประสิทธิภาพของฐานข้อมูลให้พร้อมใช้งานได้ตลอดเวลา เพื่อรักษาความมั่นคงปลอดภัยและความถูกต้องของข้อมูล

ตารางที่ 5 สรุปการบริหารจัดการการจัดเก็บและการดำเนินการกับข้อมูล

การบริหารจัดการการจัดเก็บและการดำเนินการกับข้อมูล	
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)

2.3.2.4 การบูรณาการและความสามารถในการทำงานร่วมกัน (Data Integration and Interoperability)

การเชื่อมโยงข้อมูล (Data Integration) เป็นการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ในรูปแบบที่สอดคล้องกันเข้ามารวมอยู่ในแหล่งข้อมูลเดียวกัน เพื่อนำไปใช้ในการจัดทำข้อมูลหลัก (Master Data) คลังข้อมูล (Data Warehouse) ดาต้าเลค (Data Lake) รวมถึงการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน รูปที่ 8 แสดงความสัมพันธ์ระหว่างการบูรณาการข้อมูล คลังข้อมูล และดาต้าเลค ส่วนความสามารถในการทำงานร่วมกัน (Interoperability) จะมีการกำหนดมาตรฐานหรือข้อตกลงร่วมกันระหว่างหน่วยงานหรือระบบ โดยมีการอ้างถึงคุณลักษณะของระบบต่าง ๆ ที่สามารถแลกเปลี่ยนข้อมูลกันหรือสื่อสารกันได้ เช่น มีการแลกเปลี่ยนข้อมูลในรูปแบบของ Application Programming Interfaces – API

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

ตารางที่ 6 สรุปการบริหารจัดการการบูรณาการและความสามารถในการทำงานร่วมกัน

การบริหารจัดการการบูรณาการและความสามารถในการทำงานร่วมกัน	
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)

2.3.2.5 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 7 สรุปการบริหารจัดการเอกสารและเนื้อหา

การบริหารจัดการเอกสารและเนื้อหา	
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

2.3.2.6 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 มีการกำหนดให้เป็นมาตรฐาน และใช้งานร่วมกัน มีการเปลี่ยนแปลงค่อนข้างน้อย เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัดระยะทาง ขณะที่ข้อมูลหลักมีโอกาสเปลี่ยนแปลงได้มากกว่า มีรายละเอียดหรือจำนวนฟิลด์ข้อมูลที่มากกว่าและเป็นข้อมูลที่สร้างและใช้งานร่วมกันภายในขอบเขตการดำเนินงานตามภารกิจของหน่วยงาน เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลผู้ขาย ข้อมูลสินค้า ข้อมูลครุภัณฑ์ ข้อมูลสถานที่

ตารางที่ 8 สรุปการบริหารจัดการข้อมูลหลักและข้อมูลอ้างอิง

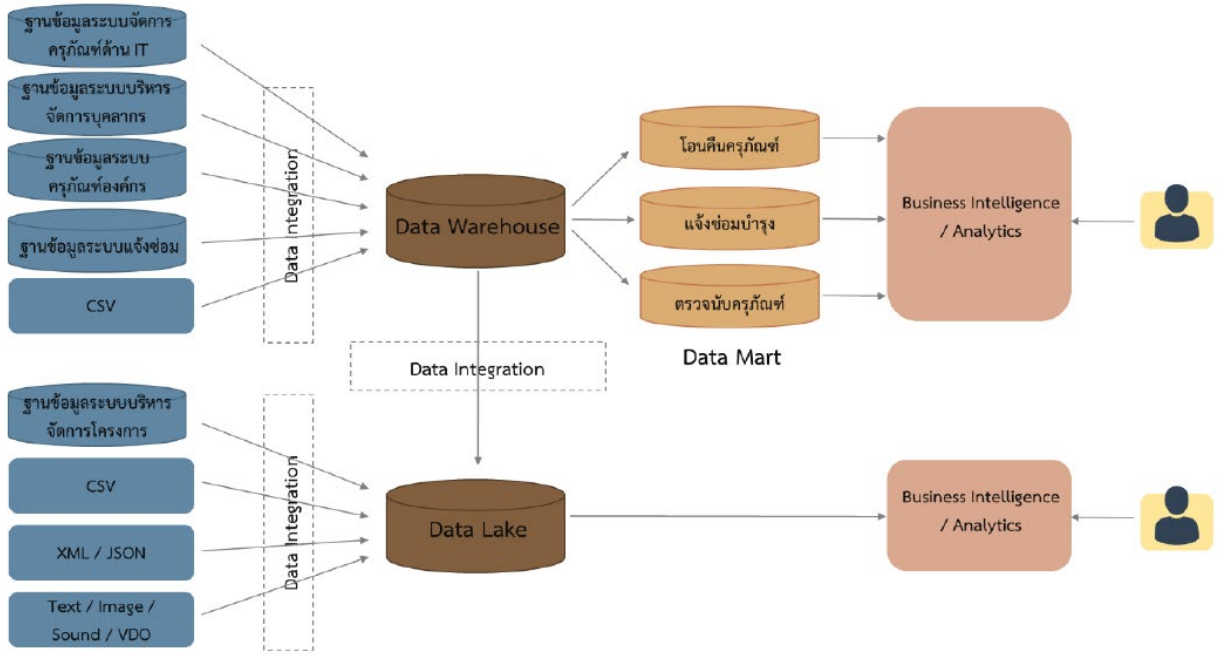
การบริหารจัดการหลักและข้อมูลอ้างอิง	
วิธีการดำเนินการ	- ทำความเข้าใจเกี่ยวกับความต้องการข้อมูลทั้งข้อมูลหลักและข้อมูลอ้างอิง - กำหนดแหล่งที่มา (Source) ของข้อมูลหลักและข้อมูลอ้างอิง - ดำเนินการจัดทำข้อมูลหลักและข้อมูลอ้างอิง
สิ่งที่นำเข้า	- อภิธานศัพท์ข้อมูล (Data Glossary)
เครื่องมือที่ใช้	- เครื่องมือบริหารจัดการข้อมูลหลัก (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)

2.3.2.7 คลังข้อมูล ดาต้าเลค ระบบรายงานอัจฉริยะ และดาต้าอนาไลติกส์ (Data Warehouse, Data Lake, Business Intelligence, and Data Analytics)

คลังข้อมูล (Data Warehouse) เป็นข้อมูลที่ได้จากการเชื่อมโยงข้อมูล (Data Integration) ซึ่งเกิดจากการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ที่มีหลากหลายรูปแบบมาเก็บในคลังข้อมูล โดยผ่านกระบวนการของ Extract Transform Load (ETL) ในรูปแบบข้อมูลที่มีโครงสร้างและถูกจัดทำให้อยู่ในรูปแบบที่เหมาะสมสำหรับการนำไปวิเคราะห์ข้อมูล ทั้งในรูปแบบของรายงานอัจฉริยะ (Business Intelligence) และดาต้าอนาไลติกส์ (Data Analytics)

ดาต้าเลค (Data Lake) เป็นแหล่งสำหรับเก็บรวบรวมข้อมูลที่มีหลากหลายรูปแบบ ข้อมูลที่จัดเก็บเป็นข้อมูลที่มีโครงสร้าง ข้อมูลกึ่งโครงสร้าง และข้อมูลที่ไม่มีโครงสร้าง โดยข้อมูลถูกเก็บรักษา

ไว้ในรูปแบบที่เหมือนหรือใกล้เคียงกับรูปแบบที่ได้รับมาจากแหล่งข้อมูลต้นฉบับ และสามารถใช้เป็นที่สำรองข้อมูลต้นฉบับได้



รูปที่ 8 ตัวอย่างความสัมพันธ์ระหว่างคลังข้อมูล ดาต้าเลค ระบบรายงานอัจฉริยะและดาต้าอนาไลติกส์สำหรับงานบริหารจัดการพัสดุ

จากรูปที่ 8 คลังข้อมูลและดาต้าเลคจะเกิดจากการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ซึ่งแต่ละแหล่งอาจจะมีรูปแบบของข้อมูลที่แตกต่างกัน การรวบรวมข้อมูลใช้วิธีการบูรณาการข้อมูล (ดูที่หัวข้อ 2.3.2.4) โดยข้อมูลจากคลังข้อมูลสามารถรวมเข้าไปที่ดาต้าเลคเพื่อใช้สำหรับการวิเคราะห์ข้อมูลที่ซับซ้อนมากยิ่งขึ้น ข้อมูลในคลังข้อมูลจะต้องถูกจัดกลุ่มออกเป็นดาต้ามาร์ท (Data Mart) โดยต้องสอดคล้องกับหน่วยงานที่จะนำไปใช้ เช่น ดาต้ามาร์ทของฝ่ายบุคคล ดาต้ามาร์ทของฝ่ายการตลาด ดาต้ามาร์ทของฝ่ายการเงิน หลังจากนั้นข้อมูลในดาต้ามาร์ทถูกนำไปใช้สำหรับการทำรายงานอัจฉริยะ (Business Intelligence) หรือการทำนายสิ่งที่จะเกิดขึ้นในอนาคตผ่านวิธีการของดาต้าอนาไลติกส์ ในกรณีของดาต้าเลคสามารถนำข้อมูลไปใช้สำหรับทำรายงานอัจฉริยะและดาต้าอนาไลติกส์ได้ทันที โดยไม่ต้องสร้างดาต้ามาร์ทหลังจากข้อมูลต่าง ๆ ถูกทำการวิเคราะห์ออกเป็นรายงานอัจฉริยะและผลการทำนายแล้ว จะถูกนำไปใช้ เพื่อสนับสนุนการตัดสินใจของหน่วยงานทั้งในระดับปฏิบัติการและระดับบริหารต่อไป

ตารางที่ 9 สรุปการบริหารจัดการคลังข้อมูล ดาต้าเลค ระบบรายงานอัจฉริยะ และดาต้าอนาไลติกส์

การบริหารจัดการคลังข้อมูล ดาตาเลค 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)

2.3.2.8 คำอธิบายชุดข้อมูลดิจิทัล หรือ Metadata (Metadata)

คำอธิบายชุดข้อมูลดิจิทัล หรือ Metadata (Metadata) เป็นข้อมูลที่ใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่น ๆ ที่เกี่ยวข้องทั้งกระบวนการเชิงธุรกิจและเชิงเทคโนโลยีสารสนเทศ กฎและข้อจำกัดของข้อมูล และโครงสร้างของข้อมูล Metadata ช่วยให้หน่วยงานสามารถเข้าใจข้อมูล ระบบ และขั้นตอนการทำงานได้ดียิ่งขึ้นโดยการบริหารจัดการ Metadata (Metadata Management) เริ่มตั้งแต่ การเก็บรวมรวม การจัดกลุ่ม การดูแล และการควบคุม Metadata ทั้งนี้ข้อมูลแต่ละชุดควรมีMetadata เพื่อให้ผู้ใช้งานทราบเกี่ยวกับชุดข้อมูล เช่น รายละเอียดชุดข้อมูล สิ่งที่เกี่ยวข้องกับชุดข้อมูล วัตถุประสงค์การนำไปใช้ฟิลด์ข้อมูล

ตารางที่ 10 ตัวอย่าง Metadata ของข้อมูลครุภัณฑ์

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 ตัวอย่าง: 2016-04-15	DATETIME	Y	
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 11 สรุปการบริหารจัดการคำอธิบายชุดข้อมูลดิจิทัล หรือ Metadata

การบริหารจัดการคำอธิบายชุดข้อมูลดิจิทัล หรือ เมทาดาตา	
วิธีการดำเนินการ	- ทำความเข้าใจเกี่ยวกับความต้องการในการจัดทำคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา - กำหนดมาตรฐานของคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา
สิ่งที่นำเข้า	- คู่มือแนวปฏิบัติมาตรการการบริหารจัดการคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา เช่น พจนานุกรมข้อมูล (Data Dictionary) การตั้งชื่อข้อมูล (Data Naming)
เครื่องมือที่ใช้	- เครื่องมือบริหารจัดการบัญชีข้อมูล (Data Catalog Management Tools) - เครื่องมือบริหารจัดการคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (Metadata Repository Management Tools)
ผลที่ได้รับ	- เมทาดาตาที่มีคุณภาพ มีความสอดคล้อง และความมั่นคงปลอดภัย
ผู้เกี่ยวข้อง	- บริกรข้อมูล (Data Stewards) - นักวิเคราะห์ข้อมูล (Data Analyst)

2.3.2.9 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 จึงต้องมีการรักษาความลับเพื่อลดความเสี่ยงของการถูกคุกคาม และเป็นการป้องกันการรั่วไหลของข้อมูลโดยมิชอบ เช่น การส่งข้อมูลที่ปกปิดหรือเป็นความลับต้องมีวิธีการที่ทำให้ทราบได้ว่าบุคคลที่ต้องการส่งข้อมูลมาให้ หรือการที่ผู้ได้รับการอนุญาตให้เข้าถึงข้อมูลเท่านั้นที่สามารถอ่านข้อมูลได้

- ความถูกต้องของข้อมูล (Integrity) หมายถึง การคงสภาพของข้อมูลหรือการรักษาความถูกต้องสมบูรณ์ของข้อมูลให้มีความถูกต้องและน่าเชื่อถือ รวมถึงมีการปกป้องข้อมูลให้ปราศจากการถูกเปลี่ยนแปลงโดยผู้ไม่มีสิทธิ์ เช่น ข้อมูลที่ใช้จะต้องเป็นข้อมูลที่ถูกต้องอย่างแท้จริง ไม่มีการดัดแปลงหรือแก้ไขระหว่างทาง

- ความพร้อมใช้งานของข้อมูล (Availability) หมายถึง การพร้อมในการใช้งานอยู่เสมอ กล่าวคือ ข้อมูลต้องพร้อมสำหรับการใช้งานได้เสมอ รวมถึงมีการสำรองข้อมูลไว้เมื่อเกิดภัยพิบัติหรือเหตุการณ์ที่ไม่คาดฝัน เช่น หากต้องการใช้ข้อมูล ผู้ใช้งานสามารถใช้ข้อมูลได้ทันที และใช้ได้อย่างต่อเนื่อง

โดยความมั่นคงปลอดภัยของข้อมูลต้องดำเนินการตั้งแต่การวางแผน การจัดทำ การปฏิบัติตาม และการบังคับใช้นโยบายและขั้นตอนด้านการรักษาความปลอดภัย เพื่อสนับสนุนในด้านที่เกี่ยวข้องกับการพิสูจน์ตัวตน การกำหนดสิทธิ์ การเข้าถึงข้อมูล การตรวจสอบ และความพร้อมใช้ของข้อมูลอย่างเหมาะสม

นอกจากนี้ ต้องมีการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy) ตั้งแต่การรวบรวม จัดเก็บใช้เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูล โดยจะต้องมีการระบุวัตถุประสงค์เป็นหลักฐานให้ชัดเจน ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดที่ไม่สอดคล้องกับวัตถุประสงค์ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนั้น ๆ หรือมีกฎหมายกำหนดให้สามารถกระทำสิ่งนั้นได้

ตารางที่ 12 สรุปการบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล

การบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล	
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) - มาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Standard)
ผู้เกี่ยวข้อง	- ผู้บริหารจัดการฐานข้อมูล (Database Administrator) - บริกรข้อมูล (Data Stewards) - ผู้ตรวจสอบภายใน (Internal Auditor)

2.3.2.10 คุณภาพของข้อมูล (Data Quality)

คุณภาพของข้อมูล (Data Quality) เป็นเครื่องมือในการวัดความน่าเชื่อถือและประสิทธิภาพของการนำข้อมูลไปใช้ ต้องมีการวางแผน การดำเนินการ และการควบคุมกิจกรรมต่าง ๆ รวมถึงการปรับปรุง เพื่อให้ข้อมูลมีคุณภาพ เนื่องจากข้อมูลที่มีคุณภาพสูงทำให้การดำเนินงานของหน่วยงานเป็นไปอย่างมีประสิทธิภาพการทำให้ข้อมูลมีคุณภาพ ประกอบด้วย การทำให้ข้อมูลมีความถูกต้อง (Accuracy) ข้อมูลมีความครบถ้วน(Completeness) ข้อมูลมีความต้องกัน (Consistency) ข้อมูลมีความเป็นปัจจุบัน (Timeliness) ข้อมูลตรงตามความต้องการของผู้ใช้ (Relevancy) และข้อมูลมีความพร้อมใช้ (Availability) ดังแสดงรายละเอียด เพิ่มเติมในบทที่ 3.6.2 การประเมินคุณภาพของข้อมูล (Data Quality Assessment)

ตารางที่ 13 สรุปการบริหารจัดการคุณภาพของข้อมูล

การบริหารจัดการคุณภาพของข้อมูล	
วิธีการดำเนินการ	- กำหนดข้อมูลที่จำเป็นต้องมีคุณภาพ - พัฒนาและส่งเสริมการให้ความสำคัญกับคุณภาพของข้อมูล (Awareness) - กำหนดขอบเขตของการประเมิน (Assessment) คุณภาพของข้อมูล - กำหนดและระบุลำดับความสำคัญ (Prioritize) ของการปรับปรุงข้อมูลให้มีคุณภาพ
สิ่งที่นำเข้า	- มาตรฐาน แนวปฏิบัติ และนโยบายที่เกี่ยวกับการทำให้ข้อมูลมีคุณภาพ เช่น การจัดทำโปรไฟล์ข้อมูล (Data Profiling) ดาตาคลีนซิ่ง (Data Cleansing) - เมทาดาตาทั้งด้านธุรกิจและเทคโนโลยีสารสนเทศ
เครื่องมือที่ใช้	- เครื่องมือในการทำดาตาคลีนซิ่ง (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)

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

2.4 ความสัมพันธ์ระหว่างธรรมาภิบาลข้อมูลกับการบริหารจัดการข้อมูล

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

ดังนั้นสิ่งที่ควรริเริ่มเป็นอันดับแรกของการวางแผนในการบริหารจัดการข้อมูล ก็คือ ธรรมาภิบาลข้อมูล เพราะเป็นเรื่องของการกำหนดบทบาท หน้าที่ความรับผิดชอบ และการตัดสินใจ เพื่อสร้างความเชื่อมั่นว่า ธรรมาภิบาลข้อมูล ความรับผิดชอบ และความเป็นเจ้าของหรือผู้มีส่วนได้เสียกับทรัพย์สินข้อมูลนั้นเป็นไปอย่างมีระเบียบ ถูกต้อง และมีความยั่งยืน โดยธรรมาภิบาลข้อมูลจะต้องเข้าไปมีส่วนร่วมในทุก ๆ องค์ประกอบหรือกิจกรรมของการบริหารจัดการข้อมูล

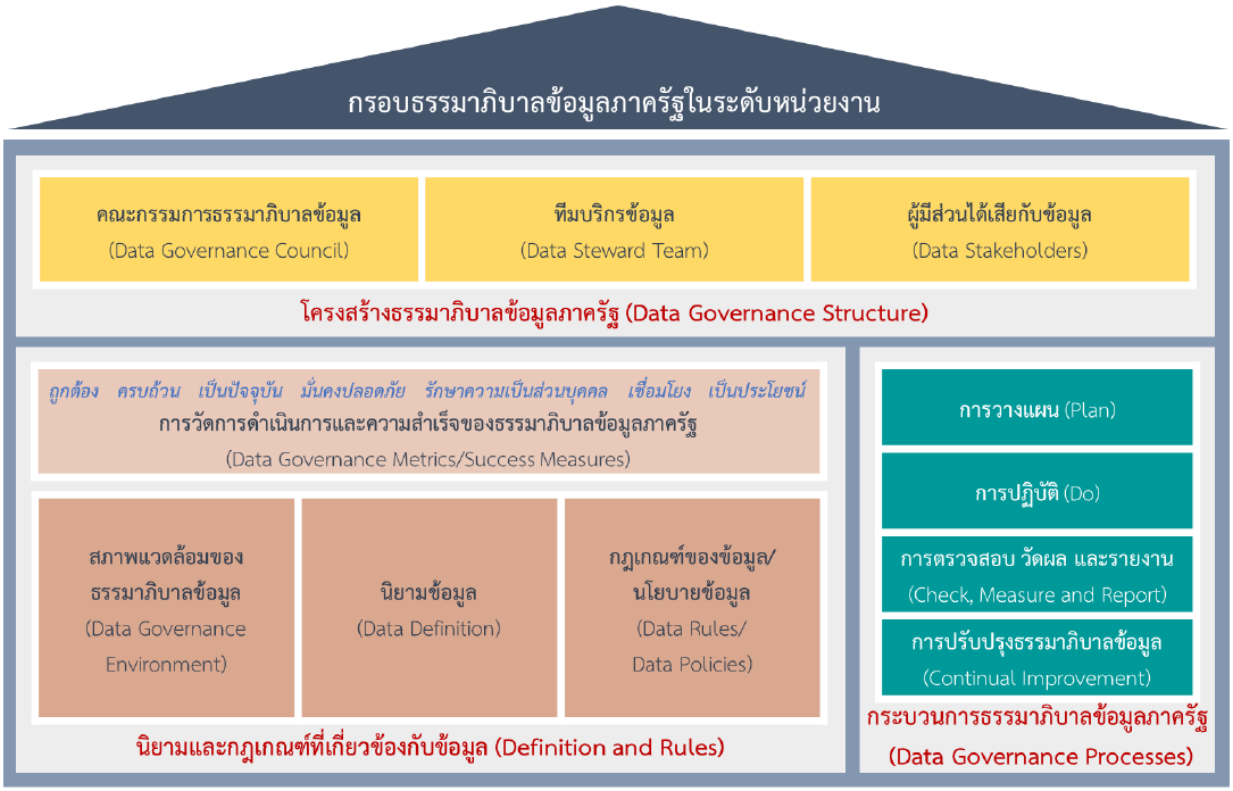
อย่างไรก็ตามการบริหารจัดการข้อมูลนั้นมีความหมายที่กว้างกว่าและเกี่ยวข้องกับแง่มุมของการใช้ข้อมูลและดำเนินงานในกระบวนการที่เกิดขึ้นซ้ำๆ ในแต่ละช่วงของระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูล

ทั้งนี้หากภาครัฐมีธรรมาภิบาลข้อมูลที่ดีจะก่อให้เกิดการบริหารจัดการข้อมูลที่ดีเช่นกัน ส่งผลให้ข้อมูลมีความมั่นคงปลอดภัย มีคุณภาพ สามารถเปิดเผย เชื่อมโยง และแลกเปลี่ยนข้อมูลกันได้ มีคุณค่าทางเศรษฐกิจและสังคม และได้รับความคุ้มทุนต่อการดำเนินงาน

ในบทที่ 3 จะกล่าวถึงรายละเอียดของกรอบธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Framework for Government) สำหรับหน่วยงานภาครัฐ

บทที่ 3
กรอบธรรมาภิบาลข้อมูลภาครัฐ
(DATA GOVERNANCE FRAMEWORK FOR GOVERNMENT)

กรอบธรรมาภิบาลข้อมูลภาครัฐประกอบด้วยองค์ประกอบต่าง ๆ ผนวกเข้าด้วยกัน ทั้งในด้านของนิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล บุคคล และกระบวนการ ซึ่งองค์ประกอบเหล่านี้มีความสำคัญที่ก่อให้เกิดประสิทธิภาพและประสิทธิผลในการดำเนินงาน อันจะนำไปสู่การบรรลุเป้าหมายในการดำเนินงานตามที่กำหนดไว้ โดยสรุปรายละเอียดดังรูปที่ 9



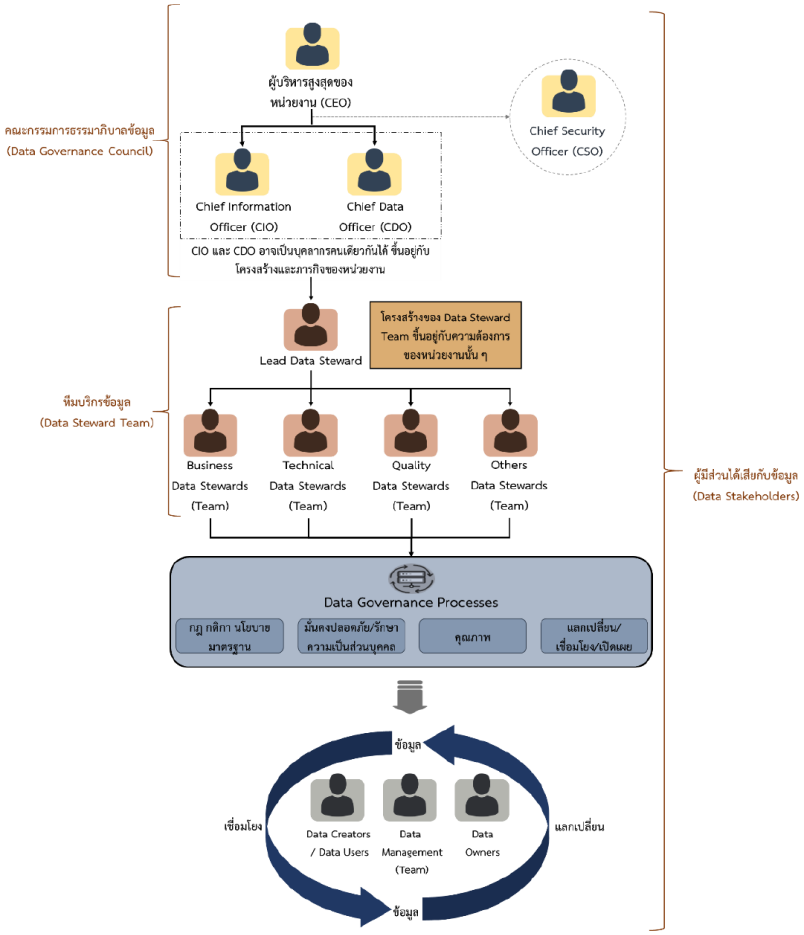
รูปที่ 9 กรอบธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน

จากรูปที่ 9 แสดงกรอบธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน ประกอบด้วย นิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล (Definition and Rules) โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Structure) และกระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Processes) โดยบุคคลต่าง ๆ ที่เกี่ยวข้องกับโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ จะถูกแต่งตั้งโดยผู้บริหารระดับสูงของหน่วยงาน เพื่อทำหน้าที่กำหนดยุทธศาสตร์และเป้าหมาย ตรวจสอบสภาพแวดล้อมของธรรมาภิบาลข้อมูล นิยามความหมายและขอบเขตของข้อมูล กำหนดกฎเกณฑ์และนโยบายข้อมูล และดำเนินการตรวจสอบการปฏิบัติตามกฎเกณฑ์และนโยบายข้อมูล ดังนี้

3.1 โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Structure)

3.1.1 โครงสร้างของบุคลากรที่รับผิดชอบในธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Structure)

การกำหนดโครงสร้างธรรมาภิบาลข้อมูลภาครัฐเพื่อแสดงลำดับขั้นระหว่างกลุ่มบุคคลที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ และแสดงถึงสิทธิ์ในการสั่งการตามลำดับขั้น ทั้งนี้จำนวนบุคลากรและความลึกของลำดับขั้นให้พิจารณาตามความเหมาะสมของแต่ละหน่วยงานของรัฐ หน่วยงานของรัฐสามารถจัดตั้งส่วนงานธรรมาภิบาลข้อมูลในรูปแบบที่แตกต่างกัน ได้แก่ (1) รูปแบบทีมเสมือน (Virtual Team) ที่คัดเลือกมาจากส่วนงานต่าง ๆ (2) รูปแบบที่มีส่วนงานรับผิดชอบชัดเจนซึ่งอาจจะจัดตั้งใหม่หรือกำหนดหน้าที่ให้กับส่วนงานที่มีหน้าที่คล้ายกับโครงสร้าง และ (3) รูปแบบผสมซึ่งจะต้องแยกหน้าที่ให้ชัดเจนระหว่างส่วนงานที่รับผิดชอบหลักกับทีมเสมือน รูปที่ 10 แสดงตัวอย่างโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ ซึ่งแบ่งออกเป็น 3 ส่วน ประกอบด้วย (1) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) (2) ทีมบริกรข้อมูล (Data Steward Team) และ (3) ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders)



รูปที่ 10 ตัวอย่าง โครงสร้างธรรมาภิบาลข้อมูลภาครัฐภายในหน่วยงาน

คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ประกอบไปด้วย ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) ผู้บริหารด้านการรักษาความปลอดภัยระดับสูง (Chief Security Officer) ผู้บริหารจากส่วนงานต่าง ๆ ทั้งจากฝ่ายบริหารและฝ่ายเทคโนโลยีสารสนเทศ รวมไปถึงหัวหน้าทีม บริกรข้อมูล (Lead Data Steward) คณะกรรมการธรรมาภิบาลข้อมูลมีอำนาจสูงสุดในธรรมาภิบาลข้อมูลภายในหน่วยงานภาครัฐ ซึ่งทำหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหา

และบริหารจัดการภายในคณะกรรมการธรรมาภิบาลข้อมูล ทั้งนี้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงอาจจะทำหน้าที่แทนผู้บริหารข้อมูลระดับสูง ซึ่งขึ้นอยู่กับความพร้อมของหน่วยงาน

ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) มีหน้าที่นำข้อมูลและวิเคราะห์ข้อมูลของหน่วยงานภาครัฐเพื่อสร้างและส่งมอบเทคโนโลยี เครื่องมือ แนวทาง และวิธีการในการทำให้ข้อมูลของหน่วยงานภาครัฐ มีคุณค่า และเกิดประโยชน์สูงสุดต่อหน่วยงานภาครัฐ เพื่อขยายผลต่อไปให้เกิดผลสัมฤทธิ์ในการส่งเสริมให้หน่วยงานภาครัฐต่าง ๆ ใช้ข้อมูลได้อย่างถูกต้องและมีประสิทธิภาพ นอกจากนี้ยังต้องวิเคราะห์และร่วมกับผู้บริหารส่วนอื่น ๆ เพื่อจัดทำยุทธศาสตร์และดำเนินการธรรมาภิบาลข้อมูลภาครัฐให้มีคุณภาพและการควบคุมอื่น ๆ เพื่อรักษาความสมบูรณ์ของข้อมูลของหน่วยงานภาครัฐ และนำแนวปฏิบัติและมาตรฐานของหน่วยงานภาครัฐไปปรับปรุงข้อมูลและยุทธศาสตร์ของประเทศ โดยในส่วนของการทำงานในระดับประเทศ ผู้บริหารข้อมูลระดับสูง จะต้องทำหน้าที่เป็นตัวกลางระหว่างหน่วยงานภาครัฐในการแลกเปลี่ยน เชื่อมโยงข้อมูล รวมไปถึงการจัดการความเสี่ยงที่อาจเกิดจากข้อมูลของหน่วยงานภาครัฐ รวมถึงส่งเสริมนวัตกรรมที่ใช้ประโยชน์จากข้อมูลในการวิเคราะห์ปัญหาเพื่อแก้ไขจนสามารถลดปัญหาของประเทศที่เกิดขึ้นในปัจจุบัน และลดความเสี่ยงของปัญหาที่อาจเกิดขึ้นในอนาคตได้ พร้อมทั้งต้องวิเคราะห์หาเทคโนโลยีใหม่ ๆ มาใช้ในการวิเคราะห์ข้อมูลให้ตอบสนองความต้องการของประชาชนด้วย

ในบางหน่วยงาน กรณีที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงมีหน้าที่และความรับผิดชอบใกล้เคียงหรือสามารถทำหน้าที่ของผู้บริหารข้อมูลระดับสูงได้ ดังนั้นผู้บริหารเทคโนโลยีสารสนเทศระดับสูงและผู้บริหารข้อมูลระดับสูงจึงสามารถเป็นบุคคลเดียวกันได้

ผู้บริหารด้านการรักษาความปลอดภัยระดับสูง (Chief Security Officer) เป็นผู้บริหารที่มีบทบาทสูงสุดในการทำให้หน่วยงานภาครัฐมีความปลอดภัยเพียงพอสำหรับการทำงานทั้งด้านการบริหารจัดการดูแลและด้านข้อมูล ทำให้เกิดการเชื่อมต่อระหว่างหน่วยงานภาครัฐ ตัวอย่างเช่น หน่วยงานภาครัฐไม่มีความกังวลเกี่ยวกับช่องโหว่ด้านความปลอดภัย ทำให้การทำงานของหน่วยงานภาครัฐเป็นไปได้อย่างราบรื่น ดังนั้น การมีผู้บริหารด้านการรักษาความปลอดภัยระดับสูงที่ดี สามารถลดความหวาดระแวงในการทำงานระหว่างส่วนงานต่าง ๆ ทำให้เพิ่มมูลค่าให้กับหน่วยงานภาครัฐได้ ดังนั้นหน้าที่หลักของผู้บริหารด้านการรักษาความปลอดภัยระดับสูง คือ การปรับปรุงความมั่นคงทางกายภาพและความปลอดภัยด้านเทคโนโลยีให้มากขึ้น รวมถึงต้องมีทำงานร่วมกับผู้บริหารอื่น ๆ ในการตัดสินใจเกี่ยวกับลำดับความสำคัญของความต้องการด้านความปลอดภัย เพื่อกำหนดเป้าหมายและวัตถุประสงค์ของการป้องกันหน่วยงานเพื่อให้ส อดคล้องกับแผนกลยุทธ์ของหน่วยงาน 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 ที่จะสนับสนุนให้เกิดธรรมาภิบาลข้อมูลภาครัฐที่ดีภายในหน่วยงานภาครัฐ ทีมบริกรข้อมูลรับคำสั่งโดยตรงจากคณะกรรมการธรรมาภิบาลข้อมูล ในขณะเดียวกันมีการให้ข้อมูลสนับสนุนในการตัดสินใจต่อคณะกรรมการธรรมาภิบาลข้อมูล โดยบริกรข้อมูลด้านธุรกิจเป็นผู้ให้การสนับสนุนด้านธุรกิจ ขณะที่บริกรข้อมูลด้านเทคนิคเป็นผู้ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศ อย่างไรก็ตามบริกรข้อมูลด้านธุรกิจและบริกรข้อมูลด้านเทคนิคอาจจะเป็นบุคคลเดียวกัน ซึ่งขึ้นอยู่กับคุณสมบัติของบุคคลหรือความเหมาะสมของหน่วยงานรัฐ

หัวหน้าบริกรข้อมูลทำหน้าที่เป็นผู้ควบคุมและสั่งการภายในทีมบริกรข้อมูล และเป็นหนึ่งในคณะกรรมการธรรมาภิบาลข้อมูล นอกเหนือจากคณะกรรมการธรรมาภิบาลข้อมูลและทีมบริกรข้อมูล ยังมีผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders) อื่น ๆ ซึ่งทำหน้าที่ให้การสนับสนุนธรรมาภิบาลข้อมูลภาครัฐต่อทีมบริกรข้อมูลและคณะกรรมการธรรมาภิบาลข้อมูล ประกอบไปด้วย เจ้าของข้อมูล (Data Owners) ทีมบริหารจัดการข้อมูล (Data Management Team) ผู้สร้างข้อมูล (Data Creators) และผู้ใช้ข้อมูล (Data Users) สำหรับรายละเอียดของบทบาทและความรับผิดชอบภายในโครงสร้างธรรมาภิบาลข้อมูลภาครัฐได้แสดงไว้ในหัวข้อถัดไป

3.1.2 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

บทบาท (Roles) และความรับผิดชอบ (Responsibilities) ที่เหมาะสมจะนำไปสู่การดำเนินงานที่มีประสิทธิภาพและประสิทธิผลต่อหน่วยงาน ซึ่งการกำหนดบทบาทและความรับผิดชอบจะต้องไม่ขัดแย้งต่อกฎระเบียบ ข้อบังคับ หรือกฎหมาย รวมทั้งกำหนดสิทธิ หน้าที่ และความรับผิดชอบในการบริหารจัดการข้อมูลที่อยู่ในความครอบครองหรือควบคุมให้มีความชัดเจน โดยอาจแต่งตั้งหรือมอบหมายเจ้าหน้าที่เป็นรายบุคคลหรือคณะบุคคลให้รับผิดชอบ และประกาศให้ผู้ที่เกี่ยวข้องหรือประชาชนรับทราบด้วยเป็นไปตามที่กำหนดไว้ตามกฎหมายว่าด้วยการนั้น มีรายละเอียดดังนี้

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 บุคคลที่ทำหน้าที่รับผิดชอบในการนิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัยซึ่งอาจจะได้รับมาจากผู้ใช้ข้อมูล (Data Users) หรือผู้มีส่วนได้เสียอื่น ๆ นิยามคำอธิบายชุดข้อมูลดิจิทัลหรือMetadataโดยการสนับสนุนจากผู้ใช้ข้อมูล สถาปนิกข้อมูล (Data Architects) และนักวิเคราะห์ระบบ (System Analyst) ร่างนโยบายข้อมูลด้วยการช่วยเหลือจากทีมบริหารจัดการข้อมูล (Data Management Team) ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ แล้วรายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ ให้ทราบ บริกรข้อมูลด้านธุรกิจมักจะเป็นบุคคลที่มาจากฝ่ายธุรกิจแต่มีความเข้าใจด้านเทคโนโลยีสารสนเทศ

บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) คือ บุคคลที่ทำหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูลด้านธุรกิจ เช่น นิยามMetadataเชิงเทคนิคซึ่งอาจจะได้รับการช่วยเหลือจากทีมบริหารจัดการข้อมูล ให้ข้อเสนอแนะเชิงเทคนิคในการร่างนโยบายข้อมูล ตรวจสอบคุณภาพข้อมูลความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามนโยบายข้อมูลในเชิงเทคนิค ทั้งนี้บริกรข้อมูลด้านเทคนิคมักจะเป็นบุคคลฝ่ายเทคโนโลยีสารสนเทศแต่มีความเข้าใจเกี่ยวกับธุรกิจ

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

เจ้าของข้อมูล (Data Owners) คือ บุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย เจ้าของ

ข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงMetadata และเกณฑ์การทำดาต้าคลีนซิ่ง (Data Cleansing) นอกจากนี้ยังหน้าที่ในการให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล เจ้าของข้อมูลมักจะอยู่ในตำแหน่งบริหาร เช่น ผู้อำนวยการฝ่ายหรือหัวหน้าส่วนงานบุคคลเป็นเจ้าของข้อมูลบุคคล ผู้อำนวยการฝ่ายหรือหัวหน้าส่วนงานการเงินเป็นเจ้าของข้อมูลการเงิน

ทีมบริหารจัดการข้อมูล (Data Management Team) มีหน้าที่หลักในการบริหารจัดการข้อมูล สอดคล้องกับ 10 องค์ประกอบ ตามรายละเอียดในหัวข้อ 2.3.2 องค์ประกอบในการบริหารจัดการข้อมูล ซึ่งมักจะเป็นเจ้าหน้าที่ภายในฝ่ายเทคโนโลยีสารสนเทศของหน่วยงาน ประกอบด้วย สถาปนิกข้อมูล (Data Architects) นักจัดการฐานข้อมูล (Database Administrators - DBA) นักวิเคราะห์ข้อมูล (Data Analysts) และนักวิทยาการข้อมูล (Data Scientists) ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ทีมบริหารจัดการข้อมูล สนับสนุนกิจกรรมของธรรมาภิบาลข้อมูลภาครัฐ เช่น ช่วยเหลือในการนิยาม Metadata ร่างนโยบายข้อมูลและมาตรฐานข้อมูล และกำหนดสิทธิการเข้าถึงข้อมูลโดย DBA

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

ผู้ใช้ข้อมูล (Data Users) คือ บุคคลที่ทำหน้าที่นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร และสนับสนุนธรรมาภิบาลข้อมูลภาครัฐโดยการให้ความต้องการในการใช้ข้อมูล พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังบริกรข้อมูล

3.2 **กระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Processes)**

หลักพื้นฐานของการกำหนดกระบวนการและผลที่ได้รับ ตามลำดับขั้นตอนของข้อมูลหรือระบบบริหารและกระบวนการจัดการข้อมูล(วงจรชีวิตของข้อมูล) เริ่มตั้งแต่ การสร้างข้อมูล การจัดเก็บข้อมูล การใช้ข้อมูล การเผยแพร่ข้อมูล การจัดเก็บข้อมูลถาวร จนถึงการทำลายข้อมูลนั้น ประกอบด้วย การเลือกข้อมูลเพื่อดำเนินการธรรมาภิบาล การระบุเป้าหมาย การกำหนดมาตรฐานและแนวปฏิบัติ รวมถึงการบริหารจัดการคน

1) การเลือกข้อมูลเพื่อดำเนินการธรรมาภิบาล ได้แก่ ข้อมูลส่วนบุคคล ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ และข้อมูลสาธารณะ โดยกระบวนการซึ่งได้มาด้วยข้อมูลนั้นสามารถใช้วิธีการ เช่น กระบวนการวิศวกรรมย้อนกลับ (Reverse Engineering) การวิเคราะห์ข้อมูล (Data Analysis) การสำรวจข้อมูล (Survey)

2) การระบุเป้าหมาย ต้องพิจารณาครอบคลุมในประเด็นดังต่อไปนี้เป็นอย่างน้อย คือ คุณภาพข้อมูล การเข้าถึงและการจัดการ ความปลอดภัยและความเป็นส่วนบุคคล การปฏิบัติตามระเบียบและกฎหมาย ต้นทุนและประสิทธิภาพ

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

4) การบริหารจัดการคน เช่น การสร้างวัฒนธรรมองค์กร การบริหารจัดการแรงต้าน การสื่อสารที่ชัดเจน การสร้างความพึงพอใจกับผู้ที่มีส่วนได้เสีย การใช้ประโยชน์จากเทคโนโลยี ซึ่งจะช่วยให้การดำเนินงานสำเร็จลุล่วงได้ดี

3.2.1 กระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Processes)

กระบวนการธรรมาภิบาลข้อมูลภาครัฐ เป็นขั้นตอนที่ใช้สำหรับกำกับดูแลการดำเนินการใด ๆ ต่อข้อมูลให้เป็นไปตาม กฎ ระเบียบ ข้อบังคับ หรือนโยบายที่เกี่ยวข้องกับข้อมูล กระบวนการธรรมาภิบาลข้อมูลภาครัฐ เริ่มตั้งแต่การวางแผนไปจนถึงการปรับปรุงอย่างต่อเนื่อง ดังนี้

รูปที่ 11 กระบวนการธรรมาภิบาลข้อมูลภาครัฐ

1) การวางแผน (Plan)

การวางแผนเริ่มตั้งแต่กำหนดวิสัยทัศน์และประเด็นปัญหา ซึ่งเป็นส่วนที่สำคัญเนื่องจากเป็นจุดเริ่มต้นที่จะกำหนดกฎระเบียบ นโยบาย มาตรฐาน หรือแนวทางปฏิบัติต่าง ๆ เพื่อใช้ในธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล หลังจากที่ได้มีการกำหนดวิสัยทัศน์และประเด็นปัญหาที่ชัดเจนแล้ว ขั้นตอนถัดไป คือ การกำหนดขอบเขตการดำเนินการ ระยะเวลาดำเนินการบุคคลที่เกี่ยวข้อง และต้นทุนที่ใช้ในการดำเนินงาน หลังจากนั้นนำแผนงาน กฎระเบียบ และนโยบายที่เกี่ยวข้องไปประกาศใช้อย่างเป็นทางการ

2) การปฏิบัติ (Do)

การปฏิบัติในที่นี้อ้างถึงการดำเนินการใด ๆ ของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ เช่น สถาปนิกข้อมูล นักออกแบบข้อมูล นักจัดการฐานข้อมูลวิศวกรข้อมูล นักวิเคราะห์ข้อมูล นักวิทยาการข้อมูล เจ้าของข้อมูล เจ้าของข้อมูลส่วนบุคคลผู้สร้างข้อมูล ผู้บริหาร ผู้ใช้ข้อมูล ซึ่งต้องดำเนินการให้สอดคล้องกับกฎระเบียบ นโยบายมาตรฐาน และแนวปฏิบัติที่ได้กำหนดไว้ ขณะที่บริกรข้อมูลจะให้ความรู้และสนับสนุนให้บุคคลที่เกี่ยวข้องสามารถปฏิบัติตามกฎระเบียบเหล่านั้น ทั้งนี้รายงานความก้าวหน้าผลการปฏิบัติงาน และประเด็นปัญหาที่พบระหว่างปฏิบัติงานจะถูกรายงานไปยังคณะกรรมการธรรมาภิบาลข้อมูล

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

ในการตรวจสอบบริกรข้อมูลจะดำเนินการตรวจสอบความสอดคล้องกันระหว่างกฎระเบียบ นโยบาย และมาตรฐานที่กำหนด กับการปฏิบัติงานของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ พร้อมทั้งทำการวัดผลด้านคุณภาพข้อมูล หลังจากนั้นรายงานผลความสอดคล้อง คุณภาพข้อมูล ความมั่นคงปลอดภัย และความเสี่ยงที่เกี่ยวข้องกับข้อมูลไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้อง เพื่อให้ทราบถึงผลการดำเนินงาน และประเด็นปัญหาที่พบ

4) การปรับปรุงอย่างต่อเนื่อง (Continual Improvement)

ธรรมาภิบาลข้อมูลภาครัฐเป็นสิ่งที่ต้องดำเนินการอย่างต่อเนื่องตลอดระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล ทั้งนี้สภาพแวดล้อมหรือกฎหมายที่เปลี่ยนแปลง รายการ

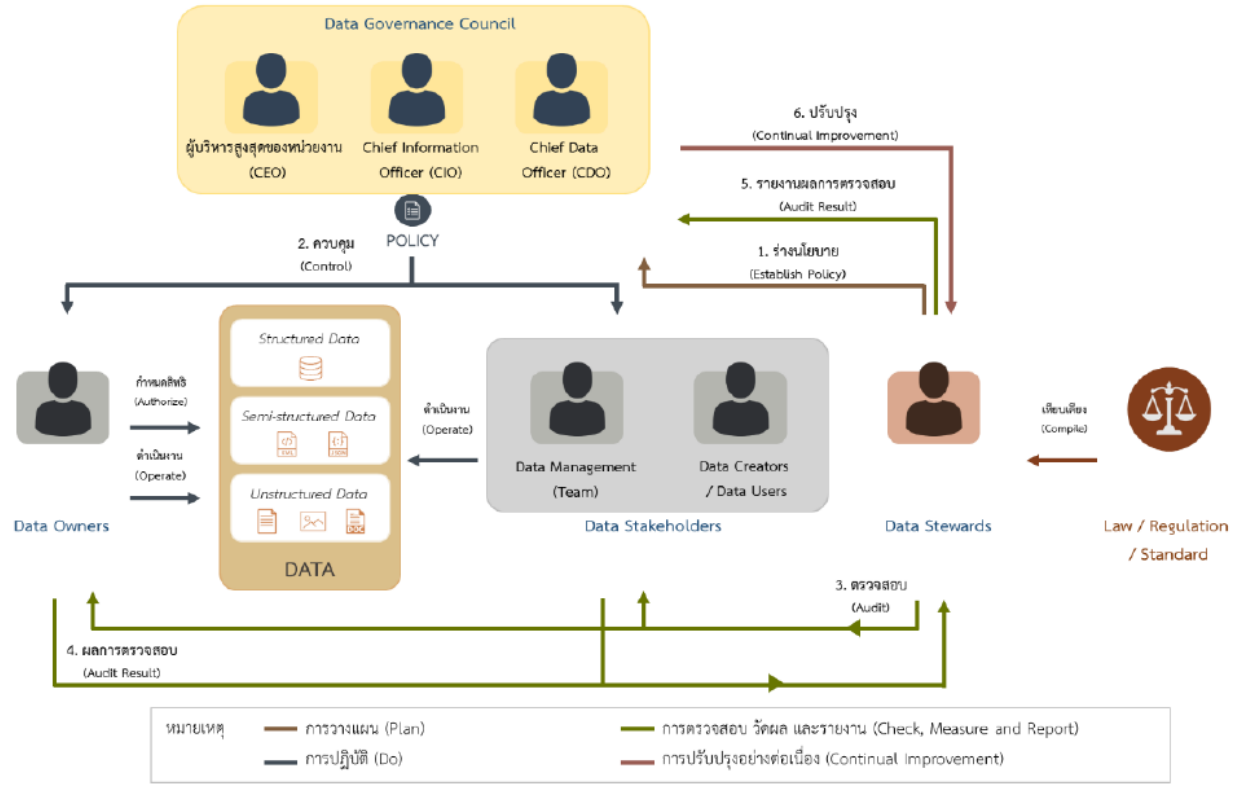
ความต้องการจากผู้บริหารและผู้มีส่วนได้เสีย รวมไปถึงผลการตรวจสอบ เช่น รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัย รายงานความเสี่ยงต่อข้อมูลจะถูกใช้สำหรับการปรับปรุงกระบวนการธรรมาภิบาลข้อมูลภาครัฐ นโยบาย กฎ ระเบียบข้อบังคับที่เกี่ยวข้องกับข้อมูล เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ เกณฑ์การวัดระดับคุณภาพข้อมูล และโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ

3.2.2 แนวทางการจัดการกระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Process Guidelines)

แนวทางการจัดการกระบวนการธรรมาภิบาลข้อมูลภาครัฐจะช่วยให้เข้าใจถึงกระบวนการและสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ ซึ่งชี้ให้เห็นถึงความสัมพันธ์ระหว่างกระบวนการธรรมาภิบาลข้อมูล เครื่องมือ หรือเอกสารที่ใช้ในธรรมาภิบาลข้อมูล ผลลัพธ์ที่ได้จากธรรมาภิบาลข้อมูล และผู้ที่เกี่ยวข้องหรือผู้มีส่วนได้เสีย ดังแสดงในตารางที่ 14 แสดงตัวอย่างแผนภาพการดำเนินการธรรมาภิบาลข้อมูลภาครัฐ ดังแสดงในรูปที่ 12 และแสดงความสัมพันธ์ระหว่างกระบวนการ/กิจกรรม และผู้มีส่วนได้เสีย ดังแสดงในตารางที่ 15

ตารางที่ 14 ความสัมพันธ์ระหว่างกระบวนการ ส่วนนำเข้า ส่วนนำออก และผู้มีส่วนได้เสียกับข้อมูล

กระบวนการ (Processes)	ส่วนนำเข้า (Input)	ส่วนนำออก (Output)	ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholder)
๑ การวางแผน	(๑) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (๒) รายการชุดข้อมูล (๓) รายการประเด็นปัญหาจากรายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล	(๑) แผนดำเนินการ (ขอบเขต เวลา กลุ่มธรรมาภิบาลข้อมูล และต้นทุน)	(๑) ผู้บริหารข้อมูลระดับสูง หรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (๒) คณะกรรมการธรรมาภิบาลข้อมูล (๓) บริกรข้อมูลด้านธุรกิจ (๔) บริกรข้อมูลด้านเทคนิค (๕) บริกรข้อมูลด้านคุณภาพ
๒ การปฏิบัติ	(๑) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (๒) แผนดำเนินการ (ขอบเขต เวลา และต้นทุน)	(๑) รายงานความก้าวหน้าในการปฏิบัติงาน (๒) ผลการปฏิบัติงาน (๓) ประเด็นปัญหาที่พบระหว่างปฏิบัติงาน	(๑) ผู้บริหารงาน (๒) ผู้ปฏิบัติงานที่เกี่ยวข้อง (๓) บริกรข้อมูลด้านธุรกิจ (๔) บริกรข้อมูลด้านเทคนิค (๕) บริกรข้อมูลด้านคุณภาพ
๓ การตรวจสอบ วัดผล และรายงาน	(๑) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (๒) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ ระดับคุณภาพข้อมูล	(๑) รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล (๒) รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล	(๑) บริกรข้อมูลด้านธุรกิจ (๒) บริกรข้อมูลด้านเทคนิค (๓) บริกรข้อมูลด้านคุณภาพ
๔ การปรับปรุงธรรมาภิบาล	(๑) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (๒) โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ (๓) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ และระดับคุณภาพข้อมูล (๔) รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล (๕) รายการความต้องการจากผู้บริหารและผู้มีส่วนได้เสีย	(๑) กระบวนการธรรมาภิบาลข้อมูลภาครัฐ (๒) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมาย ที่เกี่ยวข้องกับข้อมูล (๓) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐและระดับคุณภาพข้อมูล (๔) โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ	(๑) ผู้บริหารข้อมูลระดับสูงหรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (๒) คณะกรรมการธรรมาภิบาลข้อมูล (๓) บริกรข้อมูลด้านธุรกิจ (๔) บริกรข้อมูลด้านเทคนิค (๕) บริกรข้อมูลด้านคุณภาพ



รูปที่ 12 ตัวอย่างแผนภาพการดำเนินการธรรมาภิบาลข้อมูลภาครัฐ

จากรูปที่ 12 แสดงให้เห็นตัวอย่างของการดำเนินการธรรมาภิบาลข้อมูลภาครัฐว่าบริกรข้อมูล (Data Stewards) ทั้งด้านธุรกิจและด้านเทคนิค เป็นผู้ร่างนโยบายข้อมูล (Data Policies) ให้สอดคล้องกับกฎหมายหรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง และนำเสนอคณะกรรมการธรรมาภิบาลข้อมูล ซึ่งประกอบไปด้วย CEO CIO CDO และหรือผู้บริหารทั้งฝ่ายบริหารและฝ่ายเทคโนโลยีสารสนเทศพิจารณากำหนดนโยบายเพื่อควบคุมให้เจ้าของข้อมูล (Data Owners) และผู้มีส่วนได้เสียกับข้อมูลอื่น ๆ (Data Stakeholders) มีหน้าที่ในการปฏิบัติตามนโยบายข้อมูลที่กำหนดไว้

เจ้าของข้อมูลเป็นผู้กำหนดสิทธิการเข้าถึงและดำเนินงานใด ๆ กับข้อมูลที่ตนเป็นเจ้าของ ทั้งข้อมูลที่มีโครงสร้าง (เช่น ฐานข้อมูล) ข้อมูลกึ่งโครงสร้าง (เช่น Extensible Markup Language-XML) ข้อมูลที่ไม่มีโครงสร้าง (เช่น เสียง ภาพ ภาพเคลื่อนไหว) ขณะที่ผู้มีส่วนได้เสียกับข้อมูล เช่น ผู้บริหารจัดการฐานข้อมูล(Database Administrators) และผู้ใช้ข้อมูล (Data Users) ต้องดำเนินการกับข้อมูลให้สอดคล้องกับสิทธิที่ได้รับจากเจ้าของข้อมูล เช่น การเพิ่ม ลบ แก้ไข ประมวลผล นำไปใช้ แลกเปลี่ยน เปิดเผยข้อมูล โดยมีบริกรข้อมูลเป็นผู้ตรวจสอบความสอดคล้องกันของการดำเนินงานตามนโยบายข้อมูล ทั้งจากเจ้าของข้อมูลและผู้มีส่วนได้เสียกับข้อมูล พร้อมทั้งรายงานการตรวจสอบการดำเนินงานให้กับคณะกรรมการธรรมาภิบาลข้อมูลทราบ ทั้งนี้คณะกรรมการธรรมาภิบาลข้อมูลต้องทบทวนนโยบายข้อมูล และผลการดำเนินงานจากรายงานการตรวจสอบเพื่อการปรับปรุง และกำหนดแนวทางในการธรรมาภิบาลที่มีประสิทธิภาพต่อไป

ตารางที่ 15 ความสัมพันธ์ระหว่างกระบวนการ/กิจกรรม และผู้มีส่วนได้เสียกับข้อมูล

กระบวนการ/กิจกรรม	ผู้มีส่วนได้เสียกับข้อมูล				
	คณะกรรมการธรรมาภิบาลข้อมูล	ทีมบริกรข้อมูล	เจ้าของข้อมูล	ทีมบริหารจัดการข้อมูล	ผู้สร้างและใช้งานข้อมูล
กำหนดและปรับปรุงนโยบายและมาตรฐานข้อมูล	A	R	S	S/C	S
ตรวจสอบการปฏิบัติตามนโยบายข้อมูล	I	R	S	S/C	S
การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ	I	R	S	S	S
ประเมินความมั่นคงปลอดภัยและคุณภาพข้อมูล	I	R	S	S/C	S
รายงานผลการตรวจสอบ ความมั่นคงปลอดภัย และคุณภาพข้อมูล	I	R	I	I	I
กำหนดสิทธิในการเข้าถึงข้อมูล	I	R	A	S/C	I

หมายเหตุ : Responsible=ดำเนินการหลัก Accountable=อนุมัติ Support=ให้การสนับสนุน
Consulted=ให้คำปรึกษา Informed=รับทราบข้อมูล

ตารางที่ 15 แสดงความสัมพันธ์ระหว่างกระบวนการ/กิจกรรม และผู้มีส่วนได้เสียกับข้อมูล โดย Rหมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตามกระบวนการหรือกิจกรรมที่กำหนดไว้ A หมายถึง ผู้มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากปฏิบัติงาน S หมายถึง ผู้มีหน้าที่ในการสนับสนุนหรือให้การช่วยเหลือต่อการปฏิบัติงาน C หมายถึง ผู้มีหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน และ I หมายถึง ผู้มีหน้าที่รับทราบผลการปฏิบัติงาน

3.3 สภาพแวดล้อมของธรรมาภิบาลข้อมูล (Data Governance Environment)

3.3.1 กฎหมาย ระเบียบ ข้อบังคับ แนวนโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ

ปัจจุบันกฎหมายที่เกี่ยวข้องกับข้อมูล ข่าวสาร หรือสิทธิส่วนบุคคลในประเทศไทย มีประเด็นที่อาจส่งผลกระทบต่อหลักแนวคิดธรรมาภิบาลข้อมูลภาครัฐ ซึ่งหากหน่วยงานในประเทศไทยต้องการสร้างหรือปรับปรุงระบบภายในให้มีธรรมาภิบาลข้อมูลภาครัฐ จะต้องพิจารณาประเด็นหลัก ๆ ที่เกี่ยวข้องกับกฎหมาย ดังนี้

รูปที่ 13 กฎหมาย ระเบียบ ข้อบังคับ แนวน ยบาย และแนวปฏิบัติที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ

1) การเปิดเผยข้อมูล

การเปิดเผยข้อมูลเป็นสิ่งจำเป็นต่อการดำเนินงานของรัฐบาล ซึ่งแสดงความโปร่งใสในการดำเนินงานและความสามารถในการตรวจสอบได้จากภาคเอกชนและประชาชน รวมไปถึงการสนับสนุนให้ภาคเอกชนและประชาชนนำข้อมูลที่เปิดเผยไปสร้างนวัตกรรมผลิตภัณฑ์และบริการเพื่อยกระดับการพัฒนาประเทศ โดยแนวคิดการเปิดเผยข้อมูลเป็นที่ยอมรับของหน่วยงานระหว่างประเทศและรัฐบาลประเทศต่าง ๆ โดยในประเทศไทยมีกฎหมายที่เกี่ยวข้องกับการเปิดเผยข้อมูล ดังนี้

- รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 ในมาตราที่ 59 ได้ระบุว่า รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการ

- พระราชบัญญัติ (พ.ร.บ.) การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 โดยมีการเปิดเผยข้อมูลหรือข่าวสารสาธารณะที่หน่วยงานของรัฐจัดทำ และครอบครองในรูปแบบและช่องทางดิจิทัล เพื่อให้ประชาชนเข้าถึงโดยสะดวก มีส่วนร่วมและตรวจสอบการดำเนินงานของรัฐ และสามารถนำข้อมูลไปพัฒนาบริการ และนวัตกรรมที่จะเป็นประโยชน์ต่อประเทศในด้านต่าง ๆ

- พระราชบัญญัติ (พ.ร.บ.) ข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 โดยมี 3 ประเด็นที่เกี่ยวกับการเปิดเผยข้อมูล ได้ถูกระบุไว้ใน พ.ร.บ. ฉบับนี้ ได้แก่

- ข้อมูลภาครัฐ ต้อง “เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น”

- กำหนดหลักเกณฑ์และกลไกการเปิดเผยข้อมูล

- กำหนดประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้

- แนวทางปฏิบัติการเปิดเผยข้อมูลภาครัฐ (Government Open Data Publication Guidelines) ให้แนวทางปฏิบัติเพื่อการเปิดเผยข้อมูลภาครัฐ ซึ่งมีวัตถุประสงค์เพื่อเป็นแนวปฏิบัติสำหรับการเปิดเผยข้อมูลภาครัฐ1 ได้แก่

- แนวปฏิบัติและมาตรฐานเชิงเทคนิค เพื่อให้หน่วยงานภาครัฐนำไปใช้เป็นแนวปฏิบัติในการดำเนินการเกี่ยวกับการเปิดเผยข้อมูลของหน่วยงานให้เป็นไปในทิศทางเดียวกัน รวมถึงการกำหนดมาตรฐานเชิงเทคนิค รูปแบบ วิธีการเผยแพร่ข้อมูลผ่านศูนย์กลางข้อมูลเปิดภาครัฐ หรือ data.go.th และการกำหนดสัญญาอนุญาต (License) ที่เหมาะสมสำหรับข้อมูลเปิดภาครัฐ

- แบบฟอร์มคำอธิบายชุดข้อมูลดิจิทัลหรือMetadata เพื่อเป็นตัวอย่างการจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือMetadata โดยหน่วยงานสามารถนำไปประยุกต์ใช้งานที่เหมาะสมกับหน่วยงานได้

- คู่มือการเปิดเผยข้อมูล (Open Data Handbook) เพื่อสร้างความรู้ ความเข้าใจให้แก่หน่วยงานภาครัฐ ภาคเอกชน และผู้ที่ต้องการศึกษาเกี่ยวกับข้อมูลเปิด (Open Data)

- คู่มือการนำข้อมูลขึ้นเผยแพร่บน data.go.th เพื่อให้ผู้ใช้งานสามารถศึกษาทำความเข้าใจการทำงาน ต่าง ๆ ของระบบได้ และสามารถตรวจสอบปัญหาที่เกิดจากการใช้งานและสามารถแก้ปัญหาในขั้นต้นได้

- คู่มือแสดงรายการชุดข้อมูลที่สำคัญ เพื่อเป็นการสร้างแหล่งข้อมูลที่ใช้ประกอบในการใช้งานที่เกี่ยวกับชุดข้อมูลที่สำคัญให้แก่หน่วยงานภาครัฐ ภาคเอกชน และผู้ที่ต้องการศึกษาเกี่ยวกับข้อมูลเปิด (Open Data)

- แนวปฏิบัติในการออกแบบความคิดเชิงนวัตกรรม (Data Innovation Guideline) เป็นคู่มือที่ช่วยให้เข้าใจปัญหาที่แท้จริง และสามารถออกแบบแนวทางแก้ไขปัญหาที่เป็นแนวคิดเชิงนวัตกรรม ตลอดจนสามารถเข้าถึงชุดข้อมูล (Datasets) ต่าง ๆ เพื่อให้ได้มาซึ่งแนวทางในการแก้ปัญหา นอกจากนั้นผู้ที่ต้องการศึกษากระบวนการออกแบบนวัตกรรมสามารถนำไปประยุกต์หรือปรับใช้กับหน่วยงานได้

2) การเชื่อมโยงและแลกเปลี่ยนข้อมูล

การเชื่อมโยงและแลกเปลี่ยนข้อมูลเป็นสิ่งสำคัญต่อการบูรณาการการดำเนินงานระหว่างหน่วยงานภาครัฐ ซึ่งเป็นประโยชน์ต่อหน่วยงานภาครัฐและประชาชนในการขอใช้บริการจากภาครัฐ โดยมีกฎหมายที่เกี่ยวข้องกับการเชื่อมโยงและแลกเปลี่ยนข้อมูล ดังนี้

- พระราชบัญญัติ (พ.ร.บ.) การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 โดยมีการพัฒนามาตรฐาน หลักเกณฑ์ และวิธีการเกี่ยวกับดิจิทัล และพัฒนาโครงสร้างพื้นฐานด้านดิจิทัลที่จำเป็น ให้เป็นไปตามมาตรฐานสากล เพื่อสร้างและพัฒนากระบวนการทำงานของหน่วยงานของรัฐให้มีความสอดคล้องและมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกัน รวมทั้งมีความมั่นคงปลอดภัยและน่าเชื่อถือ โดยมีการบูรณาการและสามารถทำงานร่วมกันอย่างเป็นเอกภาพ เกิดการพัฒนาการบริการภาครัฐที่มีประสิทธิภาพและนำไปสู่การบริหารราชการและการบริการประชาชนแบบบูรณาการ รวมทั้งให้ประชาชนเข้าถึงโดยสะดวก

- ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน 2 มีวัตถุประสงค์ในการสนับสนุนการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัยและน่าเชื่อถือ รวมทั้งให้ผู้ประกอบการและหน่วยงานต่าง ๆ ได้มีแนวทางในการสร้างเอกสารอิเล็กทรอนิกส์ให้อยู่ในรูปแบบข้อความ XML ให้เป็นมาตรฐานเดียวกัน

- ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยรหัสสถานที่ออกหนังสือ3 ให้ข้อเสนอแนะสำหรับการกำหนดรหัสสถานที่ออกหนังสือรับรอง ซึ่งจะส่งผลให้ทราบที่มาของหนังสือรับรองและการอำนวยความสะดวกทางการค้า พร้อมการบริหารจัดการ มาตรฐานการแลกเปลี่ยนข้อมูลสารสนเทศด้านการค้าระหว่างประเทศผ่านระบบ National Single Window ให้เป็นไปในทิศทางเดียวกัน

3) การคุ้มครองข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคล (Privacy Data Protection) เป็นสิ่งสำคัญที่ภาครัฐต้องดำเนินการ โดยปัจจุบันมีการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย ซึ่งหน่วยงานภาครัฐอาจจะมีการรวบรวม จัดเก็บ ใช้หรือเผยแพร่ข้อมูลส่วนบุคคลของผู้ใช้บริการในรูปของข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการป้องกันการละเมิดข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิขั้นพื้นฐานสำคัญในความเป็นส่วนบุคคล (Privacy Right) ของประชาชนที่ต้องได้รับการคุ้มครอง อันจะทำให้ประชาชนมีความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์ ดังนั้นการคุ้มครองข้อมูลส่วนบุคคลจำเป็นที่จะต้องนำมาวิเคราะห์เพื่อให้เกิดธรรมาภิบาลข้อมูลภาครัฐที่ดี โดยมีกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

- พระราชบัญญัติ (พ.ร.บ.) ข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 กำหนดประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้ ซึ่งเป็นสิ่งที่จำเป็นต้องมีการพิจารณาในกรณีที่เป็นข้อมูลส่วนบุคคล เนื่องจากข้อมูลที่เป็นข้อมูลส่วนบุคคลจำเป็นต้องได้รับการคุ้มครองอย่างมีหลักเกณฑ์

- พระราชบัญญัติ (พ.ร.บ.) คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการกำหนดหลักเกณฑ์กลไก และมาตรการที่กำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล

- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.) เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 ได้ระบุเรื่องการคุ้มครองข้อมูลส่วน

บุคคลไว้ว่า “กำหนดให้ภาครัฐที่ให้บริการทางอิเล็กทรอนิกส์ ต้องมีนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล”

- แนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคลได้ (Guideline to Protect the Personally Identifiable Information) ให้แนวปฏิบัติสำหรับหน่วยงานในการเตรียมข้อมูลให้เหมาะสมต่อการบูรณาการข้อมูลเข้าด้วยกัน โดยการนำเสนอขั้นตอนในการดำเนินการปกป้องข้อมูลที่ระบุตัวบุคคลได้ นอกจากนั้นนำเสนอวิธีการเชื่อมโยงข้อมูลแบบรวมชุดข้อมูล (Integrated Datasets) การเชื่อมโยงข้อมูลผ่านตัวแบบข้อมูล (Data Model Market Place) และการเชื่อมโยงข้อมูลแบบกลุ่ม (Batch)

4) การรักษาความลับ

การรักษาความลับทางราชการเป็นสิ่งที่จำเป็นต่อการดำเนินงานของหน่วยงานภาครัฐ ซึ่งเป็นการป้องกันความเสียหายที่จะเกิดขึ้นต่อภาครัฐ ทั้งในด้านชื่อเสียง การเงิน ความสามารถในการพัฒนาประเทศ และความมั่นคงของประเทศ โดยมีกฎหมาย ระเบียบที่เกี่ยวข้องกับการรักษาความลับ ดังนี้

- พระราชบัญญัติ (พ.ร.บ.) ข่าวกรองแห่งชาติ พ.ศ.2562 ได้กำหนดข้อมูลข่าวสารที่สำนักข่าวกรองแห่งชาติได้รับมาเนื่องจากการปฏิบัติหน้าที่ตาม พ.ร.บ. นี้ จะเปิดเผยมิได้ เว้นแต่เป็นการเปิดเผยต่อหน่วยข่าวกรอง หน่วยงานความมั่นคง นายกรัฐมนตรีหรือตามคำสั่งศาล ที่จะนำมาพิจารณาในธรรมาภิบาลข้อมูลภาครัฐ

- ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม ได้มีข้อกำหนดที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ ได้แก่ กำหนดนิยามข้อมูลข่าวสารลับ และกำหนดหลักเกณฑ์และวิธีการในการรักษาความลับของหน่วยงานภาครัฐ

- แนวทางปฏิบัติในการรักษาความปลอดภัยเกี่ยวกับบุคคล เอกสาร และสถานที่ที่จัดทำขึ้นจากระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.2552 ควรนำมาพิจารณาในธรรมาภิบาลข้อมูลภาครัฐนอกจากการพิจารณากฎหมาย ระเบียบ และข้อบังคับที่มีอยู่ในปัจจุบัน หน่วยงานต้องพิจารณากฎหมาย ระเบียบ นโยบาย หรือ พ.ร.บ. ซึ่งมีกฎหมายที่เกี่ยวข้องกับเรื่องธรรมาภิบาลข้อมูลภาครัฐอีกด้วย ดังนี้

1) พระราชบัญญัติ (พ.ร.บ.) การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 โดยกำหนดให้หน่วยงานรัฐจัดให้มีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล โดยมีการบริหารจัดการและบูรณาการข้อมูลภาครัฐและการทำงาน
ให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล โดยมุ่งหมายในการเพิ่มประสิทธิภาพและอำนวยความสะดวกในการให้บริการและเข้าถึงประชาชนและในการเปิดเผยข้อมูลภาครัฐต่อสาธารณะและสร้างการมีส่วนร่วมของทุกภาคส่วน

2) พระราชบัญญัติ (พ.ร.บ.) การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมและกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อรักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์

3) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.) เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 โดยกำหนดให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยการเข้าถึงข้อมูลสารสนเทศ ในระดับเคร่งครัดระดับกลาง หรือระดับพื้นฐาน ให้หน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรปฏิบัติตามมาตรฐาน

3.3.2 หลักการของสภาพแวดล้อมและวัฒนธรรมของหน่วยงานที่เอื้อต่อการมีธรรมาภิบาลข้อมูลภาครัฐ

ธรรมาภิบาลข้อมูลภาครัฐมีองค์ประกอบหลายอย่างที่สนับสนุนให้เกิดธรรมาภิบาลข้อมูลภาครัฐที่ดีในขณะเดียวกันจะต้องคำนึงถึงข้อจำกัดที่อาจส่งผลในเชิงลบต่อการปรับเปลี่ยนหรือปฏิรูปให้เกิดธรรมาภิบาลข้อมูลภาครัฐในหน่วยงานด้วย วัฒนธรรมองค์กร และสภาพแวดล้อมเป็นหนึ่งในข้อจำกัดที่อาจส่งผลต่อการเปลี่ยนแปลงในธรรมาภิบาลข้อมูลภายในหน่วยงานได้ เนื่องจากแต่ละหน่วยงานล้วนมีวัฒนธรรมองค์กรและสภาพแวดล้อมที่แตกต่างกัน

ดังนั้นการตระหนักถึงวัฒนธรรมองค์กรและสภาพแวดล้อมที่แตกต่างกันมีความจำเป็นต่อการกำหนดโครงสร้าง นโยบาย บทบาทหน้าที่ การดำเนินงานที่เอื้อต่อธรรมาภิบาลข้อมูลภาครัฐ ตั้งแต่เริ่มต้น นอกจากนี้ยังต้องมีมาตรการรองรับกรณีที่มีการปรับเปลี่ยนโครงสร้างองค์กร เนื่องจากหากมีการปรับเปลี่ยนโครงสร้างองค์กร ธรรมาภิบาลข้อมูลภาครัฐก็จะเปลี่ยนตามไปด้วย

3.4 การนิยามข้อมูล (Data Definition)

การนิยามข้อมูลต้องมีความถูกต้องและชัดเจน เพื่อสร้างความเข้าใจที่ตรงกันระหว่างผู้ที่เกี่ยวข้อง ทั้งนี้การจัดหมวดหมู่ของข้อมูลทำให้มองเห็นถึงภาพรวมของข้อมูล ขณะที่การทำMetadataเพื่อสร้างความเข้าใจต่อข้อมูลมากยิ่งขึ้น โดยมีรายละเอียดดังนี้

3.4.1 หมวดหมู่ของข้อมูล (Data Category)

ข้อมูลแบ่งออกได้เป็น 4 หมวดหมู่ ดังนี้

รูปที่ 14 หมวดหมู่ของข้อมูล

1) ข้อมูลส่วนบุคคล มีนิยามและที่มา ดังนี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562)

“ข้อมูลข่าวสารส่วนบุคคล” หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงานบรรดาที่มีชื่อของผู้

นั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึก ลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย (พ.ร.บ. ข้อมูลข่าวสารของทางราชการ พ.ศ. 2540)

“ข้อมูลข่าวสารส่วนบุคคล” หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึก ลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่ง เฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย (พ.ร.บ. ข้อมูลข่าวสารของทางราชการ พ.ศ. 2540)

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

2) ข้อมูลความมั่นคง มีนิยามและที่มา ดังนี้

มาตรา 59 รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการตามที่กฎหมายบัญญัติ และต้องจัดให้ประชาชนเข้าถึงข้อมูลหรือข่าวสารดังกล่าวได้โดยสะดวก (รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560)

จากนิยามข้างต้น จึงได้ข้อสรุปว่า ข้อมูลความมั่นคง คือ “ข้อมูลเกี่ยวกับความมั่นคงของรัฐที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น”

3) ข้อมูลความลับทางราชการ มีนิยามและที่มา ดังนี้

“ข้อมูลข่าวสารลับ” หมายความว่า ข้อมูลข่าวสารตามมาตรา 14 หรือมาตรา 15 ที่มีคำสั่งไม่ให้เปิดเผยและอยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นเรื่องที่เกี่ยวกับการดำเนินงานของรัฐหรือที่เกี่ยวกับเอกชน ซึ่งมีการกำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือชั้นลับที่สุด ตามระเบียบนี้โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานของรัฐและประโยชน์แห่งรัฐประกอบกัน (ระเบียบว่าด้วยการรักษาความลับของราชการ พ.ศ. 2544)

“สิ่งที่เป็นความลับของทางราชการ” หมายความว่า ข้อมูลข่าวสาร บริภัณฑ์ ยุทธภัณฑ์ ที่สงวน การรหัส ประมวลลับ และสิ่งอื่นใดบรรดาที่ถือว่าเป็นความลับของทางราชการ (ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552)

“ข้อมูลข่าวสารของราชการ” หมายความว่า ข้อมูลข่าวสารที่อยู่ในครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐไม่ว่าจะเป็นข้อมูลข่าวสารเกี่ยวกับการดำเนินงานของรัฐหรือข้อมูลข่าวสารเกี่ยวกับเอกชน (พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ.2540)

จากนิยามข้างต้น จึงได้ข้อสรุปว่า ข้อมูลความลับทางราชการ คือ “ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล”

4) ข้อมูลสาธารณะ มีนิยามและที่มา ดังนี้

มาตรา 59 รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการตามที่กฎหมายบัญญัติ และต้องจัดให้ประชาชนเข้าถึงข้อมูลหรือข่าวสารดังกล่าวได้โดยสะดวก (รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560)

“ข้อมูลข่าวสารสาธารณะ” หมายความว่า ข้อมูลข่าวสารของราชการที่หน่วยงานของรัฐต้องเปิดเผยให้ประชาชนได้รับรู้ รับทราบ หรือตรวจสอบได้โดยไม่จำเป็นต้องร้องขอ (ร่าง พรบ. ข้อมูลข่าวสารของราชการ)

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

3.4.2 คำอธิบายชุดข้อมูลดิจิทัล หรือMetadata (Metadata)

คำอธิบายชุดข้อมูลดิจิทัล หรือMetadata คือ “ข้อมูลที่ใช้กำกับและอธิบายข้อมูลหลักหรือกลุ่มของข้อมูลอื่น”4 แบ่งออกเป็น 2 กลุ่ม ดังนี้

1) Metadataเชิงธุรกิจ (Business Metadata) ซึ่งให้รายละเอียดของชุดข้อมูล (Datasets) ในด้านธุรกิจ เหมาะสำหรับผู้ใช้งานข้อมูล (Data User) นักวิเคราะห์ข้อมูล (Data Analyst) และนักวิทยาการข้อมูล (Data Scientist) ตัวอย่างรายการMetadataเชิงธุรกิจ เช่น ชื่อข้อมูล ชื่อเจ้าของข้อมูล คำสำคัญ คำอธิบายอย่างย่อ วันที่เริ่มต้นใช้งาน วันที่ทำการเปลี่ยนแปลงข้อมูลภาษาที่ใช้ ชื่อฟิลด์ข้อมูล (เช่น ชื่อพนักงาน นามสกุล เพศ) ในภาคผนวก ก อธิบายMetadataเชิงธุรกิจ ซึ่งไม่รวมชื่อฟิลด์ข้อมูล เนื่องจากชื่อฟิลด์ข้อมูลของแต่ละชุดข้อมูลมีความแตกต่างกัน

2) Metadataเชิงเทคนิค (Technical Metadata) ซึ่งให้รายละเอียดของชุดข้อมูล (Datasets) ในด้านเทคนิค (Technical) และปฏิบัติการ (Operational) เหมาะสำหรับผู้บริหารจัดการฐานข้อมูล (Database Administrator) ตัวอย่างรายการMetadataเชิงเทคนิค เช่น ชื่อตารางข้อมูลในฐานข้อมูล ชื่อฟิลด์ข้อมูลในตารางข้อมูล ประเภทข้อมูล (เช่น ตัวเลข ตัวหนังสือ หรือวันที่) ความกว้างของฟิลด์ข้อมูล (เช่น 10 ตัวอักษร 50 ตัวอักษร หรือ 100 ตัวอักษร) คีย์ข้อมูล (Primary Key หรือ Foreign Key) รวมไปถึงข้อมูลสำหรับการสำรองข้อมูล (Backup) และกู้คืนข้อมูล (Restore)

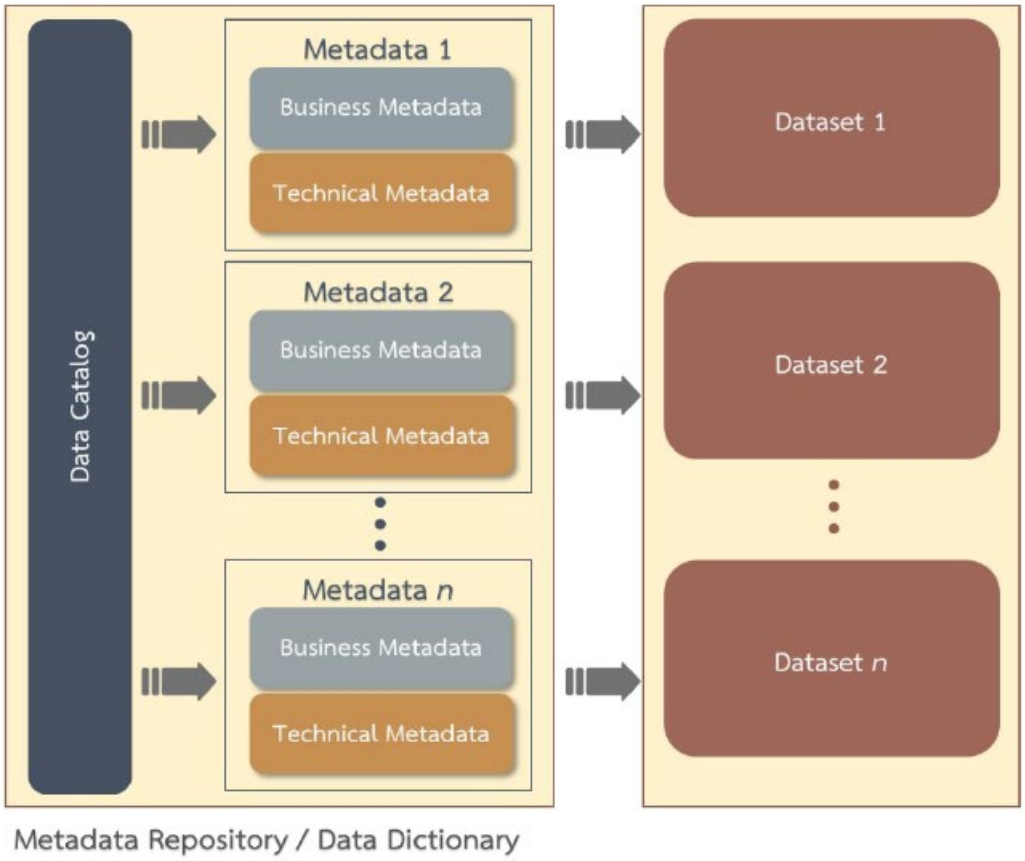
3.4.3 บัญชีข้อมูล (Data Catalog)

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

3.4.4 คลังMetadata (Metadata Repository) หรือพจนานุกรมข้อมูล (Data Dictionary)

คลังMetadata หรือพจนานุกรมข้อมูลเป็นเครื่องมือในการรวบรวมและจัดเก็บMetadata เพื่อสนับสนุนให้ผู้ที่ต้องการใช้ข้อมูลสามารถค้นหาและเข้าถึงได้โดยสะดวก อย่างไรก็ตามผู้ที่มีสิทธิในการเข้าถึงควรได้รับสิทธิ์ที่แตกต่างกันขึ้นอยู่กับบทบาทและความรับผิดชอบ เช่น ผู้ใช้งานข้อมูลสามารถเข้าถึงได้เฉพาะMetadataเชิงธุรกิจ ขณะที่บริกรข้อมูลสามารถเข้าถึงได้ทั้งMetadataเชิงธุรกิจและMetadataเชิง

เทคนิค โดยความสัมพันธ์ระหว่างบัญชีข้อมูล Metadata คลังMetadata พจนานุกรมข้อมูล และชุดข้อมูล แสดงดังรูปที่ 15



รูปที่ 15 ความสัมพันธ์ระหว่างบัญชีข้อมูล Metadata คลังMetadata พจนานุกรมข้อมูล และชุดข้อมูล

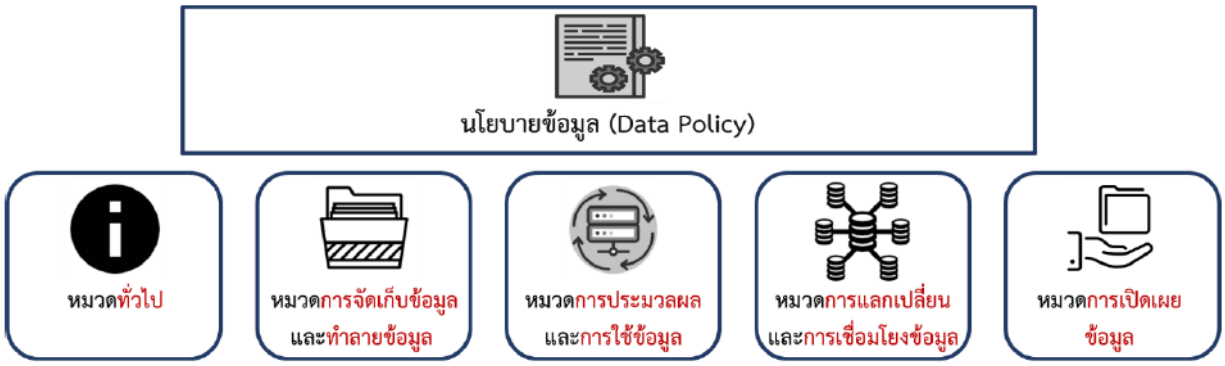
จากรูปที่ 15 บัญชีข้อมูลเปรียบเสมือนสารบัญ เมนู หรือตัวชี้ไปยังMetadataที่ถูกจัดเก็บอยู่ในคลัง Metadata โดยMetadataจะให้รายละเอียดต่าง ๆ ที่เกี่ยวข้องกับชุดข้อมูลนั้น ๆ ทั้งนี้คลังMetadata หรือพจนานุกรมข้อมูลมักจะถูกพัฒนาให้อยู่ในรูปแบบของซอฟต์แวร์

3.5 กฎเกณฑ์ข้อมูล (Data Rules)

กฎเกณฑ์ข้อมูลมักจะอ้างถึงนโยบายและมาตรฐานที่เกี่ยวข้องกับข้อมูล โดยนโยบายข้อมูลอธิบายถึงข้อควรปฏิบัติและข้อห้ามปฏิบัติ ขณะที่มาตรฐานข้อมูลอธิบายถึงวิธีการหรือขั้นตอนการปฏิบัติ เพื่อเป็นหลักในการปฏิบัติเกี่ยวกับธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูลของหน่วยงาน ดังนั้นในการจัดทำมาตรฐานควรจะมีความสอดคล้องกับนโยบายข้อมูลที่กำหนดไว้ โดยทั้งนโยบายและมาตรฐานจะต้องสอดคล้องกับธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงานและกฎหมายที่เกี่ยวข้อง เพื่อเป็นหลักและแนวทางในการปฏิบัติของหน่วยงาน รวมทั้งประกาศเผยแพร่ต่อผู้ที่เกี่ยวข้องและประชาชนทราบด้วยเป็นไปตามที่กำหนดไว้ตามกฎหมายว่าด้วยการนั้น ดังนี้

3.5.1 นโยบายข้อมูล (Data Policies)

การกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในพื้นฐานของธรรมาภิบาลข้อมูลภาครัฐ ดังนั้นเพื่อให้ธรรมาภิบาลข้อมูลภาครัฐมีประสิทธิภาพ จึงต้องมีการกำหนดนโยบายที่ระบุอย่างชัดเจน สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง โดยผ่านการอนุมัติจากผู้บริหาร มีการเผยแพร่และสื่อสารให้กับเจ้าหน้าที่และผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน รวมถึงควรมีการทบทวนนโยบายอย่างสม่ำเสมอ เพื่อให้นโยบายข้อมูลได้ถูกนำมาปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง โดยนโยบายข้อมูลควรจะครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูล ซึ่งอาจจะประกอบไปด้วยนโยบายต่าง ๆ หรือหมวดนโยบาย ทั้งนี้หน่วยงานควรจัดทำนโยบายข้อมูลภายใต้กรอบนโยบายข้อมูล (Data Policy Framework) ดังนี้



รูปที่ 16 นโยบายข้อมูล

1) หมวดทั่วไป (General Domain)

เพื่อกำหนดนโยบายทั่วไปที่เกี่ยวข้องกับข้อมูล เช่น โครงสร้างที่เกี่ยวข้อง หน้าที่ความรับผิดชอบ โดยมีรายละเอียด ดังนี้

- กำหนดบทบาทและความรับผิดชอบที่ประกอบกันเป็นโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ โดยต้องได้รับการมอบอำนาจและการอนุมัติจากผู้บริหาร
- กำหนดกลุ่มบุคคลหรือบุคคลภายในหน่วยงาน เพื่อเป็นเจ้าของข้อมูลในการบริหารจัดการข้อมูลของหน่วยงาน เพราะหน่วยงานถือเป็นเจ้าของข้อมูลทุกประเภทที่เกิดจากการดำเนินงานภายในหน่วยงานนั้น ๆ
- กำหนดขอบเขตข้อมูลที่นโยบายข้อมูลครอบคลุม เช่น ข้อมูลที่มีโครงสร้าง (ฐานข้อมูล และ CSV) ข้อมูลกึ่งโครงสร้าง (XML และ JSON) ข้อมูลที่ไม่มีโครงสร้าง (เอกสาร เสียง ภาพ และภาพเคลื่อนไหว)
- กำหนดนโยบาย มาตรการการรักษาความปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึงการสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับการอนุญาต
- นำระบบเทคโนโลยีสารสนเทศหรือระบบอัตโนมัติมาใช้ในการจัดทำMetadata
- ตรวจสอบความสอดคล้องกันระหว่างนโยบายข้อมูลกับการดำเนินการใด ๆ ของผู้มีส่วนได้เสีย อย่างน้อยปีละ 1 ครั้ง
- ทบทวนนโยบายข้อมูล อย่างน้อยปีละ 1 ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่อง หากพบว่านโยบายข้อมูลยังไม่มีประสิทธิภาพเพียงพอ
- สื่อสารและเผยแพร่นโยบายข้อมูลให้กับผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน

- สนับสนุนให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูลภาครัฐ และการบริหารจัดการข้อมูล โดยให้ครอบคลุมทุกกระบวนการของการบริหารจัดการและระบบบริหาร และกระบวนการจัดการข้อมูล(วงจรชีวิตของข้อมูล)

2) หมวดการจัดเก็บข้อมูลและทำลายข้อมูล (Data Storage and Destruction Domain)

เพื่อกำหนดนโยบายในการจัดเก็บข้อมูลและทำลายข้อมูลอย่างมีคุณภาพ มีการรักษาความปลอดภัยของข้อมูล โดยมีรายละเอียด ดังนี้

- กำหนดสภาพแวดล้อมของการจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล

- กำหนดชั้นความลับของข้อมูล และจัดเก็บให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Guideline/Standard) ที่กำหนดไว้เพื่อให้ข้อมูลมีความมั่นคงปลอดภัย และรักษาคุณภาพของข้อมูล

- กำหนดสิทธิ์การเข้าถึงข้อมูล และเครื่องมือที่ใช้ในการเข้าถึงข้อมูล

- จัดเก็บข้อมูลให้สอดคล้องกับความต้องการ และวัตถุประสงค์ในการดำเนินงาน โดยข้อมูลนั้นจะต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบันอยู่เสมอ ทั้งนี้ควรจัดทำMetadataสำหรับชุดข้อมูลที่มีการจัดเก็บ

- ในกรณีที่มีการร้องขอให้ทำลายข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล หรือหน่วยงานที่จัดเก็บต้องดำเนินการทำลายให้เร็วที่สุด ทั้งนี้ต้องไม่ขัดต่อข้อตกลงระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล หรือไม่ขัดต่อข้อกฎหมายใด ๆ

- กำหนดแนวทางในการทำลายข้อมูล เมื่อข้อมูลนั้นไม่มีการใช้งานหรือมีการเก็บข้อมูลไว้นานเกินกว่าระยะเวลาที่กำหนด แต่ควรมีการเก็บรักษาMetadataของข้อมูลที่ทำลายไว้เพื่อใช้สำหรับการตรวจสอบภายหลัง

- สร้างความรู้ความเข้าใจในการจัดเก็บและทำลายข้อมูลแก่ผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน

3) หมวดการประมวลผลข้อมูลและการใช้ข้อมูล (Data Processing and Use Domain)

เพื่อกำหนดนโยบายในการประมวลผลข้อมูลและการใช้ข้อมูล ให้ได้ข้อมูลที่มีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ โดยมีรายละเอียด ดังนี้

- กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูล และทำการสื่อสารให้แก่ผู้ที่เกี่ยวข้องรับทราบ

- การดำเนินการประมวลผลข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ให้เป็นไปตามขอบเขต เงื่อนไข หรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น

- จัดทำMetadataสำหรับข้อมูลที่จัดเก็บอยู่ในคลังข้อมูล (Data Warehouse)

- ต้องมีการบันทึกประวัติการประมวลผลและการใช้ข้อมูล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

4) หมวดการแลกเปลี่ยนและการเชื่อมโยงข้อมูล (Data Exchange and Integration Domain)

เพื่อกำหนดนโยบายในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานให้มีความมั่นคงปลอดภัยและข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีรายละเอียด ดังนี้

- กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)

- กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลให้ชัดเจนเริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ

- กำหนดMetadataของชุดข้อมูลที่ต้องการแลกเปลี่ยนที่จำเป็นให้ครบถ้วน

- ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

- กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล

- บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้

- สามารถตรวจสอบได้ว่าการแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติ กระบวนการแลกเปลี่ยน และมาตรฐานตามที่กำหนด

5) หมวดการเปิดเผยข้อมูล (Data Disclosure Domain)

เพื่อกำหนดนโยบายในการเปิดเผยข้อมูล เพื่อให้สามารถเปิดเผยข้อมูลได้อย่างถูกต้องตรงตามวัตถุประสงค์ของการให้นำข้อมูลไปใช้ประโยชน์ โดยมีรายละเอียด ดังนี้

- ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

- ต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล

- ควรมีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

- ควรมีการเปิดเผยMetadataควบคู่ไปกับข้อมูลที่เปิดเผย

- สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล

3.5.2 มาตรฐานข้อมูล (Data Standards)

มาตรฐานข้อมูลอ้างถึงมาตรฐานที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและการใช้ข้อมูล ซึ่งเป็นกลไกอย่างหนึ่งในธรรมาภิบาลข้อมูลภาครัฐ มีวัตถุประสงค์เพื่อสร้างความเข้าใจที่ตรงกัน และลดความหลากหลายของวิธีการปฏิบัติ เช่น มาตรฐานMetadata (Metadata Standard) มาตรฐานชุดข้อมูล (Datasets Standard) มาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Standard)

มาตรฐาน Metadata (Metadata Standard) คือ การกำหนดรูปแบบ และข้อกำหนดของMetadataเพื่อให้สามารถเข้าใจได้ถูกต้องตรงกันตลอดทั้งหน่วยงาน ISO/IEC 11179 และ Dublin Core Metadata Initiative (DCMI) 5 ได้กำหนดมาตรฐาน Metadata สำหรับอธิบายชุดข้อมูล เช่น ชื่อข้อมูล ชื่อเจ้าของข้อมูลคำอธิบายข้อมูล ขอบเขตการจัดเก็บ รูปแบบข้อมูล ภาษา สิทธิการเข้าถึง ทั้งนี้มาตรฐาน Metadata มักจะอ้างถึงทั้ง Metadata เชิงธุรกิจ และ Metadata เชิงเทคนิค แต่มักจะไม่รวมองค์ประกอบของฟิลด์ข้อมูล ซึ่งเป็นคุณลักษณะเฉพาะของแต่ละชุดข้อมูล

มาตรฐานชุดข้อมูล (Datasets Standard) คือ การกำหนดรูปแบบและข้อกำหนดของข้อมูลที่มีการใช้ร่วมกันจากหลาย ๆ ส่วนงานหรือหน่วยงาน เพื่อลดความซ้ำซ้อนของข้อมูล ลดความยุ่งยากในการบริหารจัดการ และสนับสนุนให้ข้อมูลมีคุณภาพ ซึ่งส่วนงานหรือหน่วยงานต้องร่วมกันกำหนดMetadataขึ้นมาเพื่ออธิบายคุณลักษณะของชุดข้อมูลที่ใช้ร่วมกัน แล้วดำเนินการบูรณาการข้อมูลที่กระจายอยู่ตามส่วนงานหรือหน่วยงานต่าง ๆ เข้าด้วยกัน มาตรฐานชุดข้อมูลมักจะอธิบายถึงองค์ประกอบของฟิลด์ข้อมูล เช่น ชื่อฟิลด์

ข้อมูล ประเภทข้อมูล (เช่น ตัวเลข ตัวหนังสือ วันที่) ช่วงค่าของข้อมูล และการอนุญาตให้ฟิลด์ข้อมูลเป็นค่าว่าง

มาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Standard) คือ การกำหนดรูปแบบและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อป้องกันการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ชั้นความลับของข้อมูลมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของประเทศ ตัวอย่างชั้นความลับ ได้แก่ ลับที่สุด ลับมาก ลับ และเปิดเผยได้ ตัวอย่างประเภทของผลกระทบ 1) ด้านชื่อเสียง เช่น ข้อมูลในเชิงลบของหน่วยงานถูกเปิดเผยส่งผลให้หน่วยงานหรือประเทศเสียชื่อเสียง 2) ด้านความต่อเนื่องของการดำเนินการ เช่น ข้อมูลระบบเครือข่ายถูกเปิดเผยทำให้ระบบเครือข่ายหรือระบบอินเทอร์เน็ตถูกโจมตี ซึ่งส่งผลให้การดำเนินงานของหน่วยงานหยุดชะงักหรือล่าช้า 3) ด้านการเงิน เช่น ข้อมูลบัตรเครดิตในหน่วยงานถูกเปิดเผย ทำให้สูญเสียงบประมาณของหน่วยงาน 4) ด้านทรัพยากรบุคคล เช่น ข้อมูลเงินเดือนถูกเปิดเผย ส่งผลให้บุคลากรคนสำคัญต้องลาออก

3.6 การวัดการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Metrics and Success Measures)

การวัดการดำเนินการธรรมาภิบาลข้อมูลภาครัฐเป็นการประเมินความพร้อมของธรรมาภิบาลข้อมูลจะแสดงให้เห็นถึงสถานะปัจจุบันของหน่วยงานในเรื่องความพร้อมและความก้าวหน้าในการดำเนินการธรรมาภิบาลข้อมูลภาครัฐ ซึ่งผลของการดำเนินการธรรมาภิบาลข้อมูลจะส่งผลถึงความสำเร็จของธรรมาภิบาลข้อมูลภาครัฐ ประกอบด้วย คุณภาพของข้อมูล ความมั่นคงปลอดภัยของข้อมูล และมูลค่าเชิงธุรกิจ ระดับความพร้อมที่สูงควรจะสะท้อนถึงความสำเร็จที่สูง อย่างไรก็ตามระดับความพร้อมกับความสำเร็จอาจจะไม่สอดคล้องกัน ซึ่งอาจจะมาจากสาเหตุอื่นหรือเกณฑ์การประเมินความพร้อมยังไม่มีประสิทธิภาพเพียงพอ ดังนั้นหน่วยงานควรจะค้นหาสาเหตุที่แน่ชัดพร้อมทั้งดำเนินการแก้ไขเกณฑ์การประเมินความพร้อมเพื่อให้สอดคล้องกับลักษณะเฉพาะของหน่วยงาน แนวทางการประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐการประเมินคุณภาพของข้อมูล และการประเมินความมั่นคงปลอดภัยของข้อมูล มีรายละเอียดดังนี้

3.6.1 การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Readiness Assessment)

การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐจะทำให้เราได้ทราบถึงสิ่งที่เราได้ดำเนินการแล้วและสิ่งใดบ้างที่ควรจะดำเนินการต่อไป เพื่อปรับปรุงการดำเนินงานให้เกิดประสิทธิภาพสูงสุด ระดับความพร้อมของธรรมาภิบาลข้อมูลภาครัฐถูกใช้เป็นเครื่องมือในการประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ ซึ่งประกอบด้วย 6 ระดับดังนี้

- ระดับ 0 : None หมายถึง ไม่มีธรรมาภิบาลข้อมูลภาครัฐหรือมีแต่ไม่ได้ดำเนินการอย่างเป็นทางการ นั่นคือ มีการดำเนินงานบางส่วนและไม่มีการประกาศให้ทราบอย่างเป็นทางการ

- ระดับ 1 : Initial หมายถึง ไม่มีการกำหนดมาตรฐานของกระบวนการ นั่นคือ กระบวนการถูกกำหนดขึ้นมาเฉพาะกิจ (Adhoc) ทำให้แต่ละโครงการหรือบริการมีรูปแบบของกระบวนการที่แตกต่างกันและอำนาจในการจัดการและธรรมาภิบาลข้อมูลส่วนใหญ่ถูกดำเนินการโดยฝ่ายเทคโนโลยีสารสนเทศทำให้การทำงานร่วมกันระหว่างฝ่ายธุรกิจและฝ่ายเทคโนโลยีสารสนเทศไม่สอดคล้องกัน

- ระดับ 2 : Managed หมายถึง เริ่มมีการกำหนดมาตรฐานของกระบวนการเฉพาะแต่ละส่วนงานหรือบริการ และมีการกำหนดบุคคลที่เกี่ยวข้องกับการกำกับติดตาม เช่น บริกรข้อมูลและเจ้าของข้อมูล

- ระดับ 3 : Standardized หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศมีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลหรือความมั่นคงปลอดภัย

- ระดับ 4 : Advanced หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศมีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลและความมั่นคงปลอดภัย

- ระดับ 5 : Optimized หมายถึง มีการดำเนินการสอดคล้องกับระดับ 4 วิเคราะห์สาเหตุของปัญหา (Root Cause) ประกอบไปด้วย ความไม่สอดคล้องในการปฏิบัติงานกับนโยบายข้อมูล (Non-Conformation) คุณภาพข้อมูลที่ต่ำ และความไม่คุ้มทุนในการบริหารจัดการข้อมูลดำเนินการปรับปรุงกระบวนการ กฎเกณฑ์และนโยบายข้อมูล หรือโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ เพื่อแก้ไขปัญหาที่พบจากผลการวิเคราะห์ และให้สอดคล้องกับความต้องการของผู้ที่เกี่ยวข้องและวัตถุประสงค์ที่เปลี่ยนไปของหน่วยงาน

ตารางที่ 16 ระดับความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ

ระดับ	โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ	กระบวนการธรรมาภิบาลข้อมูลภาครัฐ	นโยบายข้อมูลและการตรวจสอบ	การประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	การปรับปรุงอย่างต่อเนื่อง
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	มีส่วนงานกลางในธรรมาภิบาลข้อมูล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลหรือความมั่นคงปลอดภัย	ไม่มีหรือมีแต่ไม่เป็นทางการ
๔ : Advanced	มีส่วนงานกลางในธรรมาภิบาลข้อมูล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	ไม่มีหรือมีแต่ไม่เป็นทางการ
๕ : Optimized	มีส่วนงานกลางในธรรมาภิบาลข้อมูล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	มีการปรับปรุงกระบวนการอย่างต่อเนื่อง

3.6.2 การประเมินคุณภาพของข้อมูล (Data Quality Assessment)

การประเมินคุณภาพของข้อมูลเป็นการตรวจสอบผลลัพธ์หรือความสำเร็จจากธรรมาภิบาลข้อมูลภาครัฐ โดยองค์ประกอบในการประเมินคุณภาพ ประกอบด้วย

รูปที่ 17 องค์ประกอบในการประเมินคุณภาพข้อมูล

1) ข้อมูลมีความถูกต้อง (Accuracy) ข้อมูลจะมีความถูกต้องและเชื่อถือได้ขึ้นกับวิธีการที่ใช้ในการควบคุมข้อมูลนำเข้า และการควบคุมการประมวลผล การควบคุมข้อมูลนำเข้าเป็นการกระทำเพื่อให้เกิดความมั่นใจว่าข้อมูลนำเข้ามีความถูกต้องเชื่อถือได้ เพราะถ้าข้อมูลนำเข้าไม่มีความถูกต้องแล้ว ถึงแม้จะใช้วิธีการวิเคราะห์และประมวลผลข้อมูลที่ดีเพียงใด ผลลัพธ์ที่ได้ก็จะไม่มีความถูกต้อง หรือนำไปใช้ไม่ได้ ข้อมูลนำเข้าจะต้องเป็นข้อมูลที่ผ่านการตรวจสอบว่าถูกต้องแล้วข้อมูลบางประเภทอาจต้องแปลงให้อยู่ในรูปแบบที่เครื่องคอมพิวเตอร์สามารถเข้าใจได้อย่างถูกต้อง ซึ่งอาจต้องพิมพ์ข้อมูลมาตรวจสอบก่อนการประมวลผล ถึงแม้ว่าจะมีการตรวจสอบข้อมูลนำเข้าแล้วก็ตามก็อาจทำให้ได้ข้อมูลที่ผิดพลาดได้ เช่น การเขียนโปรแกรมหรือใช้สูตรคำนวณผิดพลาด ดังนั้นจึงควรกำหนดวิธีการควบคุมการประมวลผล ได้แก่ การตรวจสอบยอดรวมที่ได้จากการประมวลผลแต่ละครั้ง หรือการตรวจสอบผลลัพธ์ที่ได้จากการประมวลผลด้วยเครื่องคอมพิวเตอร์กับข้อมูลสมมติที่มีการคำนวณด้วยว่ามีความถูกต้องตรงกันหรือไม่

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

3) ข้อมูลมีความต้องกัน (Consistency) ค่าข้อมูลในชุดข้อมูลเดียวที่สอดคล้องกับค่าในชุดข้อมูลอื่นนอกจากนี้คำจำกัดความของความสอดคล้องระบุว่าหากมีการดึงข้อมูลสองค่าจากชุดข้อมูลแยกต่างหากต้องไม่ขัดแย้งกัน เช่น ข้อมูลวันที่หรือเวลาที่เก็บในฐานข้อมูลเจ้าหน้าที่ และฐานข้อมูลผู้ลงทะเบียนใช้บริการชุดข้อมูลที่มีรูปแบบต่างกัน ทั้งนี้อาจจะเกิดขึ้นในขณะที่การออกแบบระบบมีการนำเข้าข้อมูลก็เป็นอีกสาเหตุหนึ่ง หรือแม้กระทั่งการใช้กฎตรวจวัดความถูกต้องของข้อมูลที่ต่างกัน

4) ข้อมูลมีความเป็นปัจจุบัน (Timeliness) ข้อมูลที่ดีนั้นนอกจากจะเป็นข้อมูลที่มีความถูกต้องเชื่อถือได้แล้วจะต้องเป็นข้อมูลที่เป็นปัจจุบัน ทั้งนี้เพื่อให้ผู้ใช้สามารถนำเอาผลลัพธ์ที่ได้ไปใช้ได้ทันเวลา นั่นคือ จะต้องเก็บข้อมูลได้รวดเร็วเพื่อทันความต้องการของผู้ใช้ เช่น ตัวอย่างข้อมูลเจ้าหน้าที่ที่เข้ามาปฏิบัติงานโดยส่วนงานที่มีหน้าที่นำเข้าข้อมูลเข้าสู่ระบบได้มีการดำเนินการตามเวลาที่กำหนด คือทำให้ข้อมูลเป็นปัจจุบัน ซึ่งจะทำให้หน่วยงานที่เกี่ยวข้องสามารถนำข้อมูลที่เป็นปัจจุบันไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

5) ข้อมูลตรงตามความต้องการของผู้ใช้ (Relevancy) ระดับของข้อมูลที่บริหารจัดการต้องนำเสนอโดยตรงและมีประสิทธิภาพ โดยสามารถใช้งานได้ตามวัตถุประสงค์ ตัวอย่างเช่น ข้อมูลทางสถิติที่จะเป็นการนำเสนอในรูปแบบตาราง เข้าใจง่าย และข้อความอยู่ในหลาย ๆ ย่อหน้า ซึ่งสามารถใช้งานได้ตามความต้องการ

6) ข้อมูลมีความพร้อมใช้ (Availability) ข้อมูลควรเข้าถึงได้ง่าย สามารถใช้งานได้จริง และสามารถใช้งานได้ตลอดเวลา ตัวอย่างเช่น นักวิเคราะห์แผนงานต้องการข้อมูลบัญชีของการประกันภัยต่อเขตต่าง ๆ แต่ข้อมูลไม่พร้อมใช้งาน จนกระทั่งต้องใช้คนเขียนโปรแกรมเพื่อดึงข้อมูลนั้นออกมาในกรณีนี้หากข้อมูลมีความพร้อมใช้ตรงกับความต้องการใช้ ผู้ใช้สามารถใช้ข้อมูลดังกล่าวได้ทันที ตัวอย่างการวัดคุณภาพข้อมูลที่เป็นโครงสร้าง ดังแสดงในตารางที่ 17

ตารางที่ 17 ตัวอย่างการวัดคุณภาพข้อมูลที่เป็น โครงสร้างสำหรับแต่ละชุดข้อมูล

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 ๒ : พิจารณาแถวและฟิลด์ข้อมูล** ถ้าพบว่ามี ๖๐ ฟิลด์จาก ๑๐๐ ฟิลด์ ที่มีการบันทึกข้อมูลทั้ง ๑,๐๐๐ คน ดังนั้นข้อมูลชุดนี้มีความครบถ้วน = (๑,๐๐๐ x ๖๐) / (๑,๐๐๐ x ๑๐๐) x ๑๐๐ = ๖๐ **กรณีที่ ๓ : 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
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)

3.6.3 การประเมินความมั่นคงปลอดภัยของข้อมูล (Data Security Assessment)

การประเมินความมั่นคงปลอดภัยของข้อมูลเป็นอีกหนึ่งวิธีในการวัดความสำเร็จจาก ธรรมาภิบาลข้อมูลภาครัฐ โดยใช้หลักเกณฑ์ในด้านต่าง ๆ ดังนี้

1) จัดทำนโยบายด้านความมั่นคงปลอดภัยของข้อมูลที่รวมถึงการป้องกันข้อมูลในบริบทของการรักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูล

2) ข้อมูลมีการจัดชั้นความลับ (Data Classification) ข้อมูลควรมีการจัดชั้นความลับให้สอดคล้องกับกฎหมาย เงื่อนไข และข้อกำหนดต่าง ๆ รวมถึงการคำนึงถึงมูลค่า ความสำคัญ และความอ่อนไหวของข้อมูล กรณีที่ผู้ไม่ได้รับสิทธิในการเข้าถึงนั้นทำการเปิดเผยข้อมูลดังกล่าวด้วย การกำหนดระดับชั้นความลับ เช่น ข้อมูลลับ ข้อมูลลับมาก และข้อมูลเปิดเผยได้

3) กำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูล (Data Protection) การกำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูลต้องคำนึงถึงระดับชั้นความลับของข้อมูล เช่น ข้อมูลที่มีความอ่อนไหวต้องมีการกำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูลแบบพิเศษ เพื่อป้องกันการเข้าถึงเพื่อเปิดเผยข้อมูลที่อ่อนไหวนั้น รวมถึงเพื่อป้องกันการดัดแปลง แก้ไข แต่งเติมข้อมูลโดยไม่ได้รับอนุญาต

4) ข้อมูลถูกใช้งานอย่างเหมาะสม การนำข้อมูลไปใช้ควรดำเนินการให้สอดคล้องกับสัญญาอนุญาตและไม่ขัดต่อกฎหมาย

5) ข้อมูลต้องมีความพร้อมใช้อยู่เสมอ ต้องมีการดำเนินการเตรียมความพร้อมไม่ว่าข้อมูลจะอยู่ในประเภทใดก็ตาม เช่น ข้อมูลในรูปแบบกระดาษต้องมีสถานที่จัดเก็บดูแล และสามารถเข้าถึงโดยผู้มีสิทธิได้อย่างสม่ำเสมอ ข้อมูลในรูปแบบอิเล็กทรอนิกส์ต้องมีการเตรียมความพร้อมเรื่องระบบงาน การสำรองข้อมูล รวมถึงมีแผนการดำเนินการในกรณีฉุกเฉินใด ๆ ที่อาจมีผลต่อการใช้ข้อมูลด้วย

ตารางที่ 18 ตัวอย่างการวัดความมั่นคงปลอดภัยของข้อมูล

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

บทสรุป

ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) เปรียบเสมือนเป็นแนวทางในการริเริ่มกำหนดกลไกต่าง ๆ ในธรรมาภิบาลข้อมูลภาครัฐอย่างเป็นรูปธรรมเพื่อประโยชน์ในการบริหารจัดการข้อมูล ให้ได้ซึ่งข้อมูลที่มีคุณภาพ มีความปลอดภัย สร้างมูลค่า และสามารถเพิ่มศักยภาพในการดำเนินงานทั้งการเปิดเผยข้อมูล เชื่อมโยงและแลกเปลี่ยนข้อมูล และการสร้างประโยชน์จากข้อมูลต่อไปในอนาคต ซึ่งจะเป็นประโยชน์ อย่างยิ่ง ต่อการดำเนินงานและการแข่งขันของประเทศจากกรอบธรรมาภิบาลข้อมูลภาครัฐตามหัวข้อในบทที่ 3 ซึ่งแสดงให้เห็นถึงโครงสร้าง กระบวนการและหลักเกณฑ์ต่าง ๆ ทั้งนี้เพื่อให้ได้มาซึ่งธรรมาภิบาลข้อมูลภาครัฐที่ดีนั้น หน่วยงานควรคำนึงถึงการดำเนินงานดังนี้

1. บทบาทของผู้บริหาร ผู้บริหารระดับสูงของหน่วยงาน เป็นผู้มีบทบาทสำคัญยิ่งในการผลักดันให้เกิดธรรมาภิบาลข้อมูลภาครัฐ ดังนั้นผู้บริหารระดับสูงของหน่วยงานต้องมีความมุ่งมั่นในการผลักดันให้เกิดธรรมาภิบาลข้อมูลภาครัฐ โดยผู้บริหารควรมีบทบาท ดังนี้

- สื่อสารถึงความสำคัญของธรรมาภิบาลข้อมูลภาครัฐ ขอบเขต นโยบาย และเป้าประสงค์ของธรรมาภิบาลข้อมูลภาครัฐ
- สนับสนุน ส่งเสริม จัดสรรทรัพยากรให้เพียงพอต่อการดำเนินงาน
- ทบทวนธรรมาภิบาลข้อมูลภาครัฐในหน่วยงาน และส่งเสริมให้เกิดธรรมาภิบาลข้อมูลภาครัฐอยู่สม่ำเสมอ

2. จัดตั้งคณะทำงาน จัดตั้งคณะทำงานให้สอดคล้องกับหน้าที่ความรับผิดชอบของแต่ละตำแหน่งตามที่ได้กำหนดไว้ในกรอบธรรมาภิบาลข้อมูลภาครัฐ เช่น คณะกรรมการธรรมาภิบาลข้อมูล บริกรข้อมูล ทั้งนี้หน่วยงานสามารถดูความเหมาะสมในการบริหารจัดการบุคลากรที่มีหน้าที่ในการปฏิบัติงานดังกล่าว นอกจากนั้นบางหน่วยงานอาจมีบุคลากรที่ทำหน้าที่ในลักษณะดังกล่าวอยู่ในปัจจุบัน อย่างไรก็ตามการกำหนดบทบาทหน้าที่ที่ชัดเจนจะส่งผลต่อการทำงานที่มีประสิทธิภาพและประสิทธิผลสูงสุดต่อหน่วยงาน

3. กำหนดกระบวนการธรรมาภิบาลข้อมูลภาครัฐ กำหนดกระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Process) ตามที่ได้กำหนดไว้ในกรอบธรรมาภิบาลข้อมูลภาครัฐ โดยพิจารณาถึง การเลือกข้อมูลเพื่อดำเนินการธรรมาภิบาล การระบุเป้าหมาย การกำหนดมาตรฐานและแนวปฏิบัติ รวมถึงการบริหารจัดการคน โดยกระบวนการธรรมาภิบาลข้อมูลภาครัฐ เริ่มตั้งแต่การวางแผน การปฏิบัติ การตรวจสอบวัดผลและรายงานไปจนถึงการปรับปรุงอย่างต่อเนื่อง

4. กำหนดนโยบายกฎเกณฑ์ของข้อมูล การกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในพื้นฐานของธรรมาภิบาลข้อมูลภาครัฐ นโยบายที่กำหนดสามารถใช้รายละเอียดตามที่ระบุในกรอบธรรมาภิบาลข้อมูลภาครัฐได้โดยคำนึงถึงความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่งหรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง มีการเผยแพร่และสื่อสารให้กับเจ้าหน้าที่และผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงานเพื่อดำเนินการต่อไป

5. การปฏิบัติงานต่าง ๆ ที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ กลุ่มคนที่ได้กำหนดไว้ในธรรมาภิบาลข้อมูลภาครัฐตามที่ระบุในข้อที่ 2 มีหน้าที่ในการดำเนินงานที่แตกต่างกันออกไป โดยเริ่มตั้งแต่การวางแผน การลงมือปฏิบัติ การตรวจสอบ และปรับปรุงอย่างต่อเนื่อง ตามลำดับ องค์ประกอบอย่างน้อยที่หน่วยงานจะต้องดำเนินการ ได้แก่

- สร้างการรับรู้ให้กับคนภายในหน่วยงาน
- ดำเนินการตามนโยบาย กฎเกณฑ์ของข้อมูล
- บริหารจัดการข้อมูล
- ส่งเสริมและสนับสนุนการแลกเปลี่ยน ตลอดจนการเชื่อมโยงข้อมูลระหว่างหน่วยงาน

6. ตรวจสอบเพื่อการประเมินผล การทำงานในภาพรวมเพื่อเป็นข้อมูลที่ใช้สำหรับการตัดสินใจ เพื่อการปรับปรุงหรือพัฒนาในอนาคต และบรรลุตามเป้าหมายที่วางไว้ตลอดจนเป็นแนวทางในการบริหารจัดการต่อไป ในกรอบธรรมาภิบาลข้อมูลภาครัฐนั้นจะต้องจัดทำอย่างสม่ำเสมอและต่อเนื่อง ดังนั้นหน่วยงานควรต้องดำเนินการและวัดผล ปรับปรุงประสิทธิภาพอยู่เสมอเพื่อยกระดับการดำเนินงานให้มีธรรมาภิบาลข้อมูลภาครัฐที่มีให้ดียิ่ง ๆ ขึ้น เพื่อประโยชน์ในการดำเนินงาน เพิ่มศักยภาพ ส่งผลดีทั้งต่อประชาชนและประเทศชาติต่อไป

บทที่ 4
กรอบธรรมาภิบาลข้อมูลของโรงงานไพ่

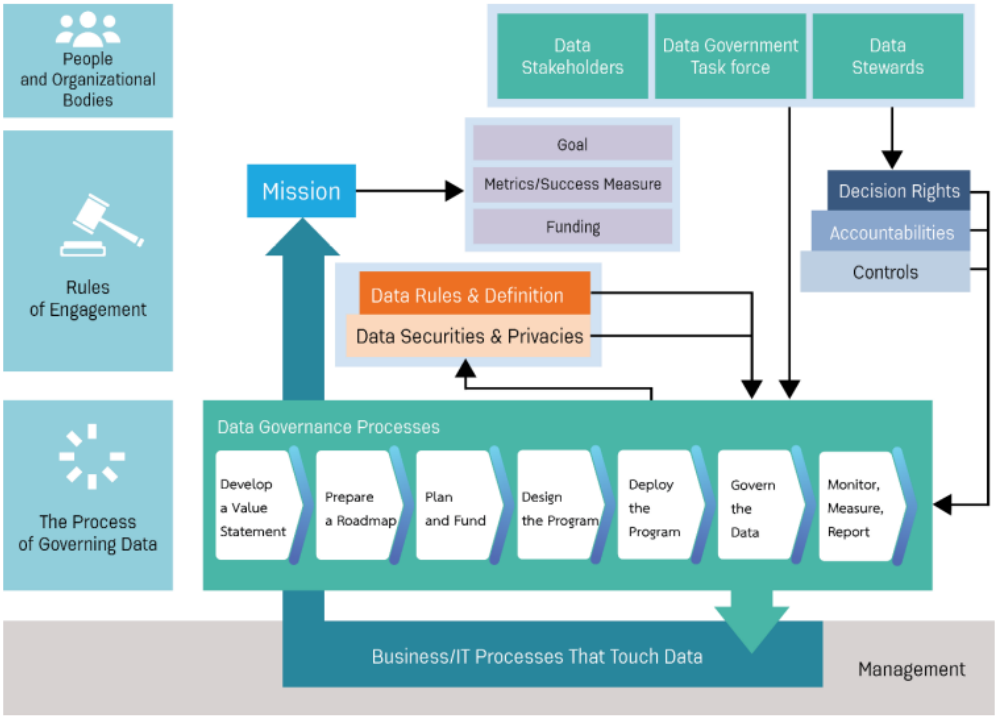
กรอบธรรมาภิบาลข้อมูลของ โรงงานไพ่ (DPO Data Governance Framework) ประกอบด้วยองค์ประกอบต่าง ๆ 3 ส่วนหลัก ได้แก่

1) ส่วนการดำเนินการด้านกฎหมาย กฎระเบียบ ข้อบังคับ แนวนโยบายที่เกี่ยวข้องกับการธรรมาภิบาลข้อมูล (Rules of Engagement)

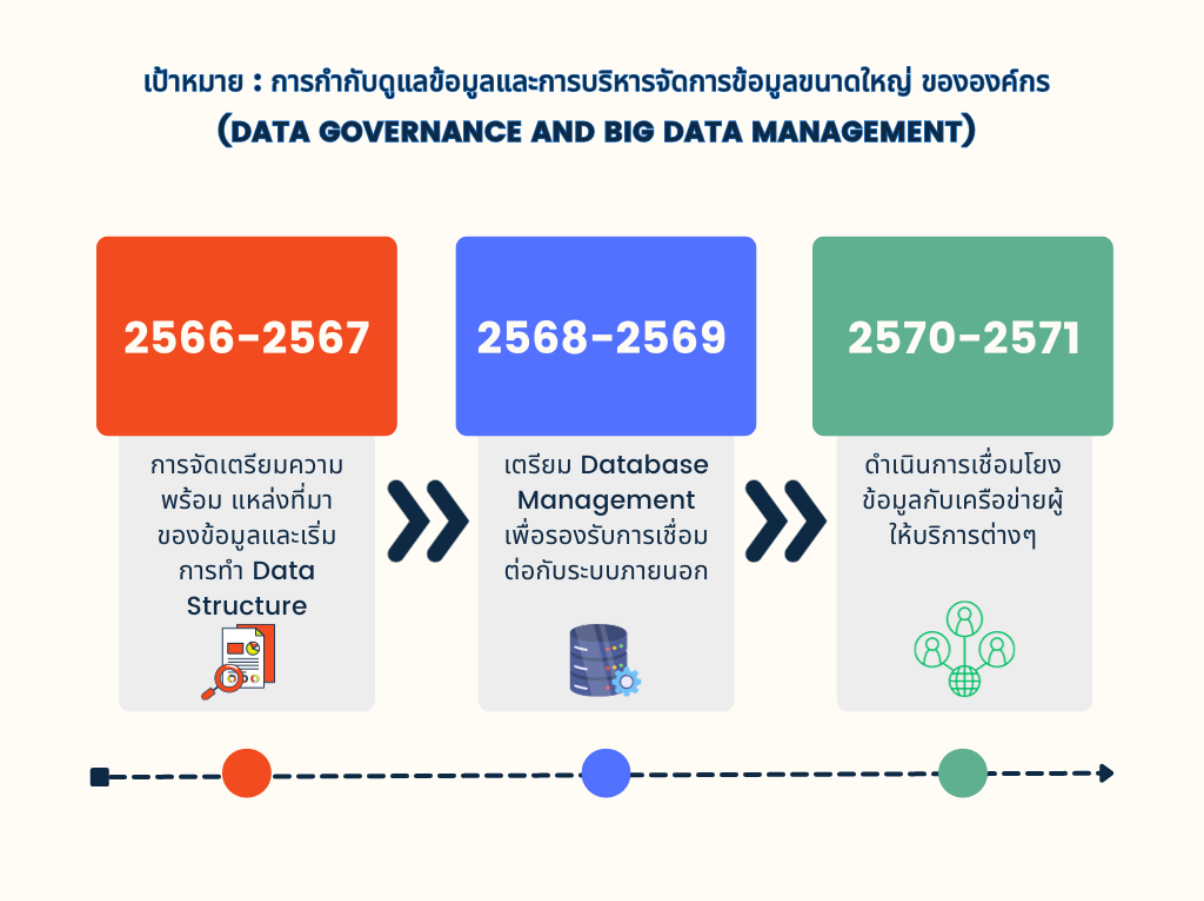
2) ส่วนการดำเนินการด้านโครงสร้างของบุคลากรที่รับผิดชอบในการธรรมาภิบาลข้อมูล (People and Organizational Bodies)

3) ส่วนการดำเนินการด้านกระบวนการธรรมาภิบาลข้อมูล (Data governance processes)

รวมถึงการดำเนินการด้านการวัดการดำเนินการและความสำเร็จของธรรมภิบาลข้อมูล ซึ่งทุกองค์ประกอบมีความสำคัญต่อการดำเนินงานด้านธรรมาภิบาลข้อมูล อันจะนำไปสู่การบรรลุเป้าหมายของการดำเนินงานตามที่ โรงงานไพ่ กำหนดไว้ ดังแสดงในภาพที่ 3-1 โดยสามารถอธิบายเป็นประเด็นต่าง ๆ ได้ดังนี้



4.1 เป้าหมาย การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management)



ระยะที่ 1 (2566-2567) จัดทำธรรมาภิบาลข้อมูล

- กำหนดกฎระเบียบและนโยบายในการใช้ข้อมูลอย่างมีความรับผิดชอบและปลอดภัย
- สร้างความตระหนักรู้และฝึกอบรมเกี่ยวกับการใช้ข้อมูลอย่างมีความรับผิดชอบ
- จัดทำแผนการบริหารจัดการข้อมูลและตัวชี้วัดเพื่อตรวจสอบความคืบหน้า

ระยะที่ 2 (2568-2569) จัดทำมาตรฐานข้อมูล

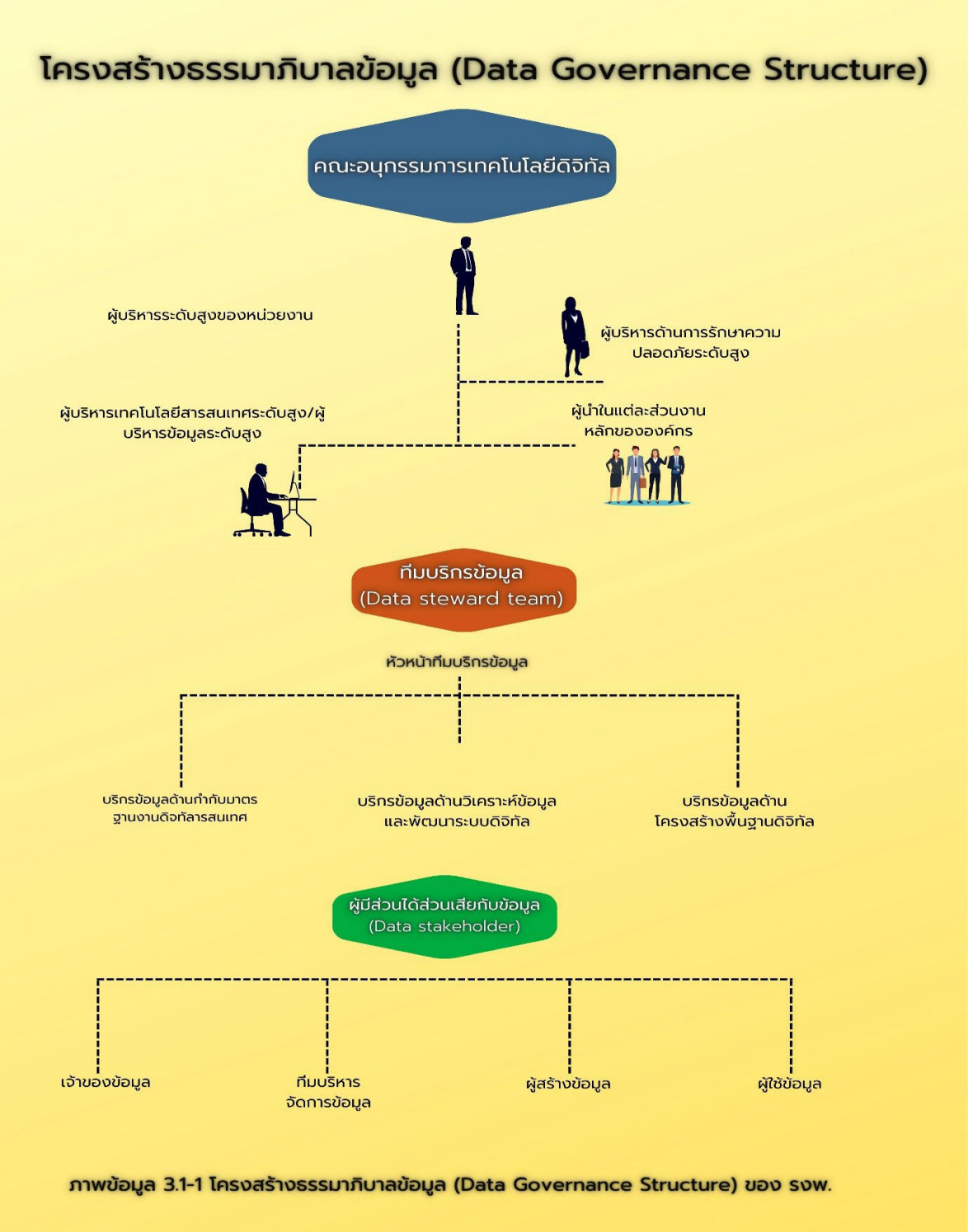
- สร้างโครงสร้างและรูปแบบข้อมูลมาตรฐาน
- จัดทำมาตรฐานการคุ้มครองข้อมูลและความเป็นส่วนตัว
- ปรับปรุงการจัดเก็บและการบริหารจัดการข้อมูลตามมาตรฐานที่กำหนด

ระยะที่ 3 (2570-2571) จัดการข้อมูลขนาดใหญ่

- สร้างโครงสร้างพื้นฐานและระบบสำหรับการจัดการข้อมูลขนาดใหญ่
- ปรับปรุงความสามารถในการวิเคราะห์ข้อมูลใหญ่และการดำเนินการตามข้อมูล
- สร้างกลยุทธ์ในการใช้ข้อมูลขนาดใหญ่ให้เป็นประโยชน์สูงสุดต่อองค์กร

4.2 โครงสร้างธรรมภิบาลข้อมูล

โครงสร้างของบุคลการที่รับผิดชอบในธรรมาภิบาลข้อมูล เป็นการกำหนดโครงสร้างบุคลากรภายในของ โรงงานไพ่ และแสดงลำดับขั้นระหว่างกลุ่มบุคคลที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล ตลอดจนการแสดงถึงสิทธิ์ในการสั่งการตามลำดับขั้น โดยใช้รูปแบบทีมเสมือน (Virtual Team) ที่คัดเลือกมาจากส่วนงานต่าง ๆ มาทำงานร่วมกัน และใช้วิธีการติดต่อสื่อสารภายในผ่านช่องทางต่าง ๆ ให้มีประสิทธิภาพ เพื่อลดข้อจำกัดด้านการปรับปรุงโครงสร้างองค์กร ดังแสดงในภาพที่ 4.1-1



ภาพข้อมูล 3.1-1 โครงสร้างธรรมาภิบาลข้อมูล (Data Governance Structure) ของ รงพ.

โครงสร้างธรรมภิบาลข้อมูลของ โรงงานไพ่ สามารถอธิบายได้ ดังนี้

4.1.1. คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล

คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล ทำหน้าที่เป็นผู้ธรรมาภิบาลข้อมูล (Data Governance) ประกอบไปด้วย รองประธานกรรมการเป็นประธานอนุกรรมการ 1 คน เป็นรองประธานอนุกรรมการ 1 คน อนุกรรมการอื่นไม่น้อยกว่า 2 คน รองผู้อำนวยการ และหัวหน้าฝ่ายอำนวยการโรงงานไพ่เป็นอนุกรรมการ โดยรวมไม่เกิน 7 คน อนุกรรมการอื่นอย่างน้อย 1 คนต้องมีความรู้ความเข้าใจและมีประสบการณ์ด้านเทคโนโลยีดิจิทัล และหัวหน้าส่วนสารสนเทศและพัฒนาระบบ เป็นเลขานุการคณะอนุกรรมการ และผู้นำ หรือผู้รับผิดชอบในแต่ละส่วนงานหลักขององค์กร (Key Business Unit Head) ได้แก่ ส่วนแผนงานและกลยุทธ์ ส่วนสารสนเทศและพัฒนาระบบ ส่วนทรัพยากรบุคคล ส่วนพัฒนาธุรกิจและการตลาด ฝ่ายผลิตไพ่ และฝ่ายโรงพิมพ์

ตารางที่ 4.1-1 ตำแหน่งและบทบาทหน้าที่ของคณะอนุกรรมการด้านเทคโนโลยีดิจิทัล

คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล	บทบาทหน้าที่
(1) ประธานกรรมการ (2) รองประธานกรรมการ (3) รองผู้อำนวยการ (4) หัวหน้าฝ่ายอำนวยการ (5) มีความรู้ความเข้าใจและมีประสบการณ์ด้านเทคโนโลยีดิจิทัล (6) หัวหน้าส่วนสารสนเทศและพัฒนาระบบ	ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการภายใน คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล
(7) ผู้รับผิดชอบในแต่ละส่วนงานหลัก ขององค์กร (Key Business Unit Head) - ฝ่ายผลิตไพ่ - ฝ่ายโรงพิมพ์ - ส่วนแผนงานและกลยุทธ์ - ส่วนสารสนเทศและพัฒนาระบบ - ส่วนทรัพยากรบุคคล - ส่วนพัฒนาธุรกิจและการตลาด	- วิเคราะห์ข้อมูลของหน่วยงานเพื่อสร้างและส่งมอบ เทคโนโลยี เครื่องมือ แนวทาง และวิธีการในการทำให้ ข้อมูลของหน่วยงานมีคุณค่า และเกิดประโยชน์สูงสุด ต่อองค์กร เพื่อขยายผลต่อไปให้เกิดผลสัมฤทธิ์ ในการส่งเสริมให้ องค์กรใช้ข้อมูลได้อย่างถูกต้อง และมีประสิทธิภาพ - วิเคราะห์ข้อมูลร่วมกับผู้บริหารส่วนอื่น ๆ เพื่อจัดทำ ยุทธศาสตร์ และดำเนินการกำกับดูแลข้อมูลให้มีคุณภาพ และการควบคุมอื่น ๆ เพื่อรักษาความสมบูรณ์ของข้อมูลขององค์กร - บริหารข้อมูลให้มีความปลอดภัย และเพียงพอสำหรับการทำงาน - ทำให้เกิดการเชื่อมต่อระหว่างหน่วยงานภาครัฐ รวมทั้งปรับปรุงความมั่นคงทางกายภาพ และความปลอดภัยด้านเทคโนโลยีให้มากขึ้น - ทำงานร่วมกับผู้บริหารอื่น ๆ ในการตัดสินใจเกี่ยวกับ ลำดับความสำคัญของความต้องการด้านความปลอดภัย

คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล	บทบาทหน้าที่
	- กำหนดเป้าหมายและวัตถุประสงค์ของการป้องกัน หน่วยงานเพื่อให้สอดคล้องกับแผนกลยุทธ์ของ หน่วยงาน - ให้คำแนะนำ ข้อเสนอแนะ และวิพากษ์ประเด็นต่าง ๆ - ที่เกี่ยวข้องกับการบริหารจัดการข้อมูลในส่วนงานที่ตนเอง รับผิดชอบ และส่วนงานอื่น ๆ ที่เกี่ยวข้อง - ร่วมกำหนดนโยบายธรรมาภิบาลข้อมูล - สื่อสารไปยังทีมงานภายใต้ส่วนงานที่ตนรับผิดชอบ เพื่อให้บุคลากรอื่น ๆ ในองค์กร ได้รับทราบถึงนโยบาย และแนวปฏิบัติของธรรมาภิบาลข้อมูล

4.1.2. ทีมบริกรข้อมูล (Data Steward Team)

ทีมบริกรข้อมูลทำหน้าที่ในการให้ข้อมูล และให้ความรู้ต่าง ๆ ที่เกี่ยวข้องกับการบริหารงานดิจิทัล การกำกับมาตรฐานงานด้านดิจิทัล และโครงสร้างพื้นฐานของงานดิจิทัลในด้านต่าง ๆ อันจะสนับสนุนให้เกิดการกำกับดูแลข้อมูลที่ดีอย่างเป็นระบบ อย่างไรก็ตาม ทีมบริกรข้อมูลไม่ได้มีการกำหนดโครงสร้างของทีมงานอย่างชัดเจน โดยสามารถปรับเปลี่ยนตามความต้องการ หรือบริบทองค์กรนั้น ๆ เป็นสำคัญ ทั้งนี้เมื่อพิจารณาจากโครงสร้างองค์กรของโรงงานไพ่ ในปัจจุบัน สามารถนำมากำหนดเป็นทีมบริกรข้อมูลได้ ดังนี้

ตารางที่ 4.1-2 ตำแหน่งและบทบาทหน้าที่ของทีมบริกรข้อมูล

ทีมบริกรข้อมูล	บทบาทหน้าที่
(1) หัวหน้าบริกรข้อมูล (Lead Data Steward) (หัวหน้าส่วนสารสนเทศและพัฒนาระบบ)	ควบคุมและสั่งการภายในทีมบริกรข้อมูล
(2) บริการข้อมูลด้านการกำกับมาตรฐาน งานดิจิทัล สารสนเทศ (เจ้าหน้าที่สารสนเทศอาวุโส 2)	- กำหนดมาตรฐาน แผนงาน และการให้บริการ - ควบคุม กำกับ และติดตามมาตรฐานการทำงานด้าน สารสนเทศ - เผยแพร่ความรู้ด้านมาตรฐานและความตระหนักในการใช้ งานระบบสารสนเทศขององค์กรร่วมกัน - สำรวจ เก็บรวบรวมข้อมูล ติดตามความเคลื่อนไหวของสถานการณ์ และแนวโน้มการพัฒนาด้านดิจิทัล
(3) บริการข้อมูลด้านวิเคราะห์ข้อมูล พัฒนาระบบดิจิทัล และโครงสร้างพื้นฐาน ดิจิทัล (เจ้าหน้าที่ส่วนสารสนเทศ)	- ให้คำปรึกษาแก่ส่วนงานต่าง ๆ ขององค์กรในการพัฒนา ด้านเทคนิคและการนำไปประยุกต์ใช้บริหารข้อมูล สารสนเทศ

ทีมบริกรข้อมูล	บทบาทหน้าที่
	- รวบรวมและสร้างความเป็นเอกภาพและความแม่นยำของ ข้อมูลที่สำคัญทั้งส่วนงานภายในและภายนอก - การพัฒนางานคอมพิวเตอร์ ให้คำปรึกษาและแนะนำ หรือ ฝึกอบรม การใช้คอมพิวเตอร์ และการใช้โปรแกรมพัฒนา บุคลากรภาครัฐด้านเทคโนโลยีสารสนเทศและการสื่อสาร - กำหนดแนวทางในการใช้โครงข่ายพื้นฐานเพื่อสนับสนุน เทคโนโลยีสารสนเทศขององค์กร - จัดทำ ปรับปรุง และพัฒนาประสิทธิภาพงานด้านโครงสร้าง พื้นฐานสารสนเทศขององค์กร ให้ครอบคลุมทุกส่วนงานให้ เกิดความพร้อมใช้ตลอดเวลา - พัฒนาระบบเครือข่าย รวมทั้งเฝ้าระวัง ป้องกันและแก้ไข ภัยคุกคาม ที่อาจเกิดขึ้น จากระบบงานเทคโนโลยี สารสนเทศ - ประสานงานและสนับสนุนด้านเทคโนโลยีสารสนเทศ โดย ดำเนินการบริหารโครงสร้างพื้นฐานด้านเทคโนโลยี สารสนเทศขององค์กรทั้งที่เป็นศูนย์กลางหรือที่ใช้ร่วมกัน - บำรุงรักษางานโครงสร้างพื้นฐานสารสนเทศให้พร้อมใช้งาน ตลอดเวลา แก้ไข และช่วยเหลือผู้ใช้งานระบบสารสนเทศในองค์กร

4.1.3. ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders)

ผู้มีส่วนได้เสียกับข้อมูลที่ทำหน้าที่ให้การสนับสนุนการกำกับดูแลข้อมูลขององค์กร ต่อทีมบริกร ข้อมูลและ คณะอนุกรรมการเทคโนโลยีดิจิทัล ประกอบไปด้วย เจ้าของข้อมูล (Data Owners) ทีมบริหารจัดการ ข้อมูล (Data Management Team) ผู้สร้างข้อมูล (Data Creators) และผู้ใช้ข้อมูล (Data Users) โดยผู้มีส่วนได้เสียกับข้อมูลกลุ่มนี้ มีบทบาทหน้าที่ดังนี้

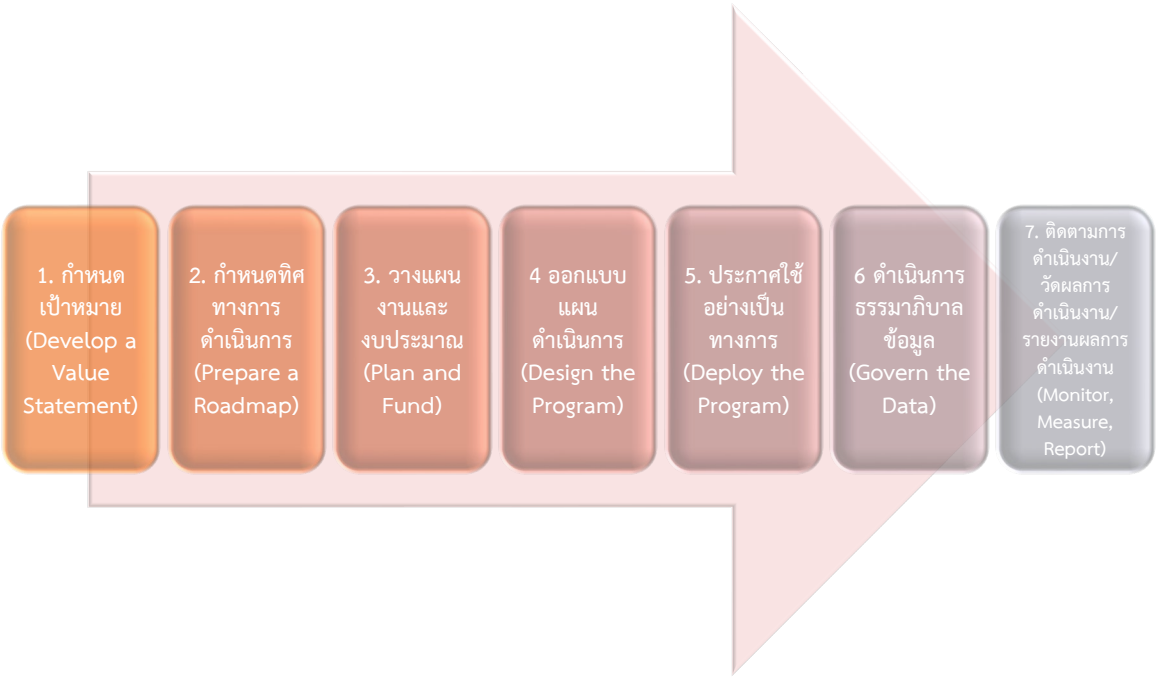
ตารางที่ 4.1-3 ตำแหน่งและบทบาทหน้าที่ของผู้มีส่วนได้เสียกับข้อมูล

ผู้มีส่วนได้ส่วนเสียข้อมูล	บทบาทหน้าที่
(1) เจ้าของข้อมูล (Data Owners)	ตรวจสอบดูแลข้อมูลโดยตรง เพื่อสร้างความมั่นใจได้ว่าการ บริหารจัดการข้อมูลมีความสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย โดยเจ้าของข้อมูลจะทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล

ผู้มีส่วนได้ส่วนเสียข้อมูล	บทบาทหน้าที่
(2) ทีมบริหารจัดการข้อมูล (Data Management Team) (2.1) สถาปนิกข้อมูล (Data Architects) (2.2) นักจัดการฐานข้อมูล (Database Administrators) (2.3) นักวิเคราะห์ข้อมูล (Data Analysts) (2.4) นักวิทยาการข้อมูล (Data Scientists)	- มีหน้าที่หลักในการบริหารจัดการข้อมูลให้สอดคล้องกับการ บริหารจัดการข้อมูล ประกอบด้วย - สถาปัตยกรรมข้อมูล (Data Architecture) - การจำลองและการออกแบบข้อมูล (Data Modeling and Design) - การจัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operations) - การบูรณาการและความสามารถในการทำงานร่วมกัน (Data Integration and Interoperability) - การบริหารจัดการเอกสารและเนื้อหา (Document and Content Management) - ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data) คลังข้อมูล ทะเลสาบข้อมูล (Data Lake) ระบบรายงานอัจฉริยะ และการวิเคราะห์ข้อมูล (Data Warehouse, Data Lake, Business Intelligence, and Data Analytics) - คำอธิบายชุดข้อมูลดิจิทัล หรือ ข้อมูลอภิพันธุ์ (Metadata) - ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคล ของข้อมูล (Data Security and Privacy) - คุณภาพของข้อมูล (Data Quality)
(3) ผู้สร้างข้อมูล (Data Creators) ได้แก่ - ฝ่ายงานต่าง ๆ ในโรงงานไพ่ - ผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้องกับโรงงานไพ่	ทำหน้าที่ในการบันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้ สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ นอกจากนี้ยังมีหน้าที่ ในการทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบและแก้ไข ปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย
(4) ผู้ใช้ข้อมูล (Data Users) ได้แก่ - ผู้บริหารและพนักงานโรงงานไพ่ - ลูกค้าของโรงงานไพ่ - คู่ค้าของโรงงานไพ่ - ผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้องกับโรงงานไพ่	ทำหน้าที่ในการนำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและ ระดับบริหาร และสนับสนุนการกำกับดูแลข้อมูลภาครัฐ โดย การให้ความต้องการในการใช้ข้อมูล พร้อมทั้งรายงานประเด็น ปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังบริกรข้อมูล

4.3 กระบวนการธรรมาภิบาลข้อมูล (Data Governance Processes)

การกำหนดกระบวนการธรรมาภิบาลข้อมูล เป็นการกำหนดขั้นตอนที่ใช้ในการดำเนินการธรรมาภิบาลข้อมูลของโรงงานไพ่ เพื่อให้เป็นไปตามกฎหมาย กฎระเบียบ ข้อบังคับ แนวนโยบายที่เกี่ยวข้องกับการธรรมาภิบาลข้อมูล โดยเริ่มตั้งแต่ระดับการวางแผน ไปจนถึงระดับการปรับปรุงอย่างต่อเนื่อง เพื่อให้การข้อมูลของโรงงานไพ่ มีคุณภาพ มีความปลอดภัย สร้างมูลค่า และสามารถเพิ่มศักยภาพในการดำเนินงานทั้งในส่วนของการ เปิดเผยข้อมูล การเชื่อมโยงข้อมูลและแลกเปลี่ยน และการสร้างประโยชน์จากข้อมูลสำหรับการดำเนินงาน ตามภารกิจของโรงงานไพ่ โดยมีขั้นตอนของกระบวนการธรรมาภิบาลข้อมูล ดังรูปที่ 4.2-2



ภาพที่ ๔.๒-๒ กระบวนการธรรมาภิบาลข้อมูลของ โรงงานไพ่

4.2.1 กำหนดเป้าหมาย (Develop a Value Statement)

เป็นการกำหนดผลลัพธ์ที่คาดหวังว่าจะ ได้รับจากการดำเนินงานธรรมาภิบาลข้อมูล โดยเป้าหมายธรรมาภิบาลข้อมูลของโรงงานไพ่ ได้แก่ ข้อมูลของโรงงานไพ่ มีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มีความมั่นคงปลอดภัย ไม่ละเมิดระเบียบข้อบังคับต่าง ๆ รวมทั้ง สามารถเชื่อมโยงและบูรณาการข้อมูลจากทั้งภายในองค์กรและภายนอกองค์กรได้อย่างมีประสิทธิภาพ สามารถนำไปสู่การพัฒนาองค์กรให้เกิดประโยชน์ได้อย่างสูงสุด

เป้าหมายการดำเนินงานธรรมาภิบาลข้อมูลของโรงงานไพ่

ข้อมูลของโรงงานไพ่ มีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มีความมั่นคงปลอดภัย ไม่ละเมิดระเบียบข้อบังคับต่าง ๆ รวมทั้ง สามารถเชื่อมโยงและบูรณาการข้อมูลจากทั้งภายในองค์กรและภายนอกองค์กรได้อย่างมีประสิทธิภาพ สามารถนำไปสู่การพัฒนาองค์กรให้เกิดประโยชน์ได้อย่างสูงสุด

4.2.2 กำหนดทิศทางการดำเนินการ (Prepare a Roadmap)

ซึ่งเป็นการกำหนดวิธีการดำเนินการ ธรรมาภิบาลข้อมูลและบริหารจัดการข้อมูล โดยพิจารณาถึงความพร้อมขององค์กร เพื่อให้สามารถขับเคลื่อน ไปสู่การบรรลุเป้าหมายที่กำหนดไว้

4.2.3 วางแผนงานและงบประมาณ (Plan and Fund)

เป็นการกำหนดรายละเอียดของขอบเขตการ ดำเนินงาน และงบประมาณที่จะต้องใช้ในการดำเนินการ

4.2.4 ออกแบบแผนดำเนินการ (Design the Program)

เป็นการกำหนดรายละเอียดของแผนการ ดำเนินงาน ประกอบด้วย

4.2.4.1. กลยุทธ์
4.2.4.2. โครงการ/กิจกรรม
4.2.4.3. วัตถุประสงค์การดำเนินงาน
4.2.4.4. หน่วยงานผู้รับผิดชอบ
4.2.4.5. วิธีการประเมินผลการดำเนินงาน
4.2.4.6. ผลผลิตและผลลัพธ์ที่ได้จากการดำเนินงาน
4.2.4.7. ระยะเวลาการดำเนินงาน

4.2.5 ประกาศใช้อย่างเป็นทางการ (Deploy the Program)

เป็นการสื่อสารให้บุคลากรภายในองค์กร ได้รับรู้ ตระหนัก และเข้าใจถึงเป้าหมาย นโยบายและแนวทางการดำเนินงานธรรมาภิบาลข้อมูลของโรงงานไพ่ อันจะนำไปสู่การปฏิบัติตนอย่างเหมาะสมกับบทบาทหน้าที่ของแต่ละบุคคล โดยวิธีการประกาศนั้นจะผ่านช่อง ทางการสื่อสารที่หลากหลายเพื่อให้สามารถเข้าถึงบุคลากรได้ทุกกลุ่ม ได้แก่ การติดประกาศตามจุดต่าง ๆ ของ องค์กร เว็บไซต์ หนังสือเวียนองค์กร และการสื่อสารในที่ประชุม

4.2.6 ดำเนินการธรรมาภิบาลข้อมูล (Govern the Data)

เป็นการปฏิบัติตามแผนการดำเนินงานที่ได้ ออกแบบไว้ของบุคคลที่เกี่ยวข้องกับกับกระบวนการธรรมาภิบาลข้อมูล ตามที่ระบุไว้ในโครงสร้างธรรมาภิบาล ข้อมูล โดยในระหว่างการดำเนินงาน

นั้น กำหนดให้มีการประชุมคณะกรรมการฯ เป็นระยะ เพื่อติดตามผลการ ดำเนินงาน หากพบประเด็นปัญหาที่เกิดขึ้นจะสามารถแก้ไขได้อย่างทันท่วงที

4.2.7 ติดตามการดำเนินงาน/วัดผลการดำเนินงาน/รายงานผลการดำเนินงาน (Monitor, Measure, Report)

เป็นการติดตามการดำเนินงาน และตรวจสอบโดยบริกรข้อมูลจะดำเนินการตรวจสอบความสอดคล้องกันระหว่างกฎระเบียบ นโยบาย และมาตรฐานที่กำหนด กับการปฏิบัติงานของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ พร้อมทั้งทำการวัดผลด้านคุณภาพข้อมูล หลังจากนั้นรายงานผลความสอดคล้อง คุณภาพข้อมูล ความมั่นคงปลอดภัย และความเสี่ยงที่เกี่ยวข้องกับข้อมูลไปยังคณะอนุกรรมการด้านเทคโนโลยีดิจิทัลและผู้ที่เกี่ยวข้อง เพื่อให้ทราบถึงผลการดำเนินงานและประเด็นปัญหาที่พบ ทั้งนี้การกำหนดตัวชี้วัดวัดผลการดำเนินงานจะขึ้นอยู่กับการออกแบบแผนการดำเนินในแต่ละกิจกรรม โดยสามารถยกตัวอย่างตัวชี้วัดที่ช่วยสะท้อนผลการดำเนินงานธรรมาภิบาลข้อมูลได้ ดังนี้

4.2.7.1. จำนวนผู้ที่ทำผิดกฎ ระเบียบ หรือข้อบังคับต่างๆ ที่เกี่ยวข้องกับข้อมูลที่โรงงานไพ่กำหนด

4.2.4.2. จำนวนหน่วยงานภายนอกที่มีการบูรณาการข้อมูลร่วมกันกับโรงงานไพ่

4.2.4.3. จำนวนข้อมูลที่ได้รับการตรวจสอบความถูกต้องสมบูรณ์

4.2.4.4. โรงงานไพ่สามารถยกระดับประสิทธิภาพการดำเนินงานมากขึ้น จากการนำข้อมูลมาช่วย สนับสนุนการดำเนินงาน

โดยสรุป กระบวนการจัดทำธรรมาภิบาลข้อมูลจะต้องดำเนินการอย่างต่อเนื่อง ตามระบบบริหาร และกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล เนื่องจากบริบทของการบริหารจัดการ กฎหมาย กฎระเบียบ รวมถึงความต้องการของผู้มีส่วนได้ส่วนเสียมีการเปลี่ยนแปลงตลอดเวลา ตลอดจนรายงานผลจาก การติดตามและตรวจสอบการดำเนินการธรรมาภิบาลข้อมูลที่พบเจอ ทำให้ต้องมีการทบทวนและปรับปรุง อย่างต่อเนื่อง (Continual Improvement)

4.4 แนวทางการจัดการกระบวนการธรรมาภิบาลข้อมูล

เพื่อให้เกิดความเข้าใจในกระบวนการธรรมาภิบาลข้อมูลของโรงงานไพ่ และเห็นความสัมพันธ์ระหว่างกระบวนการธรรมาภิบาลข้อมูล เครื่องมือ หรือเอกสารที่ใช้ในการธรรมาภิบาลข้อมูล ผลลัพธ์ที่ได้ และผู้ที่เกี่ยวข้องหรือผู้มีส่วนได้ส่วนเสีย ดังแสดงในตารางที่ 4.3-1 และความสัมพันธ์ระหว่างกระบวนการ / กิจกรรม และผู้มีส่วนได้ส่วนเสียกับข้อมูล ดังแสดงในตารางที่ 4.3-2

ตารางที่ 4.3-1 ความสัมพันธ์ระหว่างระดับของกระบวนการ กระบวนการ ส่วนนำเข้า สวนนำออก และผู้มีส่วนได้เสียกับกระบวนการ

ระดับของกระบวนการ	กระบวนการ	ส่วนนำเข้า	ส่วนนำออก	ผู้มีส่วนได้ส่วนเสีย
การวางแผน	1) กำหนดเป้าหมาย 2) กำหนดทิศทางการดำเนินการ 3) วางแผนงานและงบประมาณ 4) ออกแบบแผนดำเนินการ 5) ประกาศใช้อย่างเป็นทางการ	1) นโยบาย กฎ ระเบียบ ข้อบังคับและกฎหมายที่เกี่ยวข้องกับข้อมูล 2) รายการชุดข้อมูล 3) รายการประเด็นปัญหาจากรายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล รายงานความเสี่ยงต่อข้อมูล	1) แผนดำเนินการ (กิจกรรม บุคลากร งบประมาณและระยะเวลาในการดำเนินการ)	1) คณะกรรมการธรรมาภิบาลข้อมูล 2) บริกรข้อมูลด้านธุรกิจ 3) บริกรข้อมูลด้านเทคนิค 4) บริกรข้อมูลด้านคุณภาพ
การปฏิบัติ	1) ดำเนินการธรรมาภิบาลข้อมูล	1) นโยบาย กฎ ระเบียบ ข้อบังคับและกฎหมายที่เกี่ยวข้องกับข้อมูล 2) แผนดำเนินการ (กิจกรรม บุคลากร งบประมาณและระยะเวลาในการดำเนินการ)	1) รายงานความก้าวหน้าในการปฏิบัติงาน 2) ผลการปฏิบัติงาน 3) ประเด็นปัญหาที่พบระหว่างปฏิบัติงาน	1) ผู้บริหารงาน 2) ผู้ปฏิบัติงานที่เกี่ยวข้อง 3) บริกรข้อมูลด้านธุรกิจ 4) บริกรข้อมูลด้านเทคนิค 5) บริกรข้อมูลด้านคุณภาพ
การตรวจสอบ	1) ติดตามการดำเนินงาน /วัดผลการดำเนินงาน /รายงานผลการดำเนินงาน	1) นโยบาย กฎ ระเบียบ ข้อบังคับและกฎหมายที่เกี่ยวข้องกับข้อมูล 2) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูล ระดับคุณภาพข้อมูล	1) รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล 2) รายงานคุณภาพข้อมูล 3) รายงานความมั่นคงปลอดภัยต่อข้อมูล 4) รายงานความเสี่ยงต่อข้อมูล	1) บริกรข้อมูลด้านธุรกิจ 2) บริกรข้อมูลด้านเทคนิค 3) บริกรข้อมูลด้านคุณภาพ

ระดับของกระบวนการ	กระบวนการ	ส่วนนำเข้า	ส่วนนำออก	ผู้มีส่วนได้ส่วนเสีย
ปรับปรุงธรรมาภิบาล	1) การปรับปรุงอย่างต่อเนื่อง	1) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล 2) โครงสร้างธรรมาภิบาลข้อมูล 3) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูล และคุณภาพข้อมูล 4) รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบาย ข้อมูล รายงานความมั่นคงปลอดภัย ต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล 5) รายการความต้องการจากผู้บริหารและผู้มีส่วนได้เสีย	1) กระบวนการธรรมาภิบาลข้อมูล 2) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล 3) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูล และคุณภาพข้อมูล 4) โครงสร้างธรรมาภิบาลข้อมูล	1) คณะกรรมการธรรมาภิบาลข้อมูล 2) บริกรข้อมูลด้านธุรกิจ 3) บริกรข้อมูลด้านเทคนิค 4) บริกรข้อมูลด้านคุณภาพ

จากตารางข้างต้นจะเห็นได้ว่า แนวทางการจัดการกระบวนการธรรมาภิบาลข้อมูลของโรงงานไพ่ จะประกอบด้วยกระบวนการต่าง ๆ ซึ่งภายใต้ในแต่ละกระบวนการนั้น ๆ จะมีผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการ โดยมีบทบาทหน้าที่และความรับผิดชอบที่แตกต่างกันไป ประกอบด้วย ผู้ที่มีหน้าที่ในการดูแลรับผิดชอบให้กิจกรรม นั้น ๆ (R) ผู้ที่มีหน้าที่ในการกำหนดแนวทาง หรือเป้าหมายของกิจกรรม (A) ผู้ที่มีหน้าที่ในการให้คำปรึกษา (C) และผู้ที่ต้องรับรู้ข้อมูลกระบวนการ/กิจกรรมต่าง ๆ ที่กำลังดำเนินงาน โดยสามารถสรุปได้ดังนี้

ตารางที่ 4.3-2 ความสัมพันธ์ระหว่างกระบวนการ/ กิจกรรม และผู้มีส่วนไดส่วนเสียที่เกี่ยวข้องกับกระบวนการ

กระบวนการ/กิจกรรม	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการ				
	คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล	ทีมบริกรข้อมูล	เจ้าของข้อมูล	ทีมบริหารจัดการ ข้อมูล	ผู้สร้างและใช้งาน ข้อมูล
กำหนดและปรับปรุงนโยบายและมาตรฐานข้อมูล	A	R	R	R	R
ตรวจสอบการปฏิบัติตามนโยบายข้อมูล	A	R	R	R	R
การประเมินความพร้อมของธรรมาภิบาลข้อมูล	C,I	A	R	R	R
ประเมินความมั่นคงปลอดภัยและคุณภาพข้อมูล	C,I	C,I	I	A	I
รายงานผลการตรวจสอบความมั่นคงปลอดภัยและคุณภาพข้อมูล	C	A	I	R	I
กำหนดสิทธิในการเข้าถึงข้อมูล	A	R	I	R	I

หมายเหตุ :	**R**esponsible	หมายถึง ผู้ที่มีหน้าที่ในการดูแลรับผิดชอบให้กิจกรรมนั้น ๆ ประสบความสำเร็จ
	Accountable	หมายถึง ผู้ที่มีหน้าที่ในการกำหนดแนวทาง หรือเป้าหมายของกิจกรรมต่าง ๆ รวมทั้งอำนาจในกระบวนการปฏิบัติงานนั้น ๆ
	Consulted	หมายถึง ผู้ที่มีหน้าที่ในการให้คำปรึกษา ให้ความรู้ หรือคำแนะนำต่าง ๆ
	Informed	หมายถึง บุคคลอื่น ๆ ที่เกี่ยวข้องกับกระบวนการนั้น ๆ ที่จะต้องรับรู้ถึงข้อมูลในกระบวนการต่าง ๆ ร่วมด้วย

4.5 การกำหนดกฎหมาย กฎระเบียบ ข้อบังคับ และแนวนโยบายที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล

4.4.1 การกำหนดทิศทางการดำเนินการและแนวนโยบายที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล

4.4.1.1 การกำหนดภารกิจ (Mission) และวิสัยทัศน์ (Vision) ในธรรมาภิบาลข้อมูลจะต้องมีกำหนดเป็นภารกิจที่ชัดเจน เพื่อให้มีทิศทางการดำเนินการธรรมาภิบาลข้อมูล โดยควรมุ่งเน้นการตอบสนองและให้บริการต่อผู้มีส่วนได้ส่วนเสีย ให้ครบทุกมิติ ทั้งนี้จะต้องสอดคล้องกับวิสัยทัศน์ขององค์กร คือ เป็นผู้นำด้านสิ่งพิมพ์ปลอดการปลอมแปลงและดิจิทัลปริ้นติ้งโซลูชั่นภาครัฐ และพันธกิจหลักต่างๆ ที่กำหนดไว้ รวมถึงจะต้องมีการทบทวนนโยบายและบริบทของสภาพแวดล้อมข้อมูล เทคโนโลยีดิจิทัลในปัจจุบันและอนาคตมาประกอบรวมกันทุกส่วนแล้วกำหนดเป็นภารกิจด้านธรรมาภิบาลข้อมูลของโรงงานไพ่

4.4.1.2 การกำหนดเป้าหมาย (Goal) การวัดการดำเนินการ (Metrics) การวัดความสำเร็จ (Success Measure) และการจัดหางบประมาณ (Funding) การดำเนินการธรรมาภิบาลข้อมูลจะต้องมีการระบุเป้าหมาย และระบุแนวทางการวัดความสำเร็จของการดำเนินการ รวมถึงจะต้องการมีการวางแผนด้านงบประมาณที่ต้องใช้ในการดำเนินการ เพื่อให้มีความพร้อมในการดำเนินการและให้เกิดความสำเร็จด้านธรรมาภิบาลข้อมูล

4.4.1.3 การกำหนดสิทธิในการตัดสินใจ (Decision Rights) การดำเนินการธรรมาภิบาลข้อมูลตามกระบวนการธรรมาภิบาลข้อมูลมีผู้ที่เกี่ยวข้องในกระบวนการหลายส่วนงาน ตามที่ระบุไว้ในโครงสร้างธรรมาภิบาลข้อมูล เพื่อให้การดำเนินการเป็นมีความคล่องตัวในธรรมาภิบาลข้อมูล จะต้องกำหนดโครงสร้างสิทธิในการตัดสินใจ โดยพิจารณาจากระดับความสำคัญของข้อมูล หรือกิจกรรมที่อยู่ในกระบวนการธรรมาภิบาลข้อมูล ประกอบกับโครงสร้างองค์กร รวมถึงอำนาจหน้าที่ผู้บริหารที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล โดยในการออกแบบโครงสร้างการตัดสินใจควรคำนึงถึงความถูกต้อง รวดเร็วและตรวจสอบได้

4.4.1.4 การกำหนดความรับผิดชอบต่อความสำเร็จ (Accountabilities) การกำหนดภาระความผิดชอบตาม โครงสร้างการธรรมาภิบาลข้อมูล (People and Organizational Bodies) จะต้องระบุบทบาท (Roles) หน้าที่ (Responsibilities) และความรับผิดชอบต่อความสำเร็จ (Accountabilities) ของบุคลากรในโครงสร้างให้ชัดเจน และสอดคล้องกับโครงสร้างหลักในการดำเนินงานของโรงงานไพ่ เพื่อให้มีผู้รับผิดชอบในกิจกรรมในกระบวนการธรรมภิบาลข้อมูลที่ชัดเจนและครบถ้วน

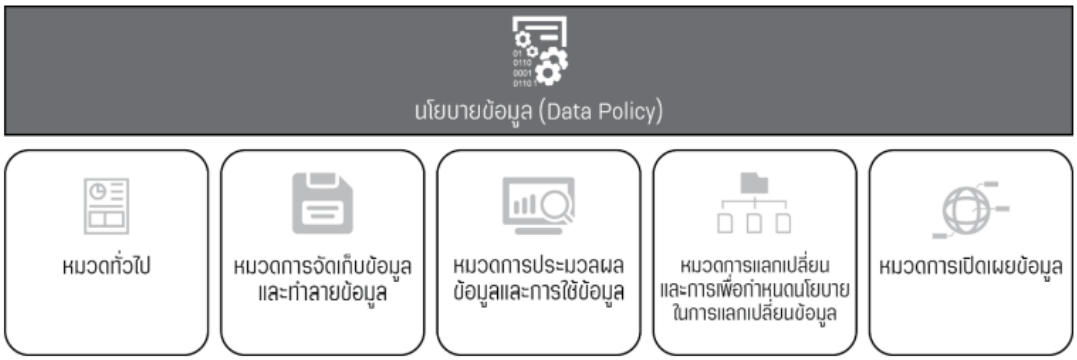
4.4.1.5 การกำหนดกลไกการควบคุมความเสี่ยง (Controls) เพื่อกำหนดขั้นตอนกระบวนการ หรือกลไกการควบคุมธรรมาภิบาลข้อมูล เพื่อให้มั่นใจว่าเป็นไปตามนโยบาย กฎ ระเบียบของธรรมาภิบาลข้อมูล โดยมีรูปแบบการควบคุม ประกอบด้วย การควบคุมแบบป้องกัน (Preventive Control) การควบคุมแบบตรวจสอบ (Detective Control) และ การควบคุมแบบแก้ไข (Corrective Control) รวมถึงการกำหนดวิธีการควบคุมโดยใช้บุคคล หรือเทคโนโลยีเข้ามาช่วยในการควบคุม

4.4.2 การกำหนดทิศทางการดำเนินการ

การกำหนดทิศทางการดำเนินการและความสอดคล้องกับกฎระเบียบด้านข้อมูลในธรรมาภิบาลข้อมูลจะต้องมีการมีการกำหนดความถูกต้องและชัดเจนของข้อมูล เพื่อให้เกิดความเข้าใจที่ตรงกันระหว่างผู้ที่เกี่ยวข้อง รวมถึงต้องมีการพิจารณาถึงกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูลทั้งในส่วนที่เป็นกฎหมาย นโยบาย และมาตรฐานของข้อมูล จะต้องมีความสอดคล้องกับธรรมาภิบาลข้อมูล เพื่อให้มีแนวทางในการดำเนินการ จะต้องพิจารณาในประเด็นหลักๆ ที่เกี่ยวข้อง ดังนี้

4.4.2.1 กฎเกณฑ์ข้อมูล (Data Rules) โดยทั่วไปการกำหนดกฎเกณฑ์ข้อมูล จะจัดทำเป็นนโยบายข้อมูล (Data Policies) และการจัดทำมาตรฐานข้อมูล (Data Standards) โดยมีรายละเอียด ดังนี้

(1) นโยบายข้อมูล (Data Policies) การกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในพื้นฐานของธรรมาภิบาลข้อมูลภาครัฐ ดังนั้น เพื่อให้ธรรมาภิบาลข้อมูลภาครัฐมีประสิทธิภาพ จึงต้องมีการกำหนดนโยบายที่ระบุอย่างชัดเจน สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง โดยผ่านการอนุมัติจากผู้บริหาร มีการเผยแพร่และสื่อสารให้กับเจ้าหน้าที่และผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน รวมถึงควรมีการทบทวนนโยบายอย่างสม่ำเสมอ เพื่อให้นโยบายข้อมูลได้ถูกนำมาปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง โดยนโยบายข้อมูลควรจะครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูล ซึ่งจะต้องประกอบไปด้วยนโยบายต่างๆ หรือหมวดนโยบาย ตามกรอบนโยบายข้อมูล (Data Policy Framework) ดังรูปที่ 4.4-1



ภาพที่ 4.4-1 กรอบนโยบายข้อมูล (Data Policy Framework)

ก. หมวดทั่วไป (General Domain) เพื่อกำหนดนโยบายทั่วไปที่เกี่ยวข้องกับข้อมูล เช่น โครงสร้างที่เกี่ยวข้อง หน้าที่ความรับผิดชอบ โดยมีรายละเอียด ดังนี้

- กำหนดบทบาทและความรับผิดชอบที่ประกอบกันเป็นโครงสร้างธรรมาภิบาลข้อมูล โดยต้องได้รับการมอบอำนาจและการอนุมัติจากผู้บริหาร
- กำหนดกลุ่มบุคคลหรือบุคคลภายในหน่วยงาน เพื่อเป็นเจ้าของข้อมูลในการบริหารจัดการข้อมูลของหน่วยงาน เพราะหน่วยงานถือเป็นเจ้าของข้อมูลทุกประเภทที่เกิดจากการดำเนินงานภายในหน่วยงานนั้น ๆ
- กำหนดขอบเขตข้อมูลที่นโยบายข้อมูลครอบคลุม เช่น ข้อมูลที่มีโครงสร้าง (ฐานข้อมูล และ CSV) ข้อมูลกึ่งโครงสร้าง (XML และ JSON) ข้อมูลที่ไม่มีโครงสร้าง (เอกสาร เสียงภาพ และภาพเคลื่อนไหว)
- กำหนดนโยบาย มาตรการการรักษาความปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับการอนุญาต
- นำระบบเทคโนโลยีสารสนเทศหรือระบบอัตโนมัติมาใช้ในการจัดทำ Metadata
- ตรวจสอบความสอดคล้องกันระหว่างนโยบายข้อมูลกับการดำเนินการใด ๆ ของผู้มีส่วนได้เสีย อย่างน้อยปีละ 1 ครั้ง

- ทบทวนนโยบายข้อมูล อย่างน้อยปีละ 1 ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่อง หากพบว่านโยบายข้อมูลยังไม่มีประสิทธิภาพเพียงพอ

- สื่อสารและเผยแพร่นโยบายข้อมูลให้กับผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน

- สนับสนุนให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล โดยให้ครอบคลุมทุกกระบวนการของการบริหารจัดการและระบบบริหารและกระบวนการจัดการข้อมูล (วงจรชีวิตของข้อมูล)

ข. หมวดการจัดเก็บข้อมูลและทำลายข้อมูล (Data Storage and Destruction Domain) เพื่อกำหนดนโยบายในการจัดเก็บข้อมูลและทำลายข้อมูลอย่างมีคุณภาพ มีการรักษาความปลอดภัยของข้อมูล โดยมีรายละเอียด ดังนี้

- กำหนดสภาพแวดล้อมของการจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล

- กำหนดชั้นความลับของข้อมูล และจัดเก็บให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Guideline/Standard) ที่กำหนดไว้เพื่อให้ข้อมูลมีความมั่นคงปลอดภัย และรักษาคุณภาพของข้อมูล

- กำหนดสิทธิ์การเข้าถึงข้อมูล และเครื่องมือที่ใช้ในการเข้าถึงข้อมูลจัดเก็บข้อมูลให้สอดคล้องกับความต้องการ และวัตถุประสงค์ในการดำเนินงาน โดยข้อมูลนั้นจะต้องมีความถูกต้องสมบูรณ์ และเป็นปัจจุบันอยู่เสมอ ทั้งนี้ควรจัดทำMetadataสำหรับชุดข้อมูลที่มีการจัดเก็บ

- ในกรณีที่มีการร้องขอให้ทำลายข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล หรือหน่วยงานที่จัดเก็บต้องดำเนินการทำลายให้เร็วที่สุด ทั้งนี้ต้องไม่ขัดต่อข้อตกลงระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล หรือไม่ขัดต่อข้อกฎหมายใด ๆ

- กำหนดแนวทางในการทำลายข้อมูล เมื่อข้อมูลนั้นไม่มีการใช้งานหรือมีการเก็บข้อมูลไว้นานเกินกว่าระยะเวลาที่กำหนด แต่ควรมีการเก็บรักษาMetadataของข้อมูลที่ทำลายไว้เพื่อใช้สำหรับการตรวจสอบภายหลัง

- สร้างความรู้ความเข้าใจในการจัดเก็บและทำลายข้อมูลแก่ผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน

ค. หมวดการประมวลผลข้อมูลและการใช้ข้อมูล (Data Processing and Use Domain) เพื่อกำหนดนโยบายในการประมวลผลข้อมูลและการใช้ข้อมูล ให้ได้ข้อมูลที่มีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ โดยมีรายละเอียดดังนี้

- กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูล และทำการสื่อสารให้แก่ผู้ที่เกี่ยวข้องรับทราบ

- การดำเนินการประมวลผลข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ให้เป็นไปตามขอบเขต เงื่อนไข หรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น

- จัดทำMetadataสำหรับข้อมูลที่จัดเก็บอยู่ในคลังข้อมูล (Data Warehouse)

- ต้องมีการบันทึกประวัติการประมวลผลและการใช้ข้อมูล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

ง. หมวดการแลกเปลี่ยนและการเพื่อกำหนดนโยบายในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานให้มีความมั่นคงปลอดภัยและข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีรายละเอียด ดังนี้เชื่อมโยงข้อมูล (Data Exchange and Integration Domain)

- กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)
- กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลให้ชัดเจนเริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ
- กำหนดMetadataของชุดข้อมูลที่ต้องการแลกเปลี่ยนที่จำเป็นให้ครบถ้วน
- ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้
- กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล
- บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้
- สามารถตรวจสอบได้ว่าการแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติ กระบวนการแลกเปลี่ยน และมาตรฐานตามที่กำหนด

จ. หมวดการเปิดเผยข้อมูล (Data Disclosure Domain) เพื่อกำหนดนโยบายในการเปิดเผยข้อมูล เพื่อให้สามารถเปิดเผยข้อมูลได้อย่างถูกต้องตรงตามวัตถุประสงค์ของการให้นำข้อมูลไปใช้ประโยชน์ โดยมีรายละเอียด ดังนี้

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

(2) มาตรฐานข้อมูล (Data Standards) มาตรฐานข้อมูลอ้างถึงมาตรฐานที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและการใช้ข้อมูล ซึ่งเป็นกลไกอย่างหนึ่งในธรรมาภิบาลข้อมูล มีวัตถุประสงค์เพื่อสร้างความเข้าใจที่ตรงกัน และลดความหลากหลายของวิธีการปฏิบัติ เช่น มาตรฐานMetadata (Metadata Standard) มาตรฐานชุดข้อมูล (Datasets Standard) มาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Standard) โดยมีรายละเอียดในแต่ละมาตรฐาน ดังนี้

ก. มาตรฐานMetadata (Metadata Standard) คือ การกำหนดรูปแบบและข้อกำหนดของMetadata เพื่อให้สามารถเข้าใจได้ถูกต้องตรงกันตลอดทั้งหน่วยงาน ISO/IEC 11179 และ Dublin Core

Metadata Initiative (DCMI) ได้กำหนดมาตรฐานMetadataสำหรับอธิบายชุดข้อมูล เช่น ชื่อข้อมูล ชื่อเจ้าของข้อมูล คำอธิบายข้อมูล ขอบเขตการจัดเก็บ รูปแบบข้อมูล ภาษา สิทธิการเข้าถึง ทั้งนี้ มาตรฐานMetadataมักจะอ้างถึงทั้งMetadataเชิงธุรกิจและMetadataเชิงเทคนิค แต่มักจะไม่รวมองค์ประกอบของฟิลด์ข้อมูล ซึ่งเป็นคุณลักษณะเฉพาะของแต่ละชุดข้อมูล

ข. มาตรฐานชุดข้อมูล (Datasets Standard) คือ การกำหนดรูปแบบและข้อกำหนดของข้อมูลที่มีการใช้ร่วมกันจากหลาย ๆ ส่วนงานหรือหน่วยงาน เพื่อลดความซ้ำซ้อนของข้อมูล ลดความยุ่งยากในการบริหารจัดการ และสนับสนุนให้ข้อมูลมีคุณภาพ ซึ่งส่วนงานหรือหน่วยงานต้องร่วมกันกำหนดMetadataขึ้นมาเพื่ออธิบายคุณลักษณะของชุดข้อมูลที่ใช้ร่วมกัน แล้วดำเนินการบูรณาการข้อมูลที่กระจายอยู่ตามส่วนงาน หรือหน่วยงานต่าง ๆ เข้าด้วยกัน มาตรฐานชุดข้อมูลมักจะอธิบายถึงองค์ประกอบของฟิลด์ข้อมูล เช่น ชื่อฟิลด์ข้อมูล ประเภทข้อมูล (เช่น ตัวเลข ตัวหนังสือ วันที่) ช่วงค่าของข้อมูล และการอนุญาตให้ฟิลด์ข้อมูลเป็นค่าว่าง

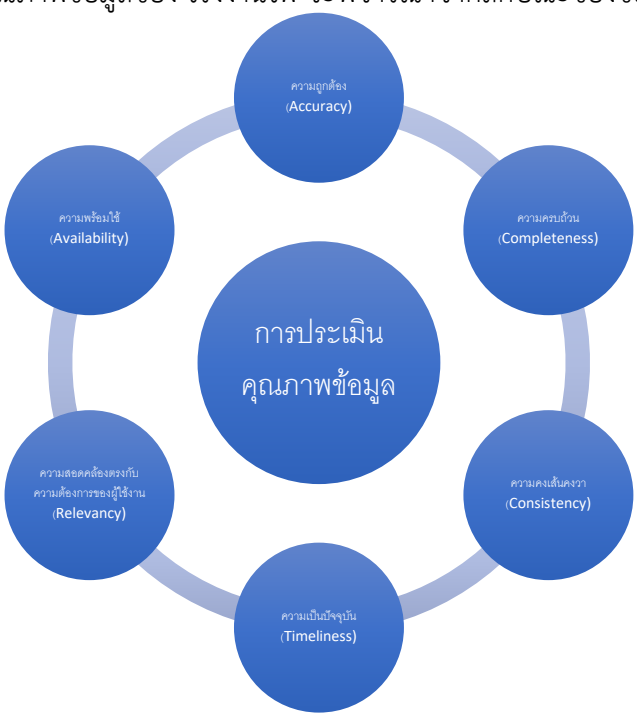
(3) มาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Standard) คือ การกำหนดรูปแบบและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อป้องกันการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ชั้นความลับของข้อมูลมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของประเทศ ตัวอย่างชั้นความลับ ได้แก่ ลับที่สุด ลับมาก ลับ และเปิดเผยได้ ตัวอย่างประเภทของผลกระทบ 1) ด้านชื่อเสียง เช่น ข้อมูลในเชิงลบของหน่วยงานถูกเปิดเผยส่งผลให้หน่วยงานหรือประเทศเสียชื่อเสียง 2) ด้านความต่อเนื่องของการดำเนินการ เช่น ข้อมูลระบบเครือข่ายถูกเปิดเผยทำให้ระบบเครือข่ายหรือระบบอินเทอร์เน็ตถูกโจมตี ซึ่งส่งผลให้การดำเนินงานของหน่วยงานหยุดชะงักหรือล่าช้า 3) ด้านการเงิน เช่น ข้อมูลบัตรเครดิตในหน่วยงานถูกเปิดเผย ทำให้สูญเสียงบประมาณของหน่วยงาน 4) ด้านทรัพยากรบุคคล เช่น ข้อมูลเงินเดือนถูกเปิดเผย ส่งผลให้บุคลากรคนสำคัญต้องลาออก

บทที่ 5
การวัดการดำเนินการและความสำเร็จของธรรมาภิบาล

การวัดความสำเร็จของธรรมาภิบาลข้อมูลเป็นการประเมินผลการดำเนินงานด้านธรรมาภิบาลข้อมูลของโรงงานไพ่ ว่าภายหลังจากที่ได้มีการดำเนินงานในด้านต่าง ๆ เป็นที่เรียบร้อยแล้วนั้น เกิดผลลัพธ์ (Outcome) อย่างไร ทั้งนี้จะช่วยสะท้อนให้เห็นถึงในปัจจุบันว่า โรงงานไพ่ มีความพร้อมในการกำกับดูแลข้อมูลมาก - น้อยเพียงใด มีปัญหา อุปสรรค และข้อจำกัดใดบ้างที่ต้องดำเนินการแก้ไข ดังนั้น การวัดผลการดำเนินงานและความสำเร็จของการกำกับดูแลข้อมูลจึงต้องมีการดำเนินการอย่างต่อเนื่อง เป็นระยะ เพื่อให้หากพบข้อผิดจะได้ดำเนินการแก้ไขได้อย่างทันท่วงที โดยในบทนี้ประกอบด้วยผลการศึกษาในส่วนต่างๆ ได้แก่ การประเมินคุณภาพข้อมูล การประเมินความมั่นคงปลอดภัยของข้อมูล และการวัดความคุ้มทุนและการปรับปรุงอย่างต่อเนื่อง ดังนี้

5.1 การประเมินคุณภาพข้อมูล

หลักการประเมินคุณภาพข้อมูลของ โรงงานไพ่ จะพิจารณาจากลักษณะของข้อมูลต่าง ๆ ดังต่อไปนี้



ภาพที่ 5.1-1 หลักการประเมินคุณภาพข้อมูลของ โรงงานไพ่

5.1.1 ความถูกต้อง (Accuracy) ความถูกต้องของข้อมูลเป็นหนึ่งในคุณสมบัติที่สำคัญในการประเมินคุณภาพของข้อมูล เพราะถึงแม้ว่าหน่วยงานจะดำเนินการเก็บรวบรวมข้อมูลไว้มากเพียงใด แต่หากข้อมูลที่ถูกจัดเก็บต่าง ๆ เหล่านั้นไม่มีความถูกต้อง ย่อมส่งผลต่อการนำไปใช้งานที่ผิดพลาด โดยเฉพาะอย่างยิ่งการตัดสินใจเชิงนโยบาย ที่ต้องอาศัยข้อมูลสำคัญประกอบการพิจารณาตัดสินใจเพื่อการขับเคลื่อนองค์กร ดังนั้น ในกระบวนการบริหารจัดการข้อมูล ขั้นตอนการทำความสะอาดข้อมูล (Data Cleansing) จึงเป็นขั้นตอนที่ใช้เวลามากที่สุด เพื่อให้ข้อมูลที่ได้มีความถูกต้องสมบูรณ์สูงสุด

5.1.2 ความครบถ้วน (Completeness) การพิจารณาตัดสินใจเพื่อดำเนินการใด ๆ ขององค์กรจำเป็นต้องอาศัยข้อมูลที่หลากหลาย เพื่อให้ได้มาซึ่งการตัดสินใจที่ดีที่สุด หรือเกิดประโยชน์ต่อองค์กรอย่างสูงสุด ในหลาย ๆ กิจกรรม หรือการตัดสินใจใดๆ มักมีความสัมพันธ์เกี่ยวข้องกับหลาย ๆ ภาคส่วน เช่น การออกผลิตภัณฑ์ใหม่ของ โรงงานไพ่ ผู้บริหารมีความจำเป็นต้องทราบข้อมูลต่าง ๆ เช่น ความต้องการของผู้บริโภค จุดเด่นของผลิตภัณฑ์เดิมที่มีอยู่ ทรัพยากรในกระบวนการผลิต และผลิตภัณฑ์ของคู่แข่ง เป็นต้น จากตัวอย่างดังกล่าว หากผู้บริหารไม่ทราบความต้องการของผู้บริโภค ก็อาจส่งผลให้ผลิตภัณฑ์ใหม่ที่ออกมานั้น ไม่สอดคล้องกับความต้องการของผู้บริโภคได้ หรือหากไม่ทราบผลิตภัณฑ์ของคู่แข่ง ก็อาจทำให้ผลิตภัณฑ์ที่ออกมานั้นไม่มีความโดดเด่นเหนือคู่แข่งขั้นได้ เป็นต้น

5.1.3 ความคงเส้นคงวา (Consistency) ความคงเส้นคงวา หรือความสอดคล้องกัน หมายถึงการได้รับข้อมูลชุดเดียวกันจากแหล่งข้อมูลต่าง ๆ ที่แตกต่างกันจะต้องมีความเหมือนกัน เพื่อมิให้เกิดความสับสนในการนำไปใช้งาน จนอาจนำไปสู่การนำข้อมูลไปใช้งานที่ผิดพลาดได้ เช่น ข้อมูลปริมาณน้ำนมดิบที่มาจากฝ่ายส่งเสริมกิจการโคนม และฝ่ายนโยบายและยุทธศาสตร์ต้องมีปริมาณที่เท่ากัน เป็นต้น

5.1.4 ความเป็นปัจจุบัน (Timeliness) ในการวิเคราะห์พิจารณาตัดสินใจเพื่อดำเนินการใด ๆ มีความจำเป็นต้องใช้ข้อมูลที่ทันสมัย เพื่อให้ทราบถึงสถานะปัจจุบันที่กำลังเกิดขึ้น อย่างไรก็ตาม ข้อมูลที่ไม่เป็นปัจจุบันก็ยังมีประโยชน์ในการช่วยให้ผู้บริหารทราบถึงแนวโน้ม (Trend) ที่อาจจะเกิดขึ้นในอนาคตได้

5.1.5 ความสอดคล้องตรงกับความต้องการของผู้ใช้งาน (Relevancy) วัตถุประสงค์หลักของการเก็บรวบรวมข้อมูลนั้น เพื่อให้ผู้บริหารและผู้ปฏิบัติงานสามารถนำข้อมูลไปใช้ประโยชน์ในกิจกรรมต่าง ๆ ขององค์กร ดังนั้น การเก็บรวบรวมข้อมูลใด ๆ จึงมีความจำเป็นต้องรับรู้และเข้าใจความต้องการของผู้ใช้งาน เพื่อให้ข้อมูลที่มีอยู่นั้นสามารถนำไปใช้พัฒนาองค์กรได้อย่างแท้จริง อย่างไรก็ตาม ในหลาย ๆ องค์กรมีการเก็บข้อมูลต่าง ๆ อยู่เป็นจำนวนมาก แต่ไม่สามารถนำไปใช้ประโยชน์ได้โดยสาเหตุส่วนหนึ่งเป็นเพราะว่า ขาดเป้าหมายในการเก็บรวบรวมข้อมูลที่ชัดเจน และไม่ทราบความต้องการของผู้ใช้งานที่แท้จริง ส่งผลทำให้สิ้นเปลืองทรัพยากรขององค์กรอย่างไม่เกิดประโยชน์ ดังนั้น ก่อนการเก็บรวบรวมข้อมูล นอกจากจะมีการวางแผนที่ดีแล้ว จะเป็นต้องมีการศึกษาความต้องการในการนำข้อมูลไปใช้งานของส่วนงานต่าง ๆ อย่างเป็นระบบ เพื่อที่จะนำความต้องการที่ได้รับเข้าสู่กระบวนการเก็บรวบรวมข้อมูลต่อไป

5.1.6 ความพร้อมใช้ (Availability)ข้อมูลที่ดีควรมีความพร้อมสำหรับการนำไปใช้งานอยู่เสมอ คือ สามารถดึงข้อมูลไปใช้งานได้ทุกที่ ทุกเวลา ผ่านอุปกรณ์ต่าง ๆ ที่หลากหลาย เพื่ออำนวยความสะดวกให้กับผู้ใช้งาน

5.2 การประเมินความมั่นคงปลอดภัยของข้อมูล

โรงงานไพ่ ได้กำหนดการประเมินความมั่นคงปลอดภัยของข้อมูลโดยมีแนวทางดังต่อไปนี้

5.2.1 กำหนดกรอบในการประเมินความมั่นคงปลอดภัยของข้อมูล

โดยในการประเมินความมั่นคงปลอดภัยของข้อมูลจะต้องอยู่ในกรอบของกฎหมาย และข้อกำหนดของหน่วยงานกำกับดูแล ดังต่อไปนี้

5.2.1.1 กฎหมาย อาทิ

(1) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562

(2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

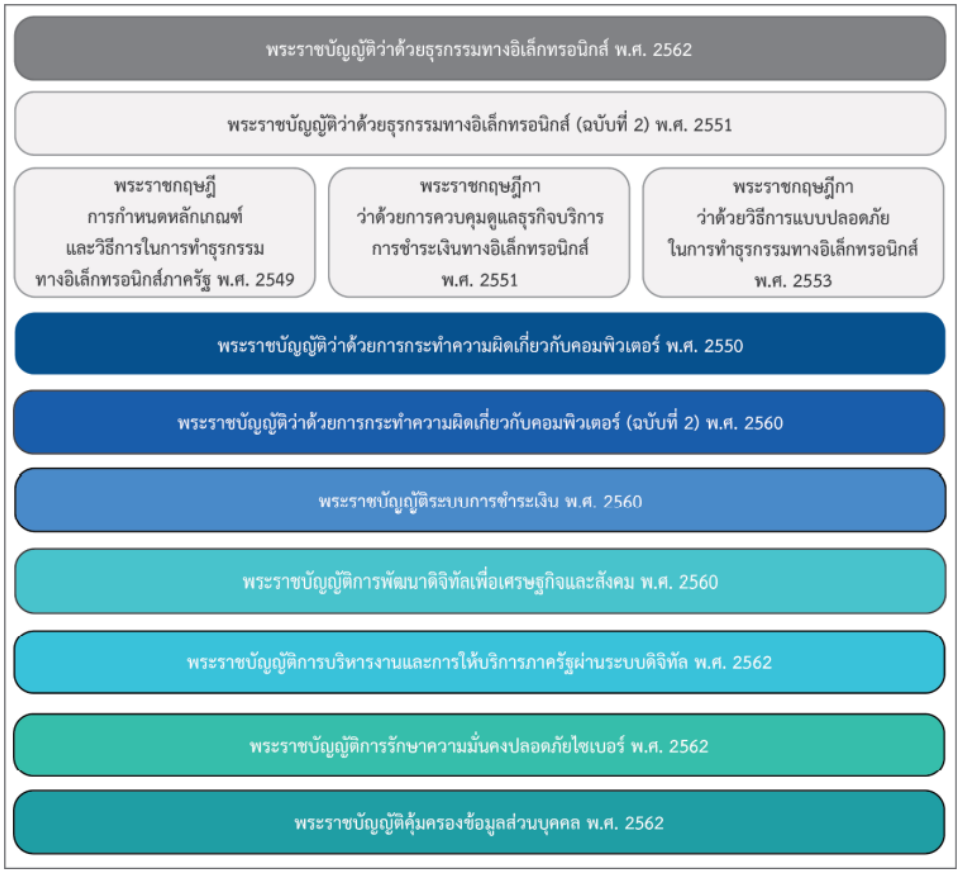
(3) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

(4) พระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560

(5) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

(6) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(7) กฎหมายอื่น ๆ ที่เกี่ยวข้อง



ภาพที่ ๔.๒-๑ ตัวอย่างกฎหมายสำคัญที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

5.2.1.2 ข้อกำหนดของหน่วยงานกำกับดูแล

ข้อกำหนดของหน่วยงานกำกับดูแล ได้แก่ สคร. ได้กำหนดหลักเกณฑ์การบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management) ขององค์กรไว้ดังนี้

(1) การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

(2) การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Data and Information

Security)

(3) การควบคุมการเข้าถึง (Access Control)

(4) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

(5) การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security)

(6) การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)

(7) การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ (System Acquisition and Development)

(8) การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident and Problem Management)

(9) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

(10) การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)

(11) การป้องกันโปรแกรมไม่ประสงค์ดี (Malicious Software Prevention)

(12) การรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเตอร์เน็ท (Website and Internet Security)

(13) การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติ (Endpoint Security)

(14) การบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศ (Cryptography) และการบริหารจัดการกุญแจ (Key management)

5.2.2 จัดทำนโยบายด้านความมั่นคงปลอดภัยของข้อมูลตามมาตรฐาน ISO 27001

ได้แก่ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) โดยแบ่งออกเป็น 2 ส่วน ได้แก่ ดังนี้

ส่วนที่ 1 กรอบนโยบายการบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร

1. นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)
2. โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of Information Security)
3. ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)
4. การบริหารจัดการสินทรัพย์ (Asset Management)
5. การควบคุมการเข้าถึง (Access Control)
6. การเข้ารหัสข้อมูล (Cryptography)
7. ความมั่นคงทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)
8. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)
9. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

10. การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)

11. ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

12. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ(Information Security Incident Management)

13. การบริหารจัดการความมั่นคงปลอดภัยเพื่อสร้างความต่อเนื่องขององค์กร (Information security aspects of business continuity management)

14. ความสอดคล้อง (Compliance)

ส่วนที่ 2 แนวปฏิบัติและกระบวนการบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร

1. แนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย
2. แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ
3. แนวปฏิบัติการควบคุมการเข้าถึงเครือข่าย
4. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
5. แนวปฏิบัติการจัดการการเข้าถึงข้อมูลผู้ใช้
6. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ
7. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพห้องควบคุมระบบ
8. แนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ
9. แนวปฏิบัติการสำรองและการกู้คืนข้อมูล
10. แนวปฏิบัติการดำเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศ
11. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
12. แนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล
13. แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
14. แนวปฏิบัติการควบคุมการเข้าถึงระบบกล้องวงจรปิด
15. ข้อกำหนดการใช้งานเครือข่าย
16. ข้อกำหนดการใช้ไอพีแอดเดรสและชื่อโดเมนของระบบเครือข่ายคอมพิวเตอร์
17. ข้อกำหนดการใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail)
18. แนวปฏิบัติรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ
19. แนวปฏิบัติการป้องกันโปรแกรมไม่ประสงค์ดี (Malicious Software Prevention)
20. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเตอร์เน็ต (Website and Internet Security)
21. แนวปฏิบัติการรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติ (Endpoint Security)
22. แนวปฏิบัติการบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศ (Cryptography) และการบริหารจัดการกุญแจ (Key management)

5.2.3 มีการจัดชั้นความลับของข้อมูล (Data Classification)

ที่สอดคล้องกับระเบียบขององค์กร และมาตรฐานสากล เพื่อป้องกันผลกระทบที่อาจจะเกิดขึ้นจากการนำข้อมูลไปใช้อย่างไม่ถูกต้อง รวมทั้งการดัดแปลง แก้ไข หรือแต่งเติมข้อมูลต่าง ๆ โดยไม่ได้รับอนุญาต โดยโรงงานไพ่ ได้มีการกำหนดชั้นความลับของข้อมูลไว้ดังนี้

5.2.3.1 ข้อมูลส่วนบุคคล

แบ่งระดับชั้นความลับได้เป็น 3 ประเภท ได้แก่

(1) ลับที่สุด (Top secret)

(2) ลับมาก (Secret)

(3) ลับ (Confidential)

5.2.3.2 ข้อมูลทั่วไป

แบ่งระดับชั้นความลับได้เป็น 5 ประเภท ได้แก่

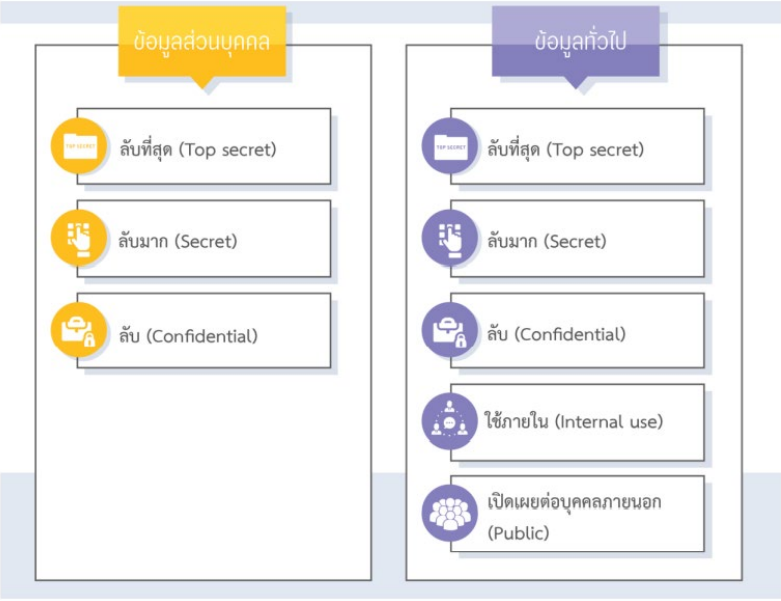
(1) ลับที่สุด (Top secret)

(2) ลับมาก (Secret)

(3) ลับ (Confidential)

(4) ใช้ภายใน (Internal use)

(5) เปิดเผยต่อบุคคลภายนอก (Public)



ภาพที่ 5.2-2 ชั้นความลับข้อมูลของ โรงงานไพ่

5.2.4 กำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูล (Data Protection)

กำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูล (Data Protection) โดยคำนึงถึงการจัดชั้นความลับของข้อมูลเป็นสำคัญ ดังนี้

1) กำหนดประเภทของข้อมูลและสารสนเทศ

2) พิจารณาประเภทของข้อมูลหรือสารสนเทศตามระดับต่าง ๆ ตามที่ได้กำหนด

3) ดำเนินการร้องขอความยินยอมในการจัดเก็บข้อมูลส่วนบุคคลจากเจ้าของข้อมูล

4) กำหนดชั้นความลับของข้อมูลและสารสนเทศตามระดับชั้นของข้อมูลและสารสนเทศ โดยเป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

5) จัดทำป้ายบ่งชี้ระดับชั้นความลับของข้อมูลและสารสนเทศตามประเภทชั้นความลับที่กำหนด

6) เมื่อเจ้าของข้อมูลกำหนดชั้นความลับของข้อมูลและสารสนเทศแล้วให้ผู้ควบคุมเอกสาร (Document Controller) และผู้ใช้งานต้องดำเนินการจัดการข้อมูลและสารสนเทศตามชั้นความลับที่ได้กำหนด ยกเว้นข้อมูลที่เปิดเผยได้ที่ไม่จำเป็นต้องมีการควบคุมการจัดการข้อมูลและสารสนเทศ แต่การเปิดเผยหรือเผยแพร่ข้อมูลและสารสนเทศในระดับชั้นความลับ “ข้อมูลที่เปิดเผยได้” ต้องได้รับการตรวจสอบความถูกต้องของข้อมูลและสารสนเทศ รวมถึงต้องได้รับอนุญาตให้เปิดเผยหรือเผยแพร่จากผู้ที่มีส่วนเกี่ยวข้องก่อน

5.3 การวัดความคุ้มทุนและการปรับปรุงอย่างต่อเนื่อง

ความคุ้มทุนของการดำเนินงานด้านธรรมาภิบาลข้อมูล เป็นการเปรียบเทียบผลประโยชน์ และต้นทุนของการดำเนินงานด้านการกำกับดูแลข้อมูล หากผลประโยชน์ที่ได้รับมีค่าเท่ากับต้นทุนในการดำเนินงานโครงการจะถือเป็นจุดคุ้มทุนทางด้านการเงิน สะท้อนให้เห็นถึงความคุ้มค่าในการลงทุนกับโครงการดังกล่าว ในปัจจุบันมีเครื่องมือที่นำมาช่วยในการวัดความคุ้มทุนหลายรูปแบบ เช่น การวิเคราะห์กำไร-ขาดทุน (Profit-Loss Analysis: PLA) การวิเคราะห์ความคุ้มค่าในการลงทุนและความเสี่ยงโดยใช้วิธี Reference class forecasting และ Monte carlo simulation เป็นต้น อย่างไรก็ตาม โดยส่วนมากเครื่องมือที่นิยมนำมาใช้ในการวัดความคุ้มทุนของหน่วยงานรัฐ คือ การวิเคราะห์ต้นทุนและประโยชน์ของโครงการ (Cost-Benefit Analysis: CBA)หรือ Benefit-Cost Analysis ซึ่งเป็นเครื่องมือในการวิเคราะห์ความคุ้มทุนตามแนวคิดพื้นฐานทางเศรษฐศาสตร์ เป็นการวิเคราะห์โครงการโดยคำนึงถึงต้นทุนและผลประโยชน์จากการดำเนินงานที่ได้รับ โดยวิธีการประเมินต้นทุนและผลประโยชน์ออกมาเป็นมูลค่าของเงิน ซึ่งมีขั้นตอนในการวิเคราะห์ ดังนี้

ภาพที่ 5.3-1 วิธีการวัดความคุ้มทุน

5.3.1 กำหนดกลุ่มอ้างอิง

5.3.2 กำหนดทางเลือกในการดำเนินงานที่เป็นไปได้

5.3.3 กำหนดผลกระทบทางกายภาพที่เกิดขึ้นจากการดำเนินโครงการ ทั้งผลกระทบเชิงบวกและผลกระทบเชิงลบ

5.3.4 ระบุสิ่งที่จะเกิดขึ้น หากไม่ดำเนินงานโครงการดังกล่าว

5.3.5 คาดการณ์ผลกระทบเชิงปริมาณตลอดช่วงอายุโครงการ

5.3.6 แปลงผลกระทบเป็นมูลค่าทางการเงิน

5.3.7 คิดลดต้นทุนและประโยชน์ของโครงการให้เป็นมูลค่าในปัจจุบัน

5.3.8 คำนวณมูลค่าปัจจุบันสุทธิ (Net Present Value: NPV) เป็นการศึกษาผลต่างระหว่างมูลค่าปัจจุบันรวมของกระแสเงินสดตลอดอายุโครงการ เปรียบเทียบกับมูลค่าปัจจุบันของเงินลงทุน โดยใช้อัตราคิดลด (discount rate) ตัวใดตัวหนึ่งมาปรับมูลค่าของกระแสเงินสดที่เกิดขึ้นในแต่ละช่วงเวลาให้มาอยู่ที่จุดเดียวกัน

5.3.9 วิเคราะห์ความอ่อนไหว (Sensitivity analysis) เพื่อศึกษาว่าเมื่อการดำเนินงานโครงการไม่เป็นไปตามเป้าหมายที่กำหนดไว้ โดยอาจมีสาเหตุมาจากปัจจัยต่าง ๆ ที่ส่งผลกระทบต่อโครงการ เช่น รายจ่ายมากขึ้น รายรับลดลง หรือต้องใช้ระยะเวลาในการดำเนินงานมากขึ้น หากดำเนินโครงการดังกล่าวจะยังคงมีความคุ้มค่าที่จะลงทุนต่อหรือไม่

5.3.10 เสนอแนะทางเลือกจากผลการวิเคราะห์ต้นทุน และประโยชน์ของโครงการ อย่างไรก็ตาม ถึงแม้ว่าการวัดความคุ้มทุนของโครงการหรือกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล จะสามารถดำเนินการผ่านวิธีการดังกล่าวข้างต้น โดยใช้หลักการทางสถิติมาช่วยในการวิเคราะห์และประเมินผลความคุ้มค่าใน

การดำเนินงาน แต่ในทางปฏิบัติจริงนั้น โรงงานไพ่ ไม่มีความจำเป็นที่จะต้องประเมินผลการดำเนินงานในทุกโครงการที่กำหนด เพราะจะทำให้สูญเสียทรัพยากรเกินความจำเป็น ทั้งนี้ โรงงานไพ่ อาจใช้วิธีการจัดลำดับความสำคัญของโครงการ เพื่อจำแนกโครงการต่าง ๆ ของเป็นกลุ่มตามลำดับความสำคัญ จากนั้นให้ดำเนินการวิเคราะห์ความคุ้มทุนเฉพาะโครงการที่จัดอยู่ในลำดับที่มีความสำคัญมาก นอกจากนั้นแล้ว การวิเคราะห์ความคุ้มทุนนั้น อาจพิจารณาจากแนวทางอื่นที่มิใช่ตัวเงิน แต่สามารถช่วยสะท้อนผลความคุ้มทุนได้

โดยสรุป การวัดการดำเนินงานและการกำกับดูแลข้อมูลของ โรงงานไพ่ เป็นส่วนหนึ่งของขั้นตอนที่สำคัญในกระบวนการกำกับดูแลข้อมูล เพื่อให้ผู้บริหารและผู้รับผิดชอบส่วนงานที่เกี่ยวข้องทราบถึงผลสะท้อนจากการดำเนินงานในตลอดระยะเวลาที่ผ่านมา สามารถนำผลต่าง ๆ เหล่านั้นมาปรับปรุงประสิทธิภาพในการดำเนินงานให้ดียิ่งขึ้นในอนาคต ทั้งในด้านของบุคลากร (People) กระบวนการ (Process) การบริหารจัดการ (Management) และเทคโนโลยี (Technology) ซึ่งล้วนแต่มีการเปลี่ยนแปลงอยู่เสมอ การวัดหรือการประเมินผลเป็นประจำจึงช่วยให้องค์กรสามารถดำเนินการแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้นได้ทันต่อสถานการณ์ในปัจจุบัน อีกทั้งยังช่วยลดความเสี่ยงจากการดำเนินงานที่ผิดพลาดลงได้

บทที่ 6
การถ่ายทอดกระบวนการ การวิเคราะห์ และการประเมินการรับรู้

6.1 ถ่ายทอดการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management Implementation)

การถ่ายทอดการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management Implementation) มีกระบวนการดำเนินงานดังนี้

6.1.1 กำหนดวัตถุประสงค์ของการถ่ายทอดการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management Implementation)

1) เพื่อสร้างการรับรู้ในกระบวนการการถ่ายทอดการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรให้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้รับทราบ

2) เพื่อสร้างความเข้าใจในกระบวนการการถ่ายทอดการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรให้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง

3) เพื่อนำข้อมูลที่ได้รับ (Feedback) จากผู้มีส่วนได้ส่วนเสียต่าง ๆ มาปรับปรุงและพัฒนากระบวนการการถ่ายทอดการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ให้มีประสิทธิภาพมากยิ่งขึ้น

6.1.2 วิเคราะห์ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management Implementation)

1) กำหนดผู้มีส่วนได้ส่วนเสียที่สำคัญ (Key Stakeholders) ที่เกี่ยวข้องกับกระบวนการการถ่ายทอดการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ผู้มีส่วนได้ส่วนเสียที่สำคัญต่อกระบวนการการถ่ายทอดการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ประกอบด้วย คณะอนุกรรมการ ผู้บริหารและเจ้าหน้าที่ ซึ่งในแต่ละกลุ่มนั้นมีบทบาทหน้าที่ที่ส่งผลกระทบต่อการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร โดยสามารถสรุปได้ ดังนี้

ตารางที่ 6-1 ความรับผิดชอบหลักของผู้มีส่วนได้ส่วนเสียที่สำคัญกับการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร

ผู้มีส่วนได้ส่วนเสียที่สำคัญ (Key Stakeholders)	ความรับผิดชอบหลัก (Key Responsibilities)
1. คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล	ให้คำแนะนำและเสนอแนะการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร
2. ผู้อำนวยการโรงงานไพ่ฯ	▪ กำหนดกรอบ/แนวทางการการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ▪ วิเคราะห์กระบวนการการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ▪ พิจารณาเห็นชอบกระบวนการการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร
3. รองผู้อำนวยการโรงงานไพ่ฯ	▪ กำหนดกรอบ/แนวทางกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ▪ วิเคราะห์กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร
4. หัวหน้าฝ่ายอำนวยการ/ผลิตไพ่/โรงพิมพ์ /หัวหน้าส่วนแผนฯ	▪ กำหนดกรอบ/แนวทางกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ▪ วิเคราะห์กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร
5. ส่วนสารสนเทศและพัฒนาระบบ	▪ ดำเนินการศึกษาทบทวนเอกสารที่เกี่ยวข้อง ▪ ถ่ายทอดกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ▪ ดำเนินการ ติดตาม วิเคราะห์ ประเมินตัววัดผลลัพธ์ ▪ ดำเนินการรายงานผลและทบทวนกระบวนการ

ผู้มีส่วนได้ส่วนเสียที่สำคัญ (Key Stakeholders)	ความรับผิดชอบหลัก (Key Responsibilities)
คณะกรรมการ บริษัท ทริส คอปอเรชั่น จำกัด	▪ ประเมินสถานะการดำเนินงานด้านการพัฒนาเทคโนโลยีดิจิทัลของโรงงานไพ่ฯ ในหัวข้อการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนในองค์กร เพื่อแสดงให้เห็นถึงช่องว่าง (Gap) ในการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ▪ ให้ข้อเสนอแนะหรือคำแนะนำที่ได้รับจากการประเมินผลการออกแบบความเชื่อมโยงและการทำงานร่วมกัน การบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกัน

กำหนดบทบาทหน้าที่ของผู้มีส่วนได้ส่วนเสียที่สำคัญ

ส่วนสารสนเทศและพัฒนาระบบได้กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรในรูปแบบตาราง RACI (RACI Matrix) โดยในแต่ละกระบวนการผู้มีส่วนได้ส่วนเสียหลักจะมีบทบาทหน้าที่ที่เหมือน และแตกต่างกันออกไป ประกอบด้วย ผู้รับผิดชอบงาน (A) ผู้ที่ทำงานนั้น ๆ (R) ผู้ที่มีหน้าที่ให้คำปรึกษา (C) และผู้ที่โรงงานไพ่ฯ จะต้องแจ้งข้อมูลข่าวสารที่เกี่ยวข้องกับการดำเนินงานให้ทราบเป็นระยะ ๆ (I) โดยสามารถสรุปได้ ดังนี้

ตารางที่ 6-2 บทบาทหน้าที่ของผู้มีส่วนได้ส่วนเสียที่สำคัญกับกระบวนการ**ดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร**

Responsible Accountable Consulted Informed

กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	คณะอนุกรรมการด้าน DT	ผู้อำนวยการโรงงานไพ่	รองผู้อำนวยการโรงงานไพ่	หัวหน้าฝ่ายอำนวยการ/ผลิตไพ่/โรงพิมพ์/หัวหน้าส่วนแผนฯ	ส่วนสารสนเทศและพัฒนาระบบ	บริษัททริส
กำหนดเป้าหมาย	C	A	R	R	R	I
ศึกษา ทบทวนเอกสารที่เกี่ยวข้อง	C	C	C	R	A	I
วิเคราะห์ข้อมูล	C	R	R	R	A	I
กำหนดแนวทางดำเนินการด้านการกำกับดูแลข้อมูลฯ	C	A	R	R	R	I
พิจารณาแนวทางการดำเนินการด้านการกำกับดูแลข้อมูลฯ	C	A	R	R	R	I
เผยแพร่ถ่ายทอดแนวทางการดำเนินการด้านการกำกับดูแลข้อมูลฯ	C	C	C	R	A	I
ติดตาม วิเคราะห์ ประเมินตัววัดผลลัพธ์	C	C	C	R	A	I
รายงานผลการดำเนินงานและปรับปรุงกระบวนการ	C	R	C	R	A	I

2) จัดทำกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรใช้วิธีการวิเคราะห์กระบวนการทำงานด้วยแบบจำลอง SIPOC หรือ “SIPOC Model” ประกอบด้วยองค์ประกอบต่าง ๆ ได้แก่ ผู้ที่เกี่ยวข้องกับการจัดทำกระบวนการ (Supplier) ปัจจัยนำเข้า (Input) กระบวนการ (Processes) ผลผลิต (Outputs) และผู้ที่นำผลผลิตไปใช้งาน (Customers) ซึ่งสามารถแสดงให้เห็นโดยภาพรวม ดังนี้

ตารางที่ .6-3 กระบวนการการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร

ชื่อกระบวนการ: กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร			**วันที่จัดทำ/ปรับปรุงกระบวนการ:** 1/8/2566	
ผู้รับผิดชอบ: ส่วนสารสนเทศและพัฒนาระบบ			**จัดทำครั้งที่:** 3	
ผู้ที่เกี่ยวข้องกับการจัดทำกระบวนการ (Supplier)	**ปัจจัยนำเข้า (Input)**	**กระบวนการ (Processes)**	**ผลผลิต (Outputs)**	**ผู้ที่นำผลผลิตไปใช้งาน (Customers)**
S1: ส่วนสารสนเทศและพัฒนาระบบ S2: หัวหน้าฝ่าย/ส่วนงาน S3: ผู้อำนวยการ/รองผู้อำนวยการ	**I1: ปัจจัยภายนอก** - แผนยุทธศาสตร์ชาติ ,แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงดิจิทัล ,แผนการพัฒนาเทคโนโลยีดิจิทัล กระทรวงการคลัง , แผนปฏิบัติการดิจิทัล กรมสรรพสามิต , พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ , พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ , พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล , พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ , พระราชบัญญัติลิขสิทธิ์ , พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และกฎหมายอื่นๆที่เกี่ยวข้อง - เทรน แนวโน้ม ทางด้านเทคโนโลยีดิจิทัล NIST Framework และปัจจัยอื่นๆ ที่เกี่ยวข้อง	**P1: กำหนด** ↓ **P2: ศึกษา ทบทวน** ↓ **P3: วิเคราะห์ข้อมูล** ↓ **P4: กำหนดแนวทาง** ↓ **P5: พิจารณา** ↓ **P6: เผยแพร่** ↓ **P7: ติดตาม** ↓ **P8: รายงานผล**	กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	**C1: ภายในองค์กร** ■ ผู้บริหาร ■ พนักงานโรงงานไพ่ ■ เจ้าหน้าที่สารสนเทศ **C2: ภายนอกองค์กร** ■ สคร. ■ บริษัท ทริสฯ

ผู้ที่เกี่ยวข้องกับการจัดทำกระบวนการ (Supplier)	ปัจจัยนำเข้า (Input)	กระบวนการ (Processes)	ผลผลิต (Outputs)	ผู้ที่นำผลผลิตไปใช้งาน (Customers)
	I2: ปัจจัยภายใน - แผนวิสาหกิจ แผนการบริหารนวัตกรรม แผนด้านการตลาด แผนยุทธศาสตร์องค์กร , แผนบริหารทรัพยากรบุคคล แผนอื่นๆที่เกี่ยวข้อง และ ระเบียบ นโยบาย ที่เกี่ยวข้อง - แบบสัมภาษณ์ และแบบสำรวจผู้บริหาร และพนักงาน **I3: บุคลากร** ประกอบด้วย ■ คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล ■ ผู้อำนวยการ ■ รองผู้อำนวยการ ■ หัวหน้าฝ่าย/ส่วนงาน ■ หัวหน้าส่วนงานแผนงานและกลยุทธ์ **I4: เทคโนโลยี** ได้แก่ ฮาร์ดแวร์และซอฟต์แวร์ของระบบคอมพิวเตอร์ **I5: วัสดุอุปกรณ์** ได้แก่ เครื่องใช้สำนักงาน **I6: เครื่องมือที่ใช้ในการวิเคราะห์** ได้แก่ ■ Data Governance Framework			

6.1.3 การวิเคราะห์ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการ

กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	ผู้ที่เกี่ยวข้องกับกระบวนการ	ผลผลิตที่ได้รับ	ผู้ที่นำผลผลิตไปใช้งาน
1. กำหนดเป้าหมาย	ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 1.1 ผู้อำนวยการโรงงานไพ่ฯ 1.2 รองผู้อำนวยการโรงงานไพ่ฯ 1.3 หัวหน้าฝ่ายอำนวยการ 1.4 หัวหน้าฝ่ายผลิตไพ่ 1.5 หัวหน้าฝ่ายโรงพิมพ์ 1.6 หัวหน้าส่วนแผนงานและกลยุทธ์	เป็นการกำหนดเป้าหมายในสิ่งที่โรงงานไพ่ต้องการเพื่อให้ได้แนวทางการดำเนินงาน	ส่วนสารสนเทศและพัฒนาระบบ
2. ศึกษา ทบทวนเอกสารที่เกี่ยวข้อง	ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 2.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2.2 เจ้าหน้าที่สาสนเทศ	ข้อมูลพื้นฐานที่สามารถนำมาช่วยในกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	ส่วนสารสนเทศและพัฒนาระบบ
3. วิเคราะห์ข้อมูล	ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 3.1 ผู้อำนวยการโรงงานไพ่ฯ 3.2 รองผู้อำนวยการโรงงานไพ่ฯ 3.3 หัวหน้าฝ่ายอำนวยการ 3.4 หัวหน้าฝ่ายผลิตไพ่ 3.5 หัวหน้าฝ่ายโรงพิมพ์ 3.6 หัวหน้าส่วนแผนงานและกลยุทธ์	ผลการวิเคราะห์ข้อมูล ▪ วิเคราะห์บริบทตามที่ได้ศึกษาในกระบวนการที่ 2	ส่วนสารสนเทศและพัฒนาระบบ

กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	ผู้ที่เกี่ยวข้องกับกระบวนการ	ผลผลิตที่ได้รับ	ผู้ที่นำผลผลิตไปใช้งาน
4. กำหนดแนวทางกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 4.1 ผู้อำนวยการโรงงานไพ่ฯ 4.2 รองผู้อำนวยการโรงงานไพ่ฯ 4.3 หัวหน้าฝ่ายอำนวยการ 4.4 หัวหน้าฝ่ายผลิตไพ่ 4.5 หัวหน้าฝ่ายโรงพิมพ์ 4.6 หัวหน้าส่วนแผนงานและกลยุทธ์	กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ประกอบด้วย ■ มีการการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรที่ครอบคลุมถึง กระบวนการกำกับดูแลข้อมูล , โครงสร้างการกำกับดูแลข้อมูล , นโยบายข้อมูลและการตรวจสอบ ,การวัดประสิทธิภาพกระบวนการและคุณภาพข้อมูล และการวัดความคุ้มทุน และการปรับปรุงอย่างต่อเนื่อง ■ มีการกำหนดข้อมูล และสารสนเทศที่สำคัญขององค์กร	ส่วนสารสนเทศและพัฒนาระบบ

กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	ผู้ที่เกี่ยวข้องกับกระบวนการ	ผลผลิตที่ได้รับ	ผู้ที่นำผลผลิตไปใช้งาน
		▪ รัฐวิสาหกิจมีการกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงาน ได้ถูกต้อง แม่นยำ ครบถ้วน เป็นปัจจุบันและใช้งานง่าย	
5. พิจารณาแนวทางกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 5.1 ผู้อำนวยการ 5.2 รองผู้อำนวยการ 5.3 หัวหน้าฝ่ายอำนวยการ 5.4 ส่วนสารสนเทศและพัฒนาระบบ	แนวทางกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรที่ได้รับการพิจารณาเห็นชอบ	ผู้บริหารและพนักงานของโรงงานไพ่ทุกคน
6. เผยแพร่แนวทางกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	6.1 คณะกรรมการและคณะอนุกรรมการประกอบด้วย 6.1.1 คณะกรรมการโรงงานไพ่ 6.1.2 คณะอนุกรรมการด้านดิจิทัล 6.2 ผู้บริหารและพนักงานของโรงงานไพ่ทุกคน	แนวทางกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	ผู้บริหารและพนักงานของโรงงานไพ่ ทุกคน

6.2 ถ่ายทอดกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร

ส่วนสารสนเทศและพัฒนาระบบได้กำหนดวิธีการถ่ายทอดกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรโดยยึดหลักการกระบวนการสื่อสารของ เดวิด เบอร์โล (David K. Berlo) ที่ได้ให้ความสำคัญกับองค์ประกอบในการสื่อสารให้ประสบความสำเร็จ ประกอบด้วย ผู้ส่งสาร (Sender) ข้อมูลข่าวสาร (Message) ช่องทางการสื่อสาร (Channel) และผู้รับสาร (Receiver) หรือที่เรียกว่า “SMCR Model” ซึ่งเป็นแบบจำลองที่ได้รับความนิยม และได้รับการยอมรับจากนักวิชาการทั้งในและต่างประเทศ ทั้งนี้ โรงงานไพ่ฯ ได้ประยุกต์ใช้แบบจำลองการสื่อสารดังกล่าว สำหรับการถ่ายทอดกระบวนกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรดังนี้

6.2.1 ผู้ส่งสาร (Sender)

ผู้ส่งสาร คือ หัวหน้าส่วนสารสนเทศและพัฒนาระบบ ซึ่งเป็นผู้ที่มีบทบาทหน้าที่ในการจัดทำกระบวนกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรโดยภายหลังจากที่ได้ดำเนินการจัดทำข้อมูลเป็นที่เรียบร้อยแล้ว จะต้องจัดส่งให้ผู้อำนวยการพิจารณาเห็นชอบในหลักการและความถูกต้องของเนื้อหาและรายละเอียด ก่อนทำการส่งต่อข้อมูลข่าวสารไปยังบุคลากรในส่วนต่าง ๆ ต่อไป

6.2.2 ข้อมูลข่าวสาร (Message)

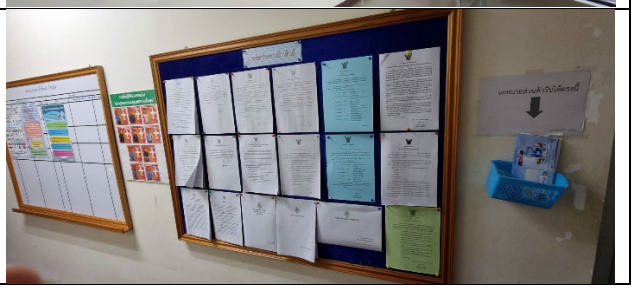
ข้อมูลข่าวสาร ได้แก่ กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรที่ผ่านการพิจารณาจากผู้อำนวยการ โดยได้รับการรับรองความถูกต้องเป็นที่เรียบร้อยแล้ว

6.2.3 ช่องทางการสื่อสาร (Channel)

ช่องทางการสื่อสารข้อมูลของโรงงานไพ่ฯ ใช้ทั้งสื่อดังเดิม (Traditional Media) และสื่อสมัยใหม่ (New Media) ดังนี้

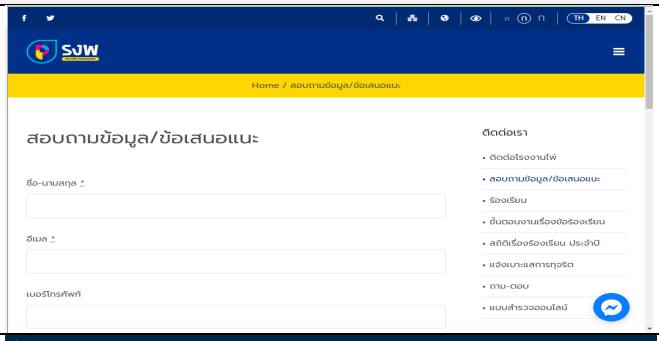
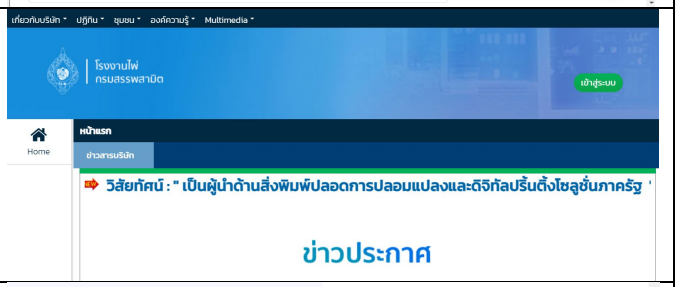
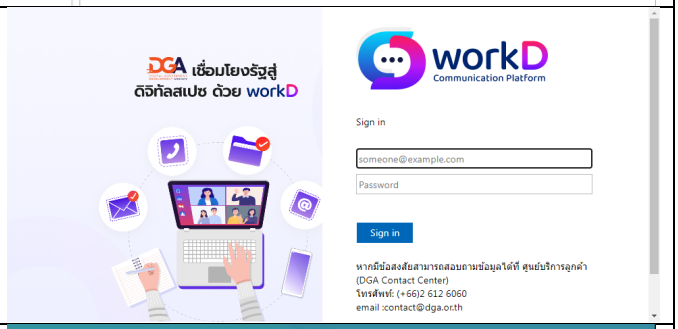
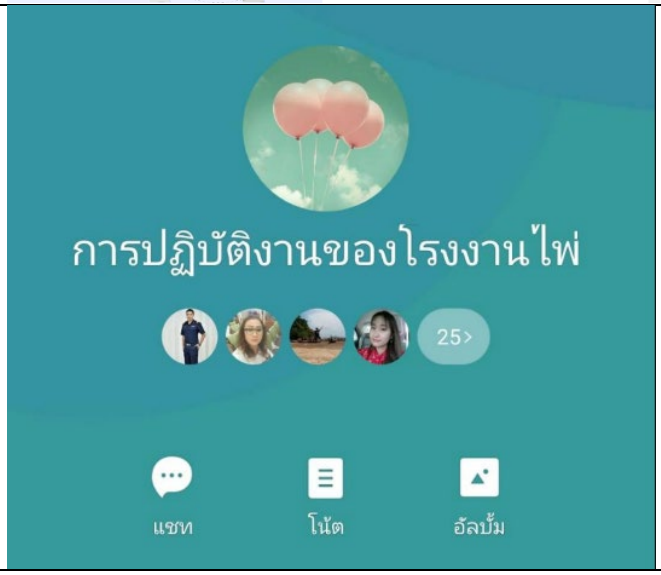
6.2.3.1 สื่อดังเดิม ได้แก่ สื่อสิ่งพิมพ์ โดยทำการสื่อสารผ่าน 2 ช่องทาง ได้แก่ (1) ติดประกาศที่ป้ายประกาศประจำจุดต่าง ๆ ของโรงงานไพ่ ซึ่งมีจำนวนทั้งสิ้น 3 จุด ได้แก่ หน้าทางเข้าโรงงานไพ่ฯ ห้องสันทนาการ และหน้าห้องส่วนบริหารงานกลาง และ (2) สื่อสารผ่านที่ประชุมคณะอนุกรรมการด้านเทคโนโลยีดิจิทัล

ตารางที่ 6-4 ป้ายประกาศตามจุดต่าง ๆ ของโรงงานไพ่ฯ

ตำแหน่ง	ภาพประกอบ
หน้าทางเข้าโรงงานไพ่ฯ	
ห้องสันทนาการ	
หน้าห้องส่วนบริหารงานกลาง	

6.2.3.2 สื่อสมัยใหม่ ประกอบด้วย เว็บไซต์ของโรงงานไพ่ฯ ได้แก่ (https://www.playingcard.or.th/) ระบบอินทราเน็ต (Intranet) โรงงานไพ่ฯ ระบบจดหมายอิเล็กทรอนิกส์ (e-Mail) และแอพลิเคชั่นไลน์ (LINE) โดยในช่องทางดังกล่าว ได้เปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องสามารถให้ความคิดเห็น และข้อเสนอแนะต่าง ๆ ที่เกี่ยวข้องกับกระบวนกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ที่สามารถเข้าถึงได้จากอุปกรณ์การอิเล็กทรอนิกส์ต่าง ๆ ทั้งสมาร์ทโฟน และคอมพิวเตอร์ เพื่อที่จะสามารถนำข้อมูลต่าง ๆ เหล่านั้นมาปรับปรุงและพัฒนากระบวนการฯ ให้มีประสิทธิภาพมากขึ้นต่อไป

ตารางที่ 6-5 ช่องทางการสื่อสารผ่านสื่อสมัยใหม่ ของโรงงานไพ่ฯ

สื่อที่ใช้	ภาพประกอบ
เว็บไซต์ของโรงงานไพ่ฯ (https://www.playingcard.or.th/)	
ระบบอินทราเน็ต (Intranet) โรงงานไพ่ฯ	
ระบบการสื่อสารแบบรวมศูนย์ (workD Platform) - workD Mail ระบบจดหมายอิเล็กทรอนิกส์ (saraban@playingcard.mail.go.th) - workD Chat การส่งข้อความเพื่อสนทนา	
แอพลิเคชั่นไลน์ (LINE)	

6.2.4 ผู้รับสาร (Receiver)

ผู้รับสาร หรือผู้ที่มีความเกี่ยวข้องกับข้อมูลข่าวสารในกระบวนกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรได้แก่ บุคลากรของโรงงานไพ่ฯ ทั้งในระดับผู้บริหาร พนักงาน และผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้อง

6.3 ประเมินการรับรู้จากผู้ที่เกี่ยวข้องกับกระบวนกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร

ในขั้นตอนนี้เป็นกระบวนการประเมินผลการรับรู้จากผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้องกับกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรโดยมีวัตถุประสงค์เพื่อให้มั่นใจได้ว่ากระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรที่ได้จัดทำขึ้นนั้น ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้รับทราบ และเข้าใจถึงกระบวนการทำงานในด้านต่าง ๆ ตามที่กำหนด โดยเฉพาะอย่างยิ่ง ในกิจกรรมที่ตนเองนั้นมีความเกี่ยวข้องโดยตรง เพื่อที่จะได้นำข้อมูลต่าง ๆ ที่ได้รับนั้นมาปรับปรุง แก้ไข และพัฒนากระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรให้มีประสิทธิภาพยิ่งขึ้นต่อไป ตามหลักการบริหารงานเชิงคุณภาพ (PDCA Cycle) โดยสรุปการประเมินผลการรับรู้จากผู้ที่เกี่ยวข้องกับกระบวนกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรจำแนกตามกระบวนการ และผู้ที่เกี่ยวข้องกับกระบวนการกับวิธีการประเมินรูปแบบต่าง ๆ ได้ดังนี้

ตารางที่ 2.6-6 ตัวชี้วัดและการประเมินผลการรับรู้กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร

กระบวนกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	ผู้ที่เกี่ยวข้องกับกระบวนการ	วิธีการประเมินการรับรู้	ตัวชี้วัดการประเมินการรับรู้
1. กำหนดเป้าหมาย	ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 1.1 ผู้อำนวยการโรงงานไพ่ฯ 1.2 รองผู้อำนวยการโรงงานไพ่ฯ 1.3 หัวหน้าฝ่ายอำนวยการ 1.4 หัวหน้าฝ่ายผลิตไพ่ 1.5 หัวหน้าฝ่ายโรงพิมพ์ 1.6 หัวหน้าส่วนแผนงานและกลยุทธ์	ผู้บริหารในระดับต่างๆ ได้เข้ามามีส่วนร่วมกับการกำหนดเป้าหมายของการจัดทำกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรผ่านการประชุม	▪ รายงานการประชุม
2. ศึกษาทบทวนเอกสารที่เกี่ยวข้อง	ส่วนสารสนเทศและพัฒนาระบบ ประกอบด้วย 2.1 หัวหน้าส่วนสารสนเทศและพัฒนาระบบ 2.2 เจ้าหน้าที่สารสนเทศ	หัวหน้าส่วนสารสนเทศและพัฒนาระบบเจ้าหน้าที่สารสนเทศ และเจ้าหน้าที่สารสนเทศได้ประชุมร่วมกันเพื่อพิจารณาทบทวนเอกสารต่าง ๆ ที่เกี่ยวข้อง	▪ ผลการศึกษาทบทวนเอกสารที่เกี่ยวข้อง
3. วิเคราะห์ข้อมูล	ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 3.1 ผู้อำนวยการโรงงานไพ่ฯ 3.2 รองผู้อำนวยการโรงงานไพ่ฯ 3.3 หัวหน้าฝ่ายอำนวยการ 3.4 หัวหน้าฝ่ายผลิตไพ่ 3.5 หัวหน้าฝ่ายโรงพิมพ์	ทำหนังสือเวียนถึงผู้บริหารเพื่อพิจารณาผลการวิเคราะห์ข้อมูล	▪ รายงานผลการวิเคราะห์ข้อมูล ▪ เอกสารสรุปรายงานประชุม ▪ หนังสือเวียน

กระบวนกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	ผู้ที่เกี่ยวข้องกับกระบวนการ	วิธีการประเมินการรับรู้	ตัวชี้วัดการประเมินการรับรู้
	3.6 หัวหน้าส่วนแผนงานและกลยุทธ์		
4. กำหนดแนวทางกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 4.1 ผู้อำนวยการโรงงานไพ่ฯ 4.2 รองผู้อำนวยการโรงงานไพ่ฯ 4.3 หัวหน้าฝ่ายอำนวยการ 4.4 หัวหน้าฝ่ายผลิตไพ่ 4.5 หัวหน้าฝ่ายโรงพิมพ์ 4.6 หัวหน้าส่วนแผนงานและกลยุทธ์	ผู้มีส่วนเกี่ยวข้องร่วมกันเพื่อกำหนดแนวทางกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	▪ มีแนวกระบวนการออกแบบความเชื่อมโยงและการทำงานร่วมกันการบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกัน ▪ เอกสารสรุปรายงานประชุม ▪ หนังสือเวียน
5. พิจารณากระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	ผู้บริหารโรงงานไพ่ฯ ประกอบด้วย 5.1 ผู้อำนวยการ 6.2 รองผู้อำนวยการ 5.3 หัวหน้าฝ่ายอำนวยการ 5.4 ส่วนสารสนเทศและพัฒนาระบบ	ทำบันทึกข้อความถึงผู้อำนวยการ เพื่อพิจารณาเห็นชอบผลการทบทวนกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	▪ กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ▪ บันทึกข้อความ
7 เผยแพร่กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	6.1 คณะกรรมการและคณะอนุกรรมการประกอบด้วย 6.1.2 คณะกรรมการโรงงานไพ่ 6.1.2 คณะอนุกรรมการด้านดิจิทัล 6.2 ผู้บริหารและพนักงานของโรงงานไพ่ทุกคน	▪ นำกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	▪ รายงานการประชุม ▪ กระบวนการการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหาร

กระบวนกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	ผู้ที่เกี่ยวข้องกับกระบวนการ	วิธีการประเมินการรับรู้	ตัวชี้วัดการประเมินการรับรู้
		เข้าสู่คณะอนุกรรมการด้านเทคโนโลยีดิจิทัลเพื่อทราบ	จัดการข้อมูลขนาดใหญ่ขององค์กร

สรุป โรงงานไพ่ฯ ได้กำหนดวิธีการประเมินผลการรับรู้กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ด้วยรูปแบบที่แตกต่างกัน จำแนกตามผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการต่าง ๆ ซึ่งได้ผ่านการวิเคราะห์ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการมาเป็นที่เรียบร้อยแล้ว ทั้งนี้เพราะผู้มีส่วนได้ส่วนเสียต่าง ๆ เหล่านั้น ล้วนเป็นส่วนหนึ่งของการกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ให้ดียิ่งขึ้น ดังนั้น การกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรในครั้งนี้ จึงเปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้เข้ามามีส่วนร่วมในการแสดงความคิดเห็น และให้ข้อเสนอแนะสำหรับการปรับปรุงกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ซึ่งสอดคล้องกับหลักการบริหารงานเชิงคุณภาพ (PDCA Cycle) โดยโรงงานไพ่ฯ ได้กำหนดให้การประเมินการรับรู้ดำเนินการควบคู่กับการจัดทำกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรประจำทุกปี เพื่อให้กระบวนการมีแนวทางปฏิบัติอย่างเป็นระบบ สามารถทำซ้ำได้ (Repeatable Practice) และเป็นมาตรฐาน (Standardized Practice)

บทที่ 7
การวัดผล ติดตาม และประเมินผล

กำหนดตัววัด ติดตาม วิเคราะห์ ประเมินตัววัดผลลัพธ์ (Outcome) ของกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร

กำหนดตัววัด ติดตาม วิเคราะห์ ประเมินตัววัดผลลัพธ์ (Outcome) ของกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร มีวัตถุประสงค์เพื่อประเมินผลกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ที่ได้พัฒนาขึ้นว่ามีลักษณะอย่างไร มีความสอดคล้องกับหลักเกณฑ์ที่กำหนด และมีความเหมาะสมกับบริบทขององค์กรหรือไม่ เพื่อให้มั่นใจได้ว่ากระบวนการที่พัฒนาขึ้นนั้นเป็นไปอย่างมีประสิทธิภาพ โดยโรงงานไพ่ฯ ได้กำหนดตัววัด ติดตาม วิเคราะห์ ประเมินตัววัดผลลัพธ์ (Outcome) ของกระบวนการการจัดการด้านคุณภาพดังนี้

ตารางที่ 2.7-1 การกำหนดตัววัด ติดตาม วิเคราะห์ ประเมินตัววัดผลลัพธ์ (Outcome) ของกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร

ตัววัดผลลัพธ์ (Outcome) ของกระบวนการฯ	วิธีการประเมิน
5.1.1.1 กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร เป็นไปตามหลักเกณฑ์การประเมินผลการดำเนินงานรัฐวิสาหกิจตามระบบประเมินผลใหม่ (SE-AM) ตามที่ สคร. กำหนด	ผลการเปรียบเทียบการกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร กับหลักเกณฑ์ของ สคร. หัวข้อการจัดการด้านคุณภาพ
5.1.1.2 กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร มีการบริหารจัดการที่ดีขึ้น	ผลการประเมินหัวข้อการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร มีระดับที่สูงขึ้นเมื่อเทียบกับปีที่ผ่านมา
5.1.1.3 กระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร มีการทบทวนอยู่เสมอ	โรงงานไพ่ฯ มีการทบทวนกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร อย่างน้อยปีละ 1 ครั้ง
5.1.1.4 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องมีการรับรู้ถึงกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร	โรงงานไพ่ฯ มีวิธีการและช่องทางการสื่อสารเพื่อให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องมีการรับรู้ถึงกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร พร้อมทั้งกำหนดและประเมินผลการรับรู้ภายหลังจากที่ทำการสื่อสาร
5.1.1.5 กระบวนการออกแบบความเชื่อมโยงและการทำงานร่วมกัน การบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันได้เปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้เข้ามามีส่วนร่วมในการ	โรงงานไพ่ฯ ได้มีการนำผลที่ได้รับจากผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง เช่น ผลการประเมินการรับรู้ ผลการสำรวจความคิดเห็นของผู้บริหาร หรือผลการแสดงความคิดเห็นของผู้มีส่วนได้ส่วนเสียจากช่องทางการ

ตัววัดผลลัพธ์ (Outcome) ของกระบวนการฯ	วิธีการประเมิน
ปรับปรุงและพัฒนากระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร จนนำไปสู่กระบวนการที่มีแนวทางการปฏิบัติอย่างเป็นระบบ	สื่อสารต่าง ๆ เข้าสู่ที่ประชุมคณะกรรมการฯ เพื่อดำเนินการปรับปรุงกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ให้มีแนวทางการปฏิบัติอย่างเป็นระบบ สามารถทำซ้ำได้ และเป็นมาตรฐานอย่างเหมาะสมของโรงงานไพ่ฯ

ภายหลังจากที่ได้ทำการกำหนดตัววัดผลลัพธ์ และได้ดำเนินการวัดผลลัพธ์ของกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร เป็นที่เรียบร้อยแล้ว โรงงานไพ่ฯ จะดำเนินการนำผลลัพธ์ดังกล่าวเข้าสู่ที่คณะอนุกรรมการฯ เพื่อชี้แจงรายละเอียดของผลที่ได้รับจากกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ให้ผู้บริหารและผู้มีส่วนได้ส่วนเสียได้รับทราบ รวมทั้งนำผลที่ได้เข้าสู่กระบวนการทบทวนเพื่อปรับปรุงกระบวนการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ของโรงงานไพ่ต่อไป โดยกระบวนการดังกล่าวจะสอดคล้องกับการประเมินกระบวนการในรูปแบบระดับวุฒิภาวะตามที่ สคร. กำหนด และสอดคล้องกับหลักการบริหารงานเชิงคุณภาพ PDCA Cycle ที่กำหนดให้ต้องมีการตรวจสอบและปรับปรุงกระบวนการอย่างต่อเนื่อง จะนำไปสู่แนวทางการปฏิบัติอย่างเป็นระบบ สามารถทำซ้ำได้ และเป็นมาตรฐานต่อไป

เอกสารอ้างอิง

“ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. ๒๕๖๓” (๒๕๖๓, ๓๑ มีนาคม). ราชกิจานุเบกษา. เล่ม ๑๓๗ ตอนพิเศษ ๗๔ ง. หน้า ๔๗-๔๘.
“พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐” (๒๕๕๐, ๑๘ มิถุนายน). ราชกิจานุเบกษา. เล่ม ๑๒๔ ตอนที่ ๒๗ ก. หน้า ๔-๑๓.
“พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒” (๒๕๖๒, ๒๗ พฤษภาคม). ราชกิจานุเบกษา. เล่ม ๑๓๖ ตอนที่ ๖๙ ก. หน้า ๕๒-๙๕.
“พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒” (๒๕๖๒, ๒๗ พฤษภาคม). ราชกิจานุเบกษา. เล่ม ๑๓๖ ตอนที่ ๖๙ ก. หน้า ๒๐-๕๑.
“พระราชบัญญัติระบบการชำระเงิน พ.ศ. ๒๕๖๐” (๒๕๖๐, ๑๘ ตุลาคม). ราชกิจานุเบกษา. เล่ม ๑๓๔ ตอนที่ ๑๑๐ ก. หน้า ๑-๑๖.
“พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. ๒๕๖๒” (๒๕๖๒, ๒๒ พฤษภาคม). ราชกิจานุเบกษา. เล่ม ๑๓๖ ตอนที่ ๖๗ ก. หน้า ๒๐๓-๒๐๗.
“พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐” (๒๕๔๐, ๒ กันยายน). ราชกิจานุเบกษา.
Askham, N. (๒๐๑๖). Squaring the circle: Using a data governance framework to support data quality. Experian Information Solutions, Inc.
Thomas, G. (๒๐๐๙). How to use the DGI data governance framework to configure your program. Data Governance Institute, ๑๗.
Intra-governmental Group on Geographic Information (IGGI). (๒๐๐๕). The Principles of Good Data Management. The Office of the Deputy Prime Minister.
Henderson, D., Earley, S., Sebastian-Coleman, L., Sykora, E., & Smith, E. (๒๐๑๗). DAMA guide to the data management body of knowledge. Second Edition. Technics Publications.