AIGPC
AI GOVERNANCE
PRACTICE CENTER

AI GOVERNANCE GUIDELINE for EXECUTIVES

แนวทางการประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีธรรมาภิบาล
สำหรับผู้บริหารองค์กร

ฉบับปรับปรุง 2569



ETDA


AI
GOVERNANCE
GUIDELINE for EXECUTIVES

สารบัญ

01

บทสรุปผู้บริหาร — **4**

02

ที่มา — **8**

03

ขอบเขตและข้อจำกัด — **10**

04

บทนำ — **12**

4.1 ทำไมจึงต้องมีธรรมาภิบาลในการประยุกต์ใช้ AI 13
4.2 ธรรมาภิบาลในการประยุกต์ใช้ AI คืออะไร 14
4.3 หลักการจริยธรรมปัญญาประดิษฐ์ 16
4.4 กรอบการทำงานเพื่อสนับสนุนธรรมาภิบาลในการประยุกต์ใช้ AI 18
4.5 คำนิยาม 20

05

การกำหนดโครงสร้างการกำกับดูแล (AI Governance Structure) — **22**

5.1 คณะกรรมการกำกับดูแลการประยุกต์ใช้ AI (AI Governance Council) 23
5.2 หน้าที่และความรับผิดชอบ (Role and Responsibility) 28
5.3 การพัฒนาศักยภาพบุคลากร (Competency Building) 32

06

การกำหนดกลยุทธ์ในการประยุกต์ใช้ AI (AI Strategy) 34

6.1 การกำหนดกลยุทธ์ในการประยุกต์ใช้ AI อย่างมีความรับผิดชอบ (Responsible AI Strategy) 35
6.2 การบริหารจัดการความเสี่ยงจากการประยุกต์ใช้ AI (AI Risk Management) 40

07

การกำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับ AI (AI Operation) 48

7.1 การกำกับดูแลตลอดวงจรชีวิตของ AI (AI Lifecycle) 49
7.2 การให้บริการ AI (AI Service) 65

08

ภาคผนวก 68

ภาคผนวก ก 69
ภาคผนวก ข 70
เอกสารอ้างอิง 71



01
บทสรุปผู้บริหาร

เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence หรือ AI) เข้ามามีบทบาทในชีวิตประจำวันของมนุษย์มากขึ้น จึงทำให้ทั่วโลกเกิดความกังวลถึงผลกระทบที่อาจเกิดขึ้นกับมนุษย์ในด้านต่าง ๆ อาทิ ด้านจริยธรรม ด้านความเป็นธรรม ด้านความเป็นส่วนตัว และด้านความปลอดภัย รวมถึงความรับผิดชอบจากผลกระทบอันเกิดจากการนำ AI มาช่วยเหลือหรือตัดสินใจแทนมนุษย์ เป็นต้น

ด้วยเหตุนี้ ธรรมาภิบาลในการประยุกต์ใช้ปัญญาประดิษฐ์ (AI Governance) หรือหลักการในการกำกับดูแลการประยุกต์ใช้ AI ที่ดีนั้น จึงเป็นเรื่องสำคัญที่องค์กรจำเป็นต้องดำเนินการตามบริบทขององค์กรอย่างเหมาะสม เพื่อให้การประยุกต์ใช้ AI สามารถบรรลุตามเป้าหมายที่องค์กรกำหนดและมีความรับผิดชอบต่อบุคคลที่เกี่ยวข้อง องค์กร และสังคมโดยกว้าง (Responsible Use of AI) โดยคำนึงถึงหลักการจริยธรรมปัญญาประดิษฐ์ (AI Ethics Principles) ความสอดคล้องตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง (Laws and Regulations) รวมถึงการควบคุมความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประยุกต์ใช้ AI

เอกสาร **“แนวทางการประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีธรรมาภิบาล สำหรับผู้บริหารองค์กร (AI Governance Guideline for Executives)”** นี้ มีวัตถุประสงค์เพื่อนำเสนอ **แนวปฏิบัติสำหรับการกำกับดูแลการประยุกต์ใช้ AI ในมุมมองของผู้บริหารองค์กร พร้อมทั้งนำเสนอตัวอย่างแนวปฏิบัติทั้งจากภายในและต่างประเทศ รวมถึงแนวปฏิบัติตามมาตรฐานสากล เพื่อเป็นแนวทางให้การประยุกต์ใช้ AI ในองค์กรสามารถบรรลุตามเป้าหมายที่กำหนดอย่างมีความรับผิดชอบ ซึ่งจะนำไปสู่ความเชื่อมั่นและการยอมรับจากผู้ที่เกี่ยวข้องในทุกภาคส่วน**

โดยเอกสารนี้ได้นำเสนอแนวทางในการกำกับดูแล ซึ่งประกอบด้วย 3 องค์ประกอบหลัก ได้แก่ การกำหนดโครงสร้างการกำกับดูแล (AI Governance Structure) การกำหนดกลยุทธ์ในการประยุกต์ใช้ AI (AI Strategy) และการกำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับ AI (AI Operation)

AI Governance มีเป้าหมายเพื่อให้การประยุกต์ใช้ AI บรรลุตามเป้าหมายขององค์กร อย่างมีความรับผิดชอบต่อบุคคลที่เกี่ยวข้อง องค์กร และสังคมโดยกว้าง



1. การกำหนดโครงสร้างการกำกับดูแล (AI Governance Structure) เป็นการนำเสนอแนวทางการกำหนดโครงสร้างการกำกับดูแลการประยุกต์ใช้ AI ขององค์กร โดยมีคณะกรรมการกำกับดูแลการประยุกต์ใช้ AI (AI Governance Council) ซึ่งมีหน้าที่ในการกำหนดกลยุทธ์และนโยบายที่เกี่ยวข้องเพื่อขับเคลื่อนการประยุกต์ใช้ AI ภายในองค์กร รวมถึงมีหน้าที่ในการเฝ้าติดตาม และประเมินผลการประยุกต์ใช้ AI อย่างต่อเนื่อง เพื่อให้มั่นใจได้ว่าองค์กรมีการกำกับดูแลการประยุกต์ใช้ AI อย่างเหมาะสม นอกจากการกำหนดคณะกรรมการเพื่อกำกับดูแลโดยภาพรวมแล้ว องค์กรยังจำเป็นต้องกำหนดหน้าที่และความรับผิดชอบ (Role and Responsibility) ของบุคลากรและผู้มีส่วนได้เสียที่เกี่ยวข้อง (Stakeholders) ตามโครงสร้างการกำกับดูแล พร้อมทั้งสนับสนุนทรัพยากรที่จำเป็น ส่งเสริมทักษะความรู้ รวมถึงสร้างความตระหนักรู้ (Awareness) ต่อความรับผิดชอบ (Responsibility) และความรับผิดชอบต่อผลของการกระทำ (Accountability) ของแต่ละหน้าที่อีกด้วย

2. การกำหนดกลยุทธ์ในการประยุกต์ใช้ AI (AI Strategy) เป็นการมองหาโอกาสหรือประโยชน์ที่องค์กรจะได้รับจากการนำ AI มาประยุกต์ใช้ที่ตอบสนองเป้าหมายขององค์กร พร้อมทั้งวิเคราะห์เป้าหมายความสำเร็จจากการนำ AI มาประยุกต์ใช้ ความเป็นไปได้ในการดำเนินการ ความพร้อมขององค์กร และทรัพยากรที่จำเป็น เพื่อให้มั่นใจได้ว่าการประยุกต์ใช้ AI จะบรรลุตามเป้าหมายและประสบความสำเร็จตามที่กำหนด นอกจากนี้ ในการกำหนดกลยุทธ์ยังจำเป็นต้องวิเคราะห์ถึงความเสี่ยงและผลกระทบจากการนำ AI มาประยุกต์ใช้ควบคู่ไปกับความสอดคล้องกับหลักการจริยธรรมปัญญาประดิษฐ์ และความสอดคล้องตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง เพื่อแสดงให้เห็นถึงความมุ่งมั่นขององค์กรที่จะประยุกต์ใช้ AI อย่างมีความรับผิดชอบต่อบุคคลที่เกี่ยวข้อง องค์กร และสังคมโดยกว้าง (Responsible use of AI)



3. การกำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับ AI (AI Operation) เป็นการอธิบายถึงแนวปฏิบัติตลอดวงจรชีวิตของ AI (AI Lifecycle) เพื่อให้มั่นใจได้ว่า AI ได้รับการออกแบบ พัฒนา และนำไปใช้งานได้อย่างสอดคล้องตามเป้าหมายขององค์กร รวมถึงสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้อง นอกจากนี้ ยังอธิบายถึงแนวปฏิบัติในการจัดเตรียมข้อมูล (Data Preparation) เพื่อให้ได้ข้อมูลที่มีคุณภาพและเหมาะสำหรับนำไปใช้สอนและทำงานร่วมกับ AI รวมถึงแนวปฏิบัติการรับมือกับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น การเฝ้าติดตามและการประเมินผลการประยุกต์ใช้งาน AI เพื่อปรับปรุงการดำเนินงานให้มีประสิทธิภาพต่อไปในอนาคต

จากแนวทางในการกำกับดูแลทั้ง 3 องค์ประกอบหลักข้างต้น เป็นการนำเสนอแนวทางการกำกับดูแลการประยุกต์ใช้เทคโนโลยี AI อย่างมีธรรมาภิบาล **โดยมีคณะกรรมการกำกับดูแลการประยุกต์ใช้ AI ซึ่งมีหน้าที่หลักในการกำกับดูแลในภาพรวม ตั้งแต่การกำหนดกลยุทธ์และนโยบาย การควบคุมความเสี่ยงและผลกระทบที่อาจเกิดขึ้น ไปจนถึงการกำกับดูแลการปฏิบัติงานตลอดวงจรชีวิตของ AI พร้อมทั้ง กำหนดหน้าที่และความรับผิดชอบของบุคลากรและผู้มีส่วนได้เสียที่เกี่ยวข้องอย่างชัดเจน** เพื่อให้มั่นใจว่าการประยุกต์ใช้ AI ขององค์กร จะบรรลุตามเป้าหมายที่กำหนดและมีความรับผิดชอบต่อบุคคลที่เกี่ยวข้อง องค์กรและสังคมโดยกว้าง ซึ่งจะทำให้เกิดความเชื่อมั่นและได้รับการยอมรับจากทุกภาคส่วน



02
ที่มา

ในยุคโลกาภิวัตน์ที่ปัญญาประดิษฐ์ได้เข้ามามีบทบาทสนับสนุนและอำนวยความสะดวกกับมนุษย์มากขึ้น **สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จึงได้มีการจัดทำเอกสารหลักการแนวทางจริยธรรมปัญญาประดิษฐ์ (Thailand AI Ethics Guideline)** และนำเสนอต่อคณะรัฐมนตรีให้ความเห็นชอบ เมื่อวันที่ 2 กุมภาพันธ์ พ.ศ. 2564 เพื่อให้หน่วยงานราชการใช้เป็นแนวทางปฏิบัติในการพัฒนา ส่งเสริม และนำไปใช้ในทางที่ถูกต้องและมีจริยธรรม รวมทั้งเพื่อสนับสนุนการดำเนินการตามยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 – 2580) ยุทธศาสตร์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2563 – 2567) และแผนปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติเพื่อการพัฒนาประเทศ (พ.ศ. 2565 - 2570)

โดยเอกสารดังกล่าวได้**มีการกำหนดหลักการจริยธรรมปัญญาประดิษฐ์ (AI Ethics Principles) ไว้ 6 หลักการ (ดังรายละเอียดในหัวข้อ 4.3) ซึ่งเป็นหลักการจริยธรรมพื้นฐานที่สอดคล้องกับหลักการจริยธรรมปัญญาประดิษฐ์ที่ได้รับการยอมรับจากองค์กรที่มีชื่อเสียงด้านเทคโนโลยีในหลายประเทศ** เพื่อเป็นหลักการพื้นฐานที่จะนำไปสู่การพัฒนาและส่งเสริมให้เกิดธรรมาภิบาลในการประยุกต์ใช้ AI ภายในประเทศ

ต่อมา สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ในฐานะหน่วยงานของรัฐซึ่งมีภารกิจในการส่งเสริมและสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือและมั่นคงปลอดภัย ได้เล็งเห็นว่าเทคโนโลยี AI มีพัฒนาการแบบก้าวกระโดดและมีผลกระทบโดยตรงกับการทำธุรกรรมอิเล็กทรอนิกส์ในปัจจุบัน จึง**ควรส่งเสริมและสนับสนุนให้ผู้ประกอบธุรกิจบริการภายใต้กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ทั้งภาครัฐและเอกชน นำหลักการจริยธรรมปัญญาประดิษฐ์ (AI Ethics Principles) ไปปรับใช้เพื่อให้เกิดธรรมาภิบาลในการประยุกต์ใช้ AI**

ด้วยเหตุนี้ สพธอ. จึงได้จัดทำเอกสาร “แนวทางการประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีธรรมาภิบาล สำหรับผู้บริหารองค์กร (AI Governance Guideline for Executives)” **เพื่อนำเสนอภาพรวมของการกำกับดูแลการประยุกต์ใช้ AI ในมุมมองของผู้บริหารองค์กร พร้อมทั้ง นำเสนอตัวอย่างแนวปฏิบัติทั้งจากภายในและต่างประเทศ รวมถึงแนวปฏิบัติตามมาตรฐานสากล เพื่อเป็นแนวปฏิบัติให้แก่ผู้ประกอบธุรกิจบริการทั้งภาครัฐและเอกชนนำไปปรับใช้และกำกับดูแลการประยุกต์ใช้ AI** ต่อไป



03

ขอบเขต และข้อจำกัด

สพธอ. จัดทำเอกสารนี้โดยมีวัตถุประสงค์เพื่อนำเสนอแนวทางการกำกับดูแลการประยุกต์ใช้ AI ในภาพรวม **โดยไม่มีการระบุเฉพาะเจาะจงประเภทของเทคโนโลยีและประเภทขององค์กรที่นำแนวปฏิบัติไปปรับใช้** ด้วยเหตุนี้ ในการนำแนวปฏิบัติหรือข้อเสนอแนะในเอกสารนี้ไปปรับใช้ จึงอาจไม่เหมาะสมกับบางบริบทของการประยุกต์ใช้ AI ดังนั้น องค์กรจึงควรพิจารณาถึงความเหมาะสมกับบริบทของการนำ AI ไปประยุกต์ใช้ เทคโนโลยีที่ใช้ การเปลี่ยนแปลงของเทคโนโลยีในอนาคต ความสอดคล้องตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง รวมถึงความเสี่ยงที่เกี่ยวข้องกับบริบทของการนำ AI ไปประยุกต์ใช้ เช่น ภัยคุกคามทางไซเบอร์ ความเสี่ยงในด้านอาชีวอนามัยและความปลอดภัย เป็นต้น

แนวปฏิบัติหรือข้อเสนอแนะในเอกสารนี้เป็นเพียงการนำเสนอผลการศึกษาตัวอย่างแนวปฏิบัติทั้งจากภายในและต่างประเทศ รวมถึงแนวปฏิบัติตามมาตรฐานสากล เพื่อส่งเสริมและสนับสนุนให้องค์กรทั้งภาครัฐและเอกชนสามารถประยุกต์ใช้ AI ได้อย่างมีธรรมาภิบาล ดังนั้น **การไม่ปฏิบัติตามแนวปฏิบัติหรือข้อเสนอแนะนี้ จึงไม่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้องกับปัญญาประดิษฐ์ของประเทศไทย**

นอกจากนี้ เอกสารฉบับนี้ไม่ใช่เกณฑ์มาตรฐานเพื่อการขอรับรองระบบ หากองค์กรมีความประสงค์ที่จะได้รับการตรวจประเมินและรับรองมาตรฐานจะต้องดำเนินการตามมาตรฐาน **ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system** ซึ่งเป็นมาตรฐานระบบการจัดการ AI สำหรับองค์กรที่ครอบคลุมการกำกับดูแล การบริหารจัดการความเสี่ยง และการควบคุมการใช้งาน AI อย่างมีความรับผิดชอบ (Responsible AI) โดยตรง



04
บทนำ

4.1 ทำไมจึงต้องมีธรรมาภิบาลในการประยุกต์ใช้ AI

ปัญญาประดิษฐ์ หรือ AI เป็นเทคโนโลยีที่มีความแตกต่างเฉพาะเมื่อเปรียบเทียบกับเทคโนโลยีอื่นในด้านความสามารถในการตัดสินใจได้โดยอัตโนมัติ ความสามารถในการประมวลผลข้อมูลที่มีความซับซ้อนและยากที่มนุษย์จะสามารถทำได้ อีกทั้ง ยังมีความสามารถในการเรียนรู้และปรับปรุงประสิทธิภาพในการตัดสินใจของตนเองได้ตามสถานการณ์หรือสภาพแวดล้อมที่เปลี่ยนแปลงด้วยการนำข้อมูลจากบริบทแวดล้อมและข้อเสนอแนะจากผู้ใช้งานมาเรียนรู้เพิ่มเติม ซึ่งจากความสามารถดังกล่าวของ AI ทำให้หลายองค์กรตัดสินใจที่จะนำ AI มาช่วยในการตัดสินใจ แก้ปัญหาหรือทำงานแทนมนุษย์ รวมถึงช่วยในการหาโอกาสใหม่ทางธุรกิจด้วยการประมวลผลข้อมูลที่มีความซับซ้อน

จากการศึกษาการประยุกต์ใช้เทคโนโลยี AI ในหลายประเทศที่ผ่านมาพบว่า **การทำงานของ AI อาจไม่เป็นไปตามที่ออกแบบไว้ตั้งแต่ต้น อีกทั้งยังอาจก่อให้เกิดความเสียหายโดยไม่คาดคิด** ซึ่งในหลายกรณีพบว่า AI มีการตัดสินใจที่ผิดพลาดและมีอคติ ทำให้ส่งผลกระทบเชิงลบทั้งในระดับบุคคล องค์กร และสังคมโดยกว้าง ตัวอย่างเช่น การเกิดอุบัติเหตุรถชนพร้อมกันหลายคัน เนื่องจากการใช้ระบบขับขี่อัตโนมัติเต็มรูปแบบ (Full Self-Driving Mode) หรือในกรณีที่คนผิวขาวในสหรัฐอเมริกาได้รับสิทธิประโยชน์ในการรักษาพยาบาลที่ดีกว่าคนผิวดำ เนื่องจาก AI ถูกสอนด้วยข้อมูลของคนผิวขาวเป็นส่วนใหญ่ ทำให้การตัดสินใจของ AI มีความเอนเอียงและมีอคติต่อคนผิวดำ เป็นต้น ด้วยเหตุนี้การนำเทคโนโลยี AI มาประยุกต์ใช้จึงจำเป็นต้องคำนึงถึงปัจจัยต่าง ๆ ที่อาจก่อให้เกิดทั้งประโยชน์และผลกระทบเชิงลบที่มนุษย์ไม่เคยคาดคิดมาก่อน

ด้วยเหตุผลดังกล่าวข้างต้น จึงทำให้เกิดการพัฒนาหลักการธรรมาภิบาลในการประยุกต์ใช้ AI หรือหลักการในการกำกับดูแลการประยุกต์ใช้ AI ที่ดี โดย**เป้าหมายของหลักการธรรมาภิบาลนั้นไม่ได้มีวัตถุประสงค์เพียงเพื่อสนับสนุนให้องค์กรประสบความสำเร็จในการประยุกต์ใช้ AI เท่านั้น แต่ยังหมายรวมถึงการประยุกต์ใช้ AI อย่างมีความรับผิดชอบ โดยนำหลักการจริยธรรมปัญญาประดิษฐ์มาปรับใช้** เช่น การตัดสินใจด้วยความเป็นธรรม ไม่มีอคติ มีความโปร่งใส สามารถตรวจสอบและอธิบายเหตุผลในการตัดสินใจของ AI ได้ เป็นต้น **และคำนึงถึงความสอดคล้องตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง พร้อมทั้งมีการควบคุมความเสี่ยงจากการประยุกต์ใช้ AI และผลกระทบเชิงลบที่อาจเกิดขึ้นต่อบุคคลที่เกี่ยวข้อง องค์กร และสังคมโดยกว้าง เพื่อนำไปสู่ความเชื่อมั่นและการยอมรับจากบุคคลที่เกี่ยวข้อง**

4.2 ธรรมาภิบาลในการประยุกต์ใช้ AI คืออะไร

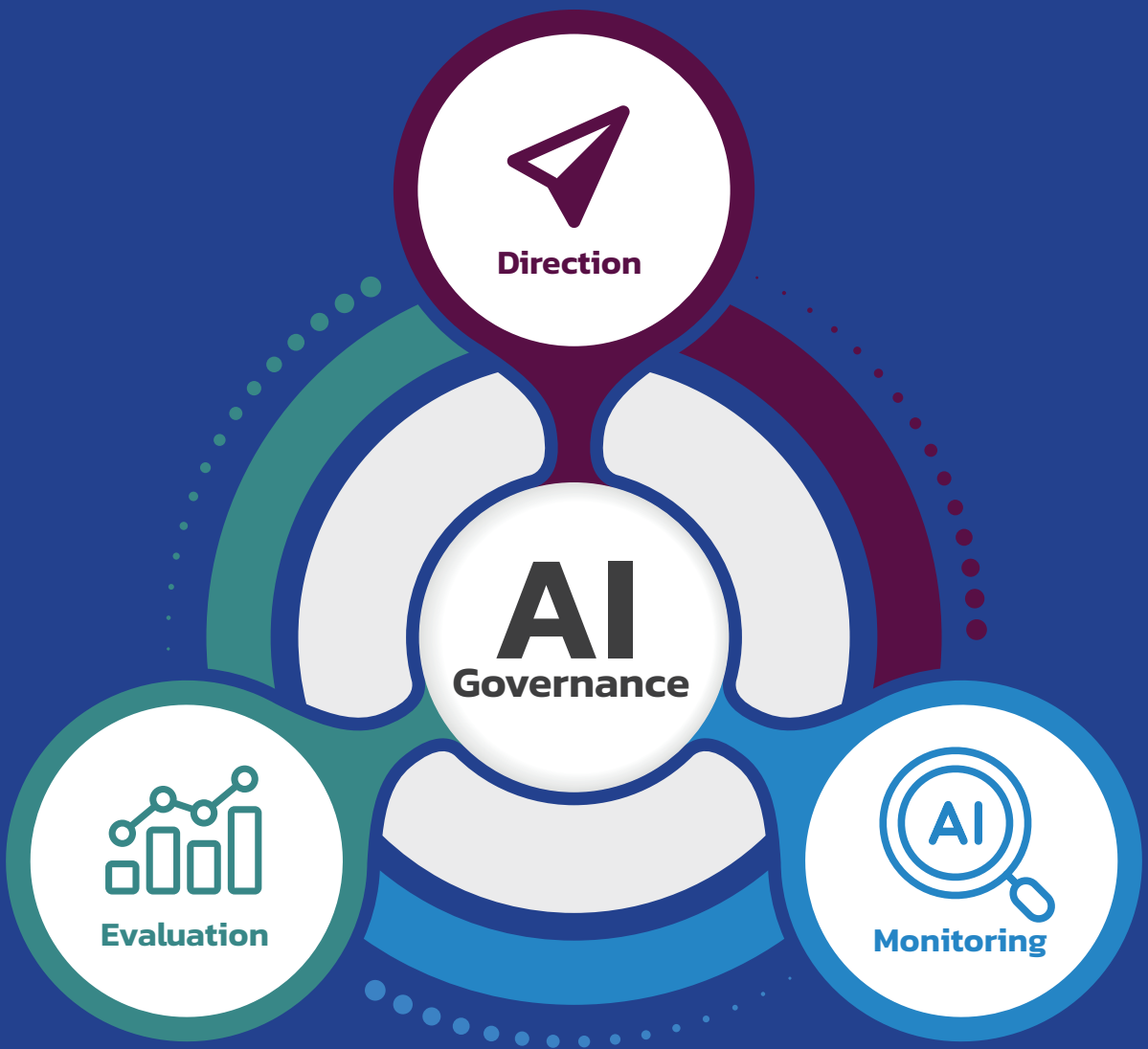
ธรรมาภิบาลในการประยุกต์ใช้ AI คือ **หลักการกำกับดูแลการปฏิบัติงานในทุกกระบวนการที่เกี่ยวข้องกับการประยุกต์ใช้ AI โดยจัดให้มีมาตรการในการกำกับดูแลผ่านการกำหนดนโยบาย ขั้นตอนปฏิบัติ และเครื่องมือในการปฏิบัติงาน เพื่อให้มั่นใจได้ว่าการประยุกต์ใช้ AI นั้น สามารถบรรลุตามเป้าหมายขององค์กรอย่างมีความรับผิดชอบ** โดยคำนึงถึงความสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ ความสอดคล้องตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง และมีการควบคุมความเสี่ยงที่อาจส่งผลกระทบต่อบุคคลที่เกี่ยวข้อง องค์กร และสังคมโดยกว้าง

โดยมีคณะกรรมการกำกับดูแลการประยุกต์ใช้ AI ซึ่งมีหน้าที่หลัก ดังนี้

1) **กำหนดทิศทางการดำเนินการ (Direction)** โดยกำหนดกลยุทธ์ในการประยุกต์ใช้ AI และนโยบายที่เกี่ยวข้อง

2) **เฝ้าติดตาม (Monitoring)** ประสิทธิภาพ (Performance) ของการประยุกต์ใช้ AI รวมถึงการปฏิบัติงานตามนโยบายและข้อกำหนดต่าง ๆ (Conformance) ทั้งภายในและภายนอกองค์กร

3) **ประเมินผล (Evaluation)** การประยุกต์ใช้งาน AI ในปัจจุบันและอนาคต โดยพิจารณาจากปัจจัยที่เกี่ยวข้องทั้งภายในและภายนอก เช่น เป้าหมายในการประยุกต์ใช้ AI ภัยคุกคามและโอกาสจากการประยุกต์ใช้ AI ความเปลี่ยนแปลงด้านเทคโนโลยี ประสิทธิภาพและประสิทธิผลในการกำกับดูแล เป็นต้น


Direction
AI
Governance
Evaluation
AI
Monitoring

4.3 หลักการจริยธรรมปัญญาประดิษฐ์

เพื่อให้การประยุกต์ใช้ AI เป็นไปอย่างมีความรับผิดชอบนั้น จำเป็นต้องมีการนำหลักการจริยธรรมปัญญาประดิษฐ์ที่เกี่ยวข้องมาปรับใช้ โดยองค์กรจะต้องกำหนดกลยุทธ์ในการประยุกต์ใช้ AI (AI Strategy) และนโยบายให้สอดคล้องตามหลักการจริยธรรมที่เกี่ยวข้อง ซึ่งในการพิจารณานำหลักการจริยธรรมปัญญาประดิษฐ์ใดมาปรับใช้นั้นขึ้นอยู่กับบริบทขององค์กรที่นำ AI ไปประยุกต์ใช้

ทั้งนี้ **องค์กรอาจพิจารณานำหลักการจริยธรรมปัญญาประดิษฐ์ตามแนวทางของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) มาปรับใช้ทั้งหมดหรือบางส่วน หรืออาจนำหลักการจริยธรรมปัญญาประดิษฐ์อื่น ๆ ที่เกี่ยวข้องกับบริบทของการประยุกต์ใช้ AI มาปรับใช้**ตามความเหมาะสม

หลักการจริยธรรมปัญญาประดิษฐ์ของไทย ตามแนวทางของ สดช.

01 **ความสามารถในการแข่งขันและการพัฒนาอย่างยั่งยืน (Competitiveness and Sustainable Development)** AI ควรถูกสร้างและใช้งานเพื่อสร้างประโยชน์และคุณค่าให้แก่มนุษย์ สังคม เศรษฐกิจและสิ่งแวดล้อมอย่างยั่งยืน รวมถึงเพิ่มความสามารถในการแข่งขันและสร้างความเจริญให้กับทุกภาคส่วนในโลกอย่างเป็นธรรม นอกจากนี้ AI ยังควรได้รับการวิจัยและพัฒนาอย่างต่อเนื่องเพื่อสร้างสรรค์นวัตกรรมและอุตสาหกรรมใหม่

02 **ความสอดคล้องกับกฎหมาย จริยธรรม และมาตรฐานสากล (Laws, Ethics, and International Standards)** AI ควรได้รับการออกแบบ พัฒนา ให้บริการและใช้งาน โดยสอดคล้องกับกฎหมาย บรรทัดฐาน จริยธรรม คุณธรรมของมนุษย์ และ มาตรฐานสากล โดยเคารพต่อความเป็นส่วนตัว เกียรติ สิทธิเสรีภาพ และสิทธิมนุษยชน นอกจากนี้ AI ยังควรได้รับการออกแบบโดยมีมนุษย์เป็นศูนย์กลางและเป็นผู้ตัดสินใจ (Human-Centered Design) และไม่ควรถูกออกแบบเพื่อใช้ในการกำหนดชะตาชีวิตของมนุษย์

03 **ความโปร่งใสและความรับผิดชอบต่อผลของการกระทำ (Transparency and Accountability)** AI ควรได้รับการออกแบบ พัฒนา ให้บริการ และใช้งานด้วยความโปร่งใส โดยจะต้องสามารถอธิบาย (Explainability) และคาดการณ์ผลลัพธ์จากการทำงานได้ อีกทั้ง ยังควรมีการเฝ้าติดตามความผิดปกติ มีความสามารถในการสืบย้อนกลับ (Traceability) และสามารถวินิจฉัยปัญหาและความผิดพลาดได้ (Diagnosability) นอกจากนี้ องค์กรยังควรมีการกำหนดหน้าที่และความรับผิดชอบ (Role and Responsibility) รวมถึงความรับผิดชอบต่อผลของการกระทำ (Accountability) ต่อผลกระทบที่เกิดขึ้นจาก AI ตามหน้าที่ที่รับผิดชอบได้

04 **ความมั่นคงปลอดภัยและความเป็นส่วนตัว (Security and Privacy)** AI ควรถูกออกแบบและพัฒนาโดยให้ความสำคัญถึงความมั่นคงปลอดภัยและการรักษาความเป็นส่วนตัว โดยจัดให้มีมาตรการป้องกันการโจมตีทางไซเบอร์ และปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมถึงมีกลไกที่ให้มนุษย์สามารถแทรกแซงเพื่อควบคุมการทำงานของ AI ในกรณีที่เกิดเหตุการณ์หรือความเสี่ยงที่มีผลกระทบกับมนุษย์ได้

05 **ความเท่าเทียม หลากหลาย ครอบคลุม และเป็นธรรม (Fairness)** ในการส่งเสริมการประยุกต์ใช้ AI อย่างเป็นธรรมและลดความมีอคติ (Bias) ระบบควรถูกออกแบบและพัฒนาโดยคำนึงความหลากหลาย (Diversity) ลดการเอนเอียง แบ่งแยก และเลือกปฏิบัติ (Discrimination) ต่อบุคคลหรือกลุ่มคนที่มีคุณลักษณะที่ต่างกัน (อาทิ อายุ เพศ ลักษณะทางกายภาพ เชื้อชาติ) โดยเฉพาะกลุ่มคนผู้ด้อยโอกาสในสังคม รวมถึงสามารถพิสูจน์ถึงความเป็นธรรมสำหรับทุกฝ่ายที่เกี่ยวข้อง

06 **ความน่าเชื่อถือ (Reliability)** AI ควรได้รับการสนับสนุนให้มีความน่าเชื่อถือและความมั่นใจในการใช้งานต่อสาธารณะ โดยสนับสนุนให้มีการพัฒนาด้วยความยึดมั่นในความถูกต้อง (Accuracy) ความน่าเชื่อถือ (Reliability) สามารถทนทานต่อเหตุการณ์ที่อาจเกิดความผิดพลาด (Robustness) และสามารถสร้างผลลัพธ์ได้เหมือนเดิม (Reproducibility) นอกจากนี้ควรมีการควบคุมคุณภาพของข้อมูล (Quality of data) รวมถึงกำหนดกระบวนการและช่องทางรับความคิดเห็น (Feedback) จากผู้ใช้งาน ให้ข้อมูลเพิ่มเติม รับเรื่องร้องเรียน แจ้งปัญหาที่พบ และมีการตอบสนองหรือดำเนินการแก้ไขปัญหาที่พบได้ทันท่วงที

4.4 กรอบการทำงานเพื่อสนับสนุน ธรรมาภิบาลในการประยุกต์ใช้ AI

AI GOVERNANCE GUIDELINE

กรอบการทำงาน
เพื่อสนับสนุนให้เกิด
ธรรมาภิบาล
ในการประยุกต์ใช้ AI
ประกอบด้วย
3 องค์ประกอบหลัก ได้แก่



AI Governance Structure

- จัดตั้งคณะกรรมการกำกับดูแล (AI Governance Council) เพื่อกำหนดทิศทางการประยุกต์ใช้งาน AI ผ่านการกำหนดกลยุทธ์และนโยบาย รวมถึงเฝ้าติดตาม และประเมินผลกาประยุกต์ใช้ AI อย่างต่อเนื่อง เพื่อสนับสนุนให้เกิดธรรมาภิบาลในการประยุกต์ใช้ AI
- กำหนดหน้าที่ของบุคลากรและผู้มีส่วน-ได้เสียที่เกี่ยวข้องกับการประยุกต์ใช้ AI พร้อมทั้งสร้างความตระหนักรู้ในด้านความรับผิดชอบ (Responsibility) และความรับผิดชอบต่อผลของการกระทำ (Accountability) ของแต่ละหน้าที่
- พัฒนาศักยภาพของบุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง เพื่อให้สามารถปฏิบัติงานได้อย่างเหมาะสมตามหน้าที่ที่ได้รับมอบหมาย



AI Strategy

- มองหาโอกาสในการนำ AI มาประยุกต์ใช้เพื่อสนับสนุนให้บรรลุเป้าหมายขององค์กรหรือเป้าหมายทางธุรกิจ
- กำหนดเป้าหมายในการประยุกต์ใช้ AI ตามลำดับความสำคัญ โดยพิจารณาจากประโยชน์ที่จะได้รับ ความพร้อมขององค์กร หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่ต้องดำเนินการให้สอดคล้อง รวมถึง ความซับซ้อนและเวลาที่จำเป็นต้องใช้ในการดำเนินการ
- กำหนดกลยุทธ์ในการบริหารจัดการข้อมูล
- กำหนดแผนปฏิบัติงานในการประยุกต์ใช้ AI (AI Roadmap)
- วิเคราะห์ความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประยุกต์ใช้ AI รวมถึงการกำหนดระดับการมีส่วนร่วมของมนุษย์ในการทำงานของ AI และมาตรการในการควบคุมความเสี่ยงที่เหมาะสม เพื่อควบคุมความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้



AI Operation

- จัดทำข้อกำหนดความต้องการในการพัฒนาระบบ AI (AI Requirement) พร้อมทั้งออกแบบโซลูชั่นที่เหมาะสมกับข้อกำหนดดังกล่าว
- จัดเตรียมข้อมูลที่มีคุณภาพสำหรับการสอน ตรวจสอบ และทดสอบโมเดลปัญญาประดิษฐ์ รวมถึงลดความมีอคติที่อาจเกิดจากข้อมูล (Data Bias)
- สร้างโมเดลปัญญาประดิษฐ์โดยนำหลักการจริยธรรมปัญญาประดิษฐ์มาปรับใช้ และควบคุมความเสี่ยงที่อาจเกิดขึ้น
- เฝ้าติดตามประสิทธิภาพ (Performance) การประยุกต์ใช้ AI รวมถึงการปฏิบัติงานตามนโยบาย หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้อง (Compliance)
- ประเมินผลการประยุกต์ใช้งาน AI ในปัจจุบัน และกำหนดแนวทางการดำเนินงานอนาคต

4.5 คำนิยาม

ปัญญาประดิษฐ์ (Artificial Intelligence: AI) – เทคโนโลยีที่ถูกพัฒนาขึ้นเพื่อให้คอมพิวเตอร์มีคุณสมบัติหรือพฤติกรรมใกล้เคียงมนุษย์ เช่น การเรียนรู้ การรับรู้และตอบสนองต่อสภาพแวดล้อม การให้เหตุผล และการแก้ไขปัญหา เป็นต้น ตามวัตถุประสงค์ที่มนุษย์กำหนด

แมชชีนเลิร์นนิ่ง (Machine Learning) – เทคโนโลยี AI ประเภทหนึ่งที่มีความสามารถในการเรียนรู้หรือปรับปรุงประสิทธิภาพการทำงานของตน โดยใช้อัลกอริทึมในการวิเคราะห์และเรียนรู้จากข้อมูลที่ได้รับจากการสอนหรือสภาพแวดล้อม

โมเดลปัญญาประดิษฐ์ (AI Model) – โปรแกรมที่ถูกสร้างขึ้นจากอัลกอริทึมและข้อมูลที่สอนโดยมนุษย์ เพื่อให้คอมพิวเตอร์มีคุณสมบัติหรือพฤติกรรมใกล้เคียงมนุษย์

หมายเหตุ: โมเดลปัญญาประดิษฐ์ประเภทแมชชีนเลิร์นนิ่ง (Machine Learning) เท่านั้นที่จำเป็นต้องมีการเรียนรู้จากข้อมูลที่สอนโดยมนุษย์

หลักการจริยธรรมปัญญาประดิษฐ์ (AI Ethics Principles) – หลักการในการออกแบบและพัฒนา ให้พฤติกรรมหรือผลลัพธ์จากการทำงานของ AI สอดคล้องตามหลักการจริยธรรมหรือหลักการอันดีที่พึงปฏิบัติตามบริบทที่ AI ถูกนำไปประยุกต์ใช้

หลักการในการประยุกต์ใช้ AI อย่างมีความรับผิดชอบ (Responsible AI) – หลักการในการนำ AI มาประยุกต์ใช้เพื่อประโยชน์ของบุคคลที่เกี่ยวข้องและองค์กร อย่างมีความรับผิดชอบต่อผลกระทบที่อาจเกิดขึ้นกับบุคคล องค์กร และสังคมโดยกว้าง เพื่อนำไปสู่การสร้างความเชื่อมั่นและการยอมรับจากบุคคลที่เกี่ยวข้องในทุกภาคส่วน

องค์กร – องค์กร หน่วยงาน หรือกลุ่มบุคคลในรูปแบบใดรูปแบบหนึ่งที่นำเทคโนโลยี AI มาประยุกต์ใช้เพื่อสนับสนุนการปฏิบัติงานหรือบริการให้บรรลุตามเป้าหมายที่กำหนด

ผู้ให้บริการโซลูชั่นด้าน AI (AI Solution Provider) – ผู้ให้บริการที่นำเทคโนโลยี AI มาพัฒนาเป็นโซลูชั่นหรือซอฟต์แวร์ เพื่อให้บริการแก่บุคคลหรือองค์กรที่ต้องการนำเทคโนโลยี AI ไปประยุกต์หรือปรับใช้ตามวัตถุประสงค์ที่ต้องการ





05

การกำหนด โครงสร้างการกำกับดูแล

(AI Governance Structure)

5.1 คณะกรรมการกำกับดูแลการประยุกต์ใช้ AI
(AI Governance Council)

ในการประยุกต์ใช้ AI อย่างมีธรรมาภิบาลนั้น องค์กรจำเป็นต้องมีการ**กำหนดโครงสร้างการกำกับดูแลภายในองค์กร โดยมีการกำหนดหน้าที่และความรับผิดชอบ (Role and Responsibility) รวมถึงกำหนดความรับผิดชอบต่อผลของการกระทำ (Accountability) ของบุคลากรภายในองค์กรและผู้มีส่วนได้เสียที่เกี่ยวข้องตามหน้าที่ที่ได้รับมอบหมาย** เพื่อให้มั่นใจได้ว่าการประยุกต์ใช้ AI จะเป็นไปตามเป้าหมาย สอดคล้องตามหลักการจริยธรรม ปัญญาประดิษฐ์ กฎหมายและข้อกำหนดต่าง ๆ พร้อมทั้ง มีการควบคุมความเสี่ยงที่อาจเกิดขึ้น โดยมี**คณะกรรมการกำกับดูแลการประยุกต์ใช้ AI (AI Governance Council) เป็นศูนย์กลางในการกำหนดทิศทางการดำเนินการ (Direction) การเฝ้าติดตาม (Monitoring) และการประเมินผล (Evaluation) การประยุกต์ใช้ AI**

กำหนดทิศทางการดำเนินการ (Direction)

ในด้านการกำหนดทิศทางนั้น คณะกรรมการกำกับดูแลฯ ทำหน้าที่ในการ**พิจารณากลยุทธ์การประยุกต์ใช้ AI (AI Strategy) รวมถึงกำหนดนโยบายที่เกี่ยวข้องกับการประยุกต์ใช้ AI และการกำกับดูแล (AI Governance Policies)** ในด้านต่าง ๆ เช่น

- โครงสร้างการกำกับดูแล
- หน้าที่และความรับผิดชอบ และความรับผิดชอบต่อผลของการกระทำ
- การบริหารจัดการและการใช้งานข้อมูล
- การออกแบบโซลูชั่น สร้าง ทดสอบ และนำ AI ไปประยุกต์ใช้งาน
- การทำงานร่วมกันระหว่าง AI กับมนุษย์
- การประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประยุกต์ใช้ AI
- การขออนุมัติ พิจารณา หรือตัดสินใจด้านต่าง ๆ เช่น แผนปฏิบัติงานในการประยุกต์ใช้ AI (AI Roadmap) การนำโมเดลปัญญาประดิษฐ์ (AI Model) ไปใช้งานจริง ความสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ การแก้ไขประเด็นปัญหาและแนวทางการดำเนินงานที่เกี่ยวข้องกับการประยุกต์ใช้ AI เป็นต้น

พร้อมทั้ง **มีหน้าที่ในการสื่อสารนโยบายและทิศทางของการกำกับดูแลให้แก่บุคลากรและผู้มีส่วนได้เสียที่เกี่ยวข้องเพื่อให้เกิดความเข้าใจและรับทราบร่วมกัน**

โดยในการกำหนดกลยุทธ์และนโยบายดังกล่าว จำเป็นต้องคำนึงถึง 1) ความสอดคล้องตามเป้าหมายขององค์กรหรือเป้าหมายในการดำเนินธุรกิจ 2) ความสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดต่าง ๆ และ 3) การควบคุมความเสี่ยงและผลกระทบที่อาจเกิดขึ้น ตามบริบทของการนำ AI ไปประยุกต์ใช้

นอกจากนี้ ในด้านของการควบคุมความเสี่ยง คณะกรรมการกำกับดูแลฯ ยังมีหน้าที่ในการ**พิจารณาว่าความเสี่ยงใดเป็นความเสี่ยงที่ยอมรับได้ (Risk Appetite) พร้อมทั้งกำกับดูแลให้มีการบริหารจัดการความเสี่ยง (Risk Management) อย่างเหมาะสม** เพื่อควบคุมความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้

การเฝ้าติดตาม (Monitoring)

การเฝ้าติดตาม (Monitoring) การประยุกต์ใช้ AI นั้น เป็นกระบวนการที่คณะกรรมการกำกับดูแลฯ ต้องดำเนินการอย่างต่อเนื่อง เพื่อ**เฝ้าติดตามประสิทธิภาพของการประยุกต์ใช้ AI (Performance) รวมถึงเฝ้าติดตามการปฏิบัติงานตามนโยบายขององค์กร หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดต่าง ๆ (Conformance) และเฝ้าติดตามความเสี่ยงว่ายังอยู่ในระดับยอมรับได้**

โดยในกระบวนการเฝ้าติดตามนี้ คณะกรรมการกำกับดูแลฯ จะทำการ**เฝ้าติดตามจากรายงานผลการปฏิบัติงานของบุคลากรและผู้มีส่วนได้เสียที่เกี่ยวข้อง** โดยรายงานอาจประกอบด้วยข้อมูล เช่น

- ผลการดำเนินงานตามตัวชี้วัดที่องค์กรกำหนด (Key Performance Indicator: KPI)
- รายงานข้อมูลเกี่ยวกับความถูกต้องของการตัดสินใจของ AI
- ความสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ที่เกี่ยวข้อง
- ข้อคิดเห็น (Feedback) ประเด็นปัญหา (Issue) และความผิดพลาด (Error) ที่พบจากประยุกต์ใช้ AI

ทั้งนี้ การรายงานผลการปฏิบัติงานต่อคณะกรรมการกำกับดูแลฯ อย่างทันท่วงทีและมีข้อมูลที่เพียงพอต่อการตัดสินใจ จะช่วยสร้างความเชื่อมั่นและการยอมรับจากบุคคลที่เกี่ยวข้อง

การประเมินผล (Evaluation)

ในด้านการประเมินผลการประยุกต์ใช้ AI นั้น **คณะกรรมการกำกับดูแลฯ ควรมีการประเมินผลการปฏิบัติงานและประเมินผลการประยุกต์ใช้งาน AI ที่ผ่านมา เพื่อพิจารณาสิ่งที่ต้องปรับปรุงและกำหนดแนวทางการดำเนินงานในอนาคต** โดยในการประเมินผลการประยุกต์ใช้ AI นั้น องค์กรอาจจัดให้มีการประเมินผลโดยผู้ตรวจประเมินภายใน (Internal Auditor) หรือผู้ตรวจประเมินภายนอก (External Auditor) ตามความเหมาะสม เพื่อช่วยเพิ่มความน่าเชื่อถือ (Reliability) และสร้างการยอมรับจากบุคคลที่เกี่ยวข้อง

โดยในการประเมินผลการประยุกต์ใช้งานนั้น อาจมีการพิจารณาในด้านต่าง ๆ ตามตัวอย่างด้านล่าง แต่อย่างไรก็ตามหลักเกณฑ์ในการประเมินผลของแต่ละองค์กรอาจมีความแตกต่างกันตามบริบทของการประยุกต์ใช้งาน AI ได้ด้วยเช่นกัน ตัวอย่างเช่น

- ประเมินประสิทธิภาพในการทำงานของ AI และผลลัพธ์ความสำเร็จจากการประยุกต์ใช้ AI ที่ผ่านมา เมื่อเทียบกับเป้าหมายที่กำหนด
- พิจารณาปรับปรุงเป้าหมายในการประยุกต์ใช้ AI หากพบว่าการประยุกต์ใช้ AI ไม่สามารถช่วยให้องค์กรบรรลุเป้าหมายตามที่กำหนดได้
- พิจารณาปรับปรุงข้อกำหนดความต้องการในการพัฒนาระบบ AI (AI Requirement) หากพบว่าข้อกำหนดความต้องการไม่ถูกต้อง หรือยกเลิกข้อกำหนดในบางเรื่องหากพบว่าไม่มีความจำเป็น
- นำความคิดเห็น (Feedback) ประเด็นปัญหา (Issue) และความผิดพลาด (Error) ที่พบ มาพิจารณาปรับปรุงเป้าหมายในการประยุกต์ใช้หรือข้อกำหนดความต้องการในการพัฒนาระบบ
- ประเมินประสิทธิภาพของมาตรการในการกำกับดูแล เพื่อให้การประยุกต์ใช้ AI สอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดต่าง ๆ ที่เกี่ยวข้อง
- ทบทวนความเสี่ยงจากการดำเนินงานที่ผ่านมา รวมถึงวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นในอนาคต เพื่อกำหนดความเสี่ยงที่ยอมรับได้ (Risk Appetite) รวมถึงปรับปรุงมาตรการในการควบคุมความเสี่ยงและแผนการจัดการความเสี่ยง (Risk Treatment Plan) ให้เหมาะสม

การจัดตั้งคณะกรรมการกำกับดูแลการประยุกต์ใช้ AI (Setting up AI Governance Council)

เนื่องจากคณะกรรมการกำกับดูแลฯ เป็นศูนย์กลางในการกำกับดูแลการประยุกต์ใช้ AI จึงอาจสรุปหน้าที่และความรับผิดชอบหลักในการกำกับดูแล ได้ดังนี้

1) **กำกับดูแลการปฏิบัติงานเพื่อให้การประยุกต์ใช้ AI ประสบความสำเร็จและบรรลุตามเป้าหมาย**ที่องค์กรกำหนด **ผ่านการกำหนดกลยุทธ์ในการประยุกต์ใช้ AI (AI Strategy) และการกำหนดนโยบาย**

2) **เฝ้าติดตามประสิทธิภาพ (Performance) และประเมินผลการประยุกต์ใช้ AI**

3) **เฝ้าติดตามและประเมินผลการปฏิบัติงานให้สอดคล้อง (Conformance)** ตามนโยบายขององค์กร หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้อง

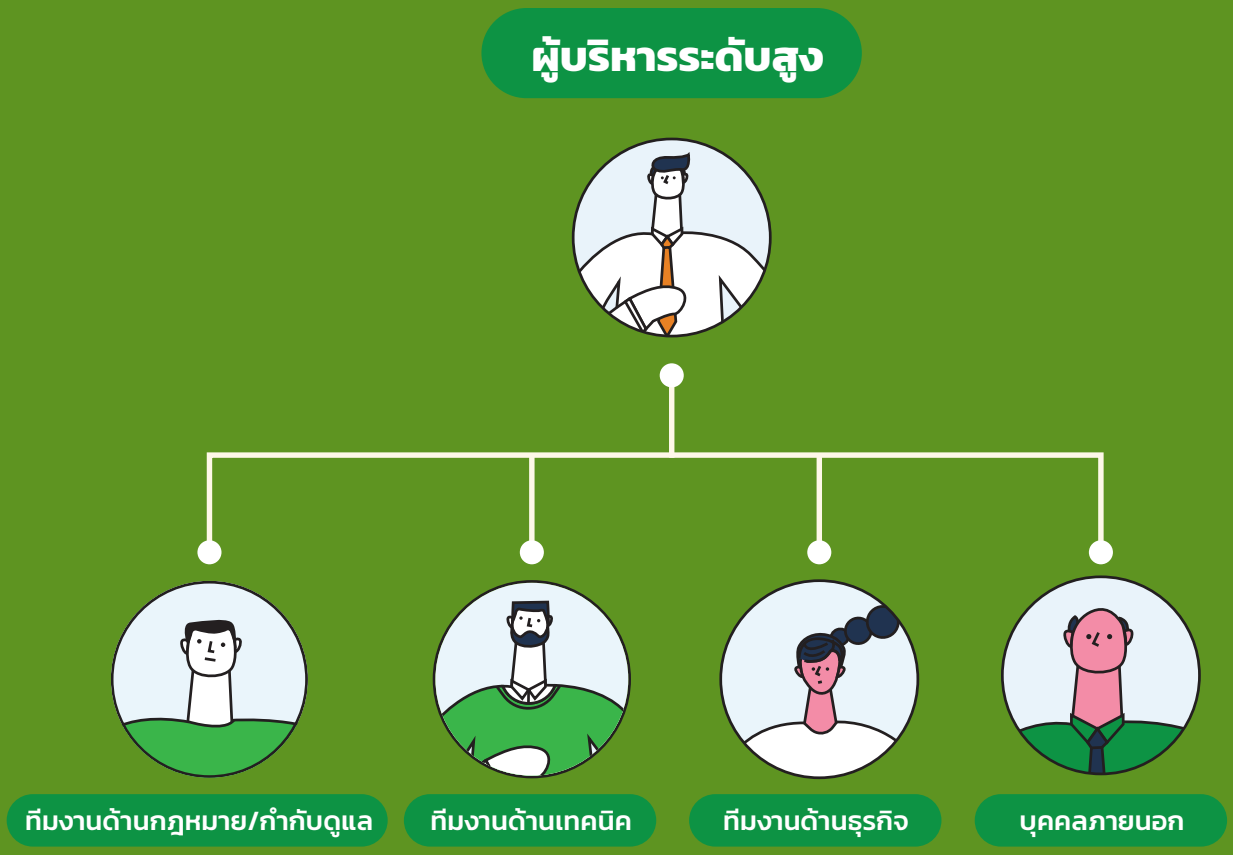
4) **กำกับดูแลและควบคุมความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้**

5) **อนุมัติ พิจารณา หรือตัดสินใจด้านต่าง ๆ** ที่เกี่ยวข้องกับการประยุกต์ใช้ AI

จากหน้าที่และความรับผิดชอบหลักข้างต้น คณะกรรมการกำกับดูแลฯ จึงควรประกอบด้วยผู้บริหารและบุคลากรด้านต่าง ๆ ที่เกี่ยวข้องกับการประยุกต์ใช้ AI ทั้งจากภายในและภายนอกองค์กร (หากจำเป็น) แต่อย่างไรก็ตาม **การคัดเลือกสมาชิกของคณะกรรมการกำกับดูแลฯ ในแต่ละองค์กรอาจมีความแตกต่างกันตามขนาดขององค์กร ข้อจำกัดด้านทรัพยากรบุคคล กฎหมายและข้อกำหนดที่เกี่ยวข้อง บริบทและความเสี่ยงที่อาจเกิดขึ้นจากการประยุกต์ใช้ AI เป็นต้น**

คณะกรรมการกำกับดูแลฯ เป็นผู้รับผิดชอบโดยตรงต่อผลลัพธ์จากการทำงานหรือการตัดสินใจของ AI ดังนั้น จึงจำเป็นต้องมีการกำกับดูแลเพื่อให้มั่นใจได้ว่าการประยุกต์ใช้ AI เป็นไปตามเป้าหมายที่กำหนด สอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้อง รวมถึงควบคุมความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้

ตัวอย่างโครงสร้างคณะกรรมการกำกับดูแลฯ



- **ผู้บริหารระดับสูง** เช่น ผู้บริหารในระดับ C-level เป็นต้น ที่มีอำนาจในการกำหนดทิศทางในการดำเนินงาน การตัดสินใจ และสนับสนุนทรัพยากรที่จำเป็น
- **ผู้บริหารหรือผู้แทนจากทีมงานด้านต่าง ๆ ที่เกี่ยวข้องกับการประยุกต์ใช้ AI** เช่น ทีมงานด้านกฎหมาย/กำกับดูแล ทีมงานด้านธุรกิจ และทีมงานด้านเทคนิค เป็นต้น
- **บุคคลภายนอก** (หากจำเป็น) เช่น หน่วยงานกำกับดูแลและผู้เชี่ยวชาญในด้านที่จะนำ AI ไปประยุกต์ใช้ เป็นต้น

ซึ่งจากโครงสร้างดังกล่าว องค์กรอาจพิจารณานำโครงสร้างการกำกับดูแลภายใน**องค์กรที่มีอยู่แล้วมาปรับใช้ เพื่อสนับสนุนหรือทำงานร่วมกับคณะกรรมการกำกับดูแลฯ** เช่น

- มอบหมายให้**คณะกรรมการจริยธรรม (Ethics Board/Committee)** กำกับดูแลเรื่องความสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์
- มอบหมายให้**คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)** กำกับดูแลเรื่องการบริหารจัดการข้อมูลให้มีคุณภาพและเหมาะสมกับการใช้งานร่วมกับ AI รวมถึงกำกับดูแลมาตรการในการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม
- มอบหมายให้**คณะกรรมการตามโครงสร้าง Governance, Risk, and Compliance (GRC)** บริหารจัดการและควบคุมความเสี่ยงที่เกี่ยวกับการประยุกต์ใช้ AI รวมถึงกำกับดูแลในด้านความสอดคล้องของการปฏิบัติงานในด้านต่าง ๆ

5.2 หน้าที่และความรับผิดชอบ (Role and Responsibility)

องค์กรที่จะนำ AI มาประยุกต์ใช้งานจำเป็นต้องมีการ**กำหนดหน้าที่และความรับผิดชอบ (Role and Responsibility) รวมถึงกำหนดความรับผิดชอบต่อผลของการกระทำ (Accountability) ของบุคลากรและผู้มีส่วนได้เสียที่เกี่ยวข้องในทุกกระบวนการ** โดยอาจสรุปได้ ดังนี้

ระดับนโยบาย (Strategic Level)

อาจประกอบด้วย:

- **ผู้บริหารระดับสูง**
- **คณะกรรมการจริยธรรม***
- **คณะกรรมการตามโครงสร้าง GRC***
- **คณะกรรมการธรรมาภิบาลข้อมูล***
- **ผู้บริหารหรือผู้แทนจากทีมงานภายในองค์กรที่เกี่ยวข้องกับการประยุกต์ใช้ AI**
- **ผู้เชี่ยวชาญหรือหน่วยงานกำกับดูแล****

หมายเหตุ:

* โครงสร้างการกำกับดูแลภายในองค์กรที่อาจนำมาปรับใช้เพื่อสนับสนุนหรือร่วมดำเนินงาน

** บุคคลหรือกลุ่มบุคคลภายนอกที่อาจเข้ามาร่วมดำเนินงาน

ด้านกำกับดูแลการปฏิบัติงานเพื่อบรรลุเป้าหมายที่กำหนด

- กำหนดกลยุทธ์และเป้าหมายในการประยุกต์ใช้ AI ภายในองค์กร
- กำหนดนโยบายที่เกี่ยวข้องกับการประยุกต์ใช้ AI และนโยบายในการกำกับดูแลการปฏิบัติงานของบุคลากรและผู้มีส่วนได้เสียที่เกี่ยวข้อง
- อนุมัติ พิจารณา หรือตัดสินใจด้านต่าง ๆ ที่เกี่ยวข้องกับการประยุกต์ใช้ AI เช่น
  - o แผนปฏิบัติงานในการประยุกต์ใช้ AI (AI Roadmap)
  - o การนำโมเดลปัญญาประดิษฐ์ (AI Model) ไปใช้งานจริง
  - o ความสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์
  - o การแก้ไขประเด็นปัญหาและกำหนดแนวทางการดำเนินงาน
- เฝ้าติดตามประสิทธิภาพการทำงานของ AI และระดับความสำเร็จในการประยุกต์ใช้ AI เมื่อเทียบกับเป้าหมายที่กำหนด
- ประเมินผลประยุกต์ใช้งาน AI ที่ผ่านมาและกำหนดแนวทางการดำเนินงานในอนาคต

ด้านการปฏิบัติงานให้สอดคล้อง (Conformance) ตามข้อกำหนดภายในและภายนอกองค์กร

- กำหนดนโยบายในการกำกับดูแลการปฏิบัติงานของบุคลากรและผู้มีส่วนได้เสียที่เกี่ยวข้อง รวมถึงเฝ้าติดตามและประเมินผลการปฏิบัติงานตามนโยบายองค์กร หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้อง

ด้านการควบคุมความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

- กำหนดความเสี่ยงที่ยอมรับได้ (Risk Appetite) และพิจารณาความเหมาะสมของมาตรการเพื่อจำกัดความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้

ระดับปฏิบัติการ (Implementation Level)

อาจประกอบด้วย:

- ผู้บริหาร/ผู้จัดการที่เกี่ยวข้องกับการประยุกต์ใช้ AI
- ทีมงานด้านธุรกิจที่เกี่ยวข้องกับการประยุกต์ใช้ AI
- ทีมงานด้านเทคนิคที่เกี่ยวข้องกับข้อมูลและ AI เช่นนักพัฒนาปัญญาประดิษฐ์ (AI Developer)
  นักวิเคราะห์ข้อมูล (Data Analyst)
  นักวิทยาศาสตร์ข้อมูล (Data Science)
  วิศวกรข้อมูล (Data Engineer)
- ทีมงานด้านเทคนิคอื่นที่เกี่ยวข้องกับการนำ AI ไปใช้งานจริง เช่น
  วิศวกรระบบ (System Engineer)
  วิศวกรซอฟต์แวร์ (Software Developer)
- หน่วยงานภายนอก* เช่น
  หน่วยงานที่รับจ้างพัฒนาระบบ (Vendor)
  ผู้ให้บริการโซลูชั่นด้าน AI (AI Solution Provider)

หมายเหตุ:

* บุคคลหรือกลุ่มบุคคลภายนอกที่อาจเข้ามาร่วมดำเนินงาน

ด้านการปฏิบัติงานตามกลยุทธ์ในการประยุกต์ใช้ AI

- จัดเตรียมข้อมูลสำหรับนำเสนอคณะกรรมการกำกับดูแลฯ เพื่อประกอบการกำหนดกลยุทธ์ในการประยุกต์ใช้ AI เช่น กระบวนการหรือขั้นตอนปฏิบัติที่สามารถนำ AI มาประยุกต์ใช้ ประโยชน์ที่จะได้รับ ระดับความสำเร็จที่คาดหวัง ความพร้อมขององค์กร ความซับซ้อนในการดำเนินการและเวลาที่ใช้ในการดำเนินการ หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้อง เป็นต้น
- จัดทำแผนปฏิบัติงานในการประยุกต์ใช้ AI (AI Roadmap) ตามกลยุทธ์ที่คณะกรรมการกำกับดูแลฯ กำหนด
- จัดทำสถาปัตยกรรมที่เกี่ยวข้องกับการประยุกต์ใช้ AI (AI Architecture) และจัดเตรียมทรัพยากรที่จำเป็นในการดำเนินงานตามแผนปฏิบัติงานในการประยุกต์ใช้ AI

ด้านการออกแบบ พัฒนา และนำ AI ไปประยุกต์ใช้

- ออกแบบโซลูชั่น พัฒนา ทดสอบ และนำ AI ไปใช้งาน พร้อมทั้งจัดทำเอกสารที่เกี่ยวข้อง
- จัดเตรียมข้อมูลและบริหารจัดการข้อมูลสำหรับทำงานร่วมกับ AI เพื่อให้ได้ข้อมูลที่มีคุณภาพและเหมาะสมในการใช้งานร่วมกับ AI
- จัดทำมาตรการในการรักษาความมั่นคงปลอดภัยและการคุ้มครองความเป็นส่วนตัว
- จัดให้มีช่องทางรับข้อคิดเห็น (Feedback) ประเด็นปัญหา (Issue) ความผิดพลาด (Error) จากการปฏิบัติงานและการให้บริการ พร้อมทั้งจัดให้มีมาตรการในการแก้ไขปัญหา และรับมือกับเหตุการณ์ผิดปกติ (Incident) ได้ทันท่วงทีเพื่อลดผลกระทบที่อาจเกิดขึ้น
- เฝ้าติดตามประสิทธิภาพการทำงานของ AI และระดับความสำเร็จในการประยุกต์ใช้ AI เพื่อนำเสนอคณะกรรมการกำกับดูแลฯ
- ประเมินผลการประยุกต์ใช้งาน AI ในปัจจุบัน และจัดทำข้อเสนอในการดำเนินงานในอนาคต เพื่อนำเสนอคณะกรรมการกำกับดูแลฯ

ระดับปฏิบัติการ (Implementation Level)

ด้านการปฏิบัติตามข้อกำหนดภายในและภายนอกองค์กร

- จัดทำขั้นตอนปฏิบัติ มาตรการ และเครื่องมือเพื่อควบคุมการปฏิบัติงานให้สอดคล้องตามนโยบายขององค์กร หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้อง
- เฝ้าติดตามผลการปฏิบัติงานตามข้อกำหนดทั้งภายในและภายนอกองค์กร เพื่อนำเสนอคณะกรรมการกำกับดูแลฯ
- ประเมินผลมาตรการในการกำกับดูแล และจัดทำข้อเสนอในการดำเนินงานในอนาคต เพื่อนำเสนอคณะกรรมการกำกับดูแลฯ

ด้านการควบคุมความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

- ประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประยุกต์ใช้ AI
- จัดทำมาตรการเพื่อควบคุมความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้
- กำหนดระดับการมีส่วนร่วมของมนุษย์ในการทำงานร่วมกับ AI เพื่อลดผลกระทบที่อาจเกิดขึ้น
- นำเสนอผลการดำเนินงานเกี่ยวกับการควบคุมความเสี่ยงต่อคณะกรรมการกำกับดูแลฯ

นอกจากการกำหนดหน้าที่และความรับผิดชอบดังกล่าวข้างต้น องค์กรยังจำเป็นต้องมี **การสื่อสารนโยบายและขั้นตอนปฏิบัติที่เกี่ยวข้อง พร้อมทั้งสร้างความตระหนักรู้ (Awareness) ต่อความรับผิดชอบ (Responsibility) และความรับผิดชอบต่อผลของการกระทำ (Accountability) ของแต่ละหน้าที่**

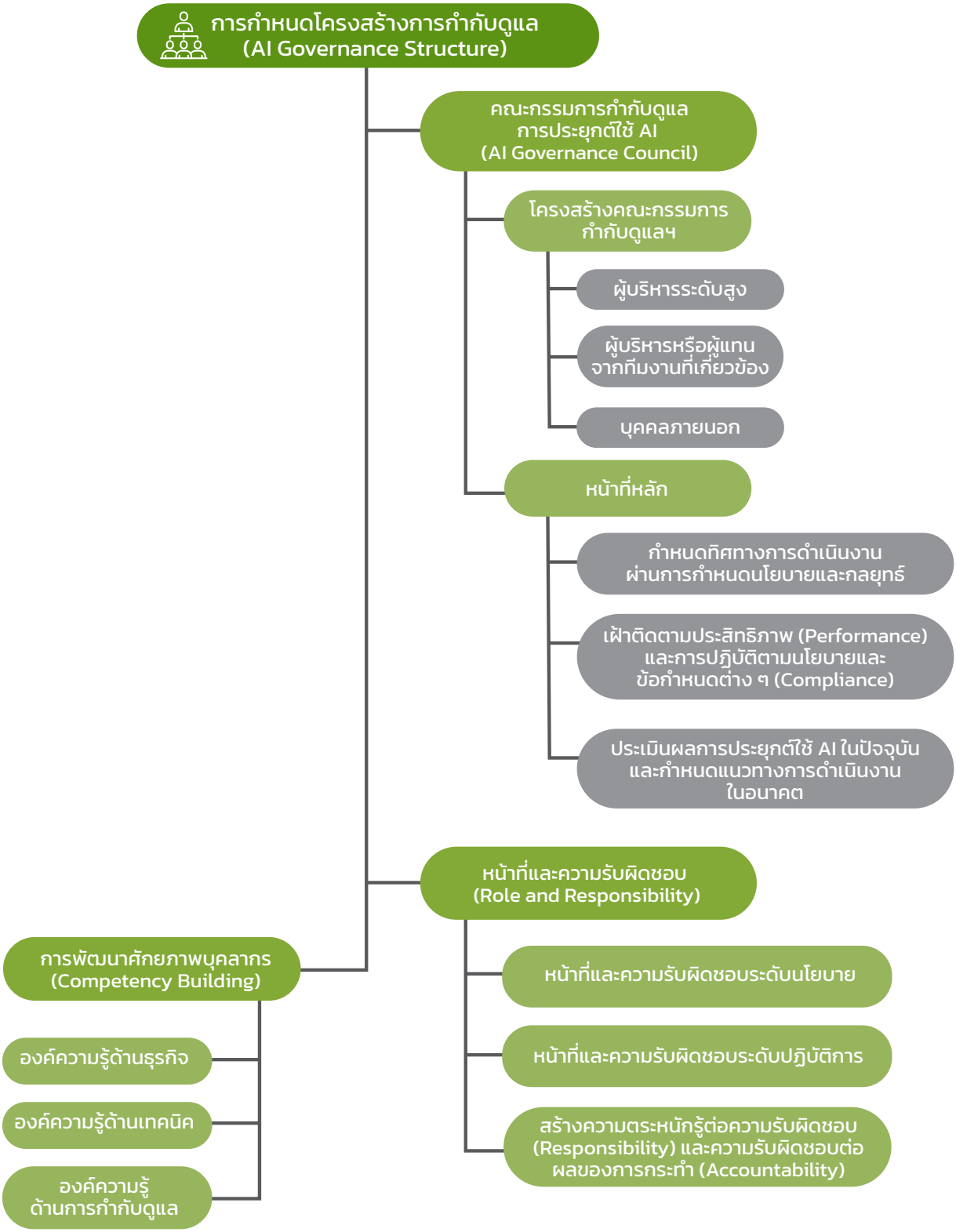
ในกรณีที่มีการว่าจ้างหน่วยงานภายนอก (Outsource) เช่น หน่วยงานที่รับจ้างพัฒนาระบบ (Vendor) ผู้ให้บริการโซลูชั่นด้าน AI (AI Solution Provider) เป็นต้น **องค์กรยังคงต้องมีความรับผิดชอบต่อผลของการกระทำ (Accountability) อันเกิดจากการทำงานของ AI ด้วยเหตุนี้ องค์กรจึงควรมีการกำกับดูแลการปฏิบัติงานของหน่วยงานภายนอกอย่างเหมาะสม พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบในข้อตกลงว่าจ้างหรือข้อตกลงการใช้บริการ**

5.3 การพัฒนาศักยภาพบุคลากร (Competency Building)

เพื่อให้องค์กรประสบความสำเร็จในการประยุกต์ใช้ AI **คณะกรรมการกำกับดูแลฯ รวมถึงบุคลากรและผู้มีส่วนได้เสียที่เกี่ยวข้อง ควรได้รับการส่งเสริมให้มีความรู้ความเข้าใจเกี่ยวกับ AI ในมิติต่าง ๆ อย่างเหมาะสมตามหน้าที่ที่ได้รับมอบหมาย** เพื่อให้สามารถปฏิบัติหน้าที่ได้อย่างถูกต้องและสอดคล้องตามนโยบายขององค์กร หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้อง รวมถึงสามารถรับมือกับความเสี่ยงและเหตุการณ์ผิดปกติได้อย่างเหมาะสม



ภาพสรุปองค์ประกอบสำคัญของการกำหนดโครงสร้างการกำกับดูแล (AI Governance Structure)





06

การกำหนดกลยุทธ์ในการประยุกต์ใช้ AI

(AI Strategy)

6.1 การกำหนดกลยุทธ์ในการประยุกต์ใช้ AI อย่างมีความรับผิดชอบ
(Responsible AI Strategy)

ปัจจุบันเทคโนโลยี AI ถูกนำมาประยุกต์ใช้ในรูปแบบที่หลากหลายแตกต่างกันตามวัตถุประสงค์หรือเป้าหมายขององค์กร เพื่อให้การประยุกต์ใช้ AI ประสบความสำเร็จและบรรลุตามเป้าหมาย องค์กรจึงควรกำหนดกลยุทธ์ในการประยุกต์ใช้ AI และแผนปฏิบัติงานอย่างเหมาะสม โดย **พิจารณาถึงโอกาสหรือประโยชน์ที่องค์กรจะได้รับและพิจารณาความเป็นไปได้ในการประยุกต์ใช้ AI**

- มองหาโอกาสในการนำ AI มาประยุกต์ใช้
- กำหนดเป้าหมายในการประยุกต์ใช้ AI ตามลำดับความสำคัญและความพร้อมขององค์กร
- กำหนดกลยุทธ์ในการบริหารจัดการข้อมูลเพื่อสนับสนุนการประยุกต์ใช้ AI
- จัดทำแผนปฏิบัติงาน (Roadmap) ในการประยุกต์ใช้ AI

โดยในการพิจารณาความเป็นไปได้นั้น องค์กรควรพิจารณาถึงปัจจัยในด้านต่าง ๆ เช่น ความสามารถของเทคโนโลยีและผลิตภัณฑ์ในปัจจุบันที่สามารถตอบโจทย์ความต้องการขององค์กร ความพร้อมของข้อมูลและทรัพยากรที่เกี่ยวข้อง ความซับซ้อนและเวลาที่ใช้ดำเนินการ ข้อจำกัดและความท้าทายในการดำเนินงาน เป็นต้น

นอกจากนี้ เพื่อให้เกิดการประยุกต์ใช้งาน AI อย่างมีความรับผิดชอบ ในการกำหนดกลยุทธ์ยังจำเป็นต้องมีการ**พิจารณาและคาดการณ์ถึงผลกระทบเชิงลบที่อาจส่งผลกระทบต่อบุคคลที่เกี่ยวข้อง องค์กร หรือสังคมโดยกว้าง** เช่น การตัดสินใจของ AI ที่มีอคติจนนำไปสู่การเลือกปฏิบัติ การทำงานที่ผิดพลาดของ AI ก่อให้เกิดความเสียหายต่อชื่อเสียง ชีวิต หรือทรัพย์สิน เป็นต้น ด้วยเหตุนี้ องค์กรจึงควรมีการกำหนดกลยุทธ์และจัดทำแผนปฏิบัติงานเพื่อให้ระบบหรือบริการที่เกี่ยวข้องกับ AI ทำงานได้อย่างสอดคล้องตามหลักการจริยธรรม ปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้อง พร้อมทั้งลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นดังกล่าว

มองหาโอกาสในการนำ AI มาประยุกต์ใช้

เพื่อให้เห็นโอกาสในการนำ AI มาประยุกต์ใช้ องค์กรจึงควรเริ่มต้นจากการ**ทำความเข้าใจภาพรวม วิสัยทัศน์ พันธกิจ รวมถึงเป้าหมายระยะสั้นและระยะยาวขององค์กร เพื่อเข้าใจเป้าหมายขององค์กรหรือเป้าหมายในการดำเนินธุรกิจ จากนั้นจึงเริ่มทำการวิเคราะห์กระบวนการหรือขั้นตอนปฏิบัติต่าง ๆ เพื่อมองหาโอกาสที่ AI จะเข้ามาเป็นองค์ประกอบหนึ่งในการทำงาน ซึ่งจะช่วยให้องค์กรบรรลุตามเป้าหมายหรือตอบโจทย์ความต้องการทางธุรกิจได้อย่างมีประสิทธิภาพมากยิ่งขึ้น** โดยในการวิเคราะห์นั้นอาจพิจารณาในประเด็นดังต่อไปนี้

- **ประโยชน์ที่องค์กรจะได้รับจากการนำ AI มาประยุกต์ใช้** เช่น เพิ่มรายได้ให้แก่องค์กร การยกระดับความพึงพอใจของลูกค้า ปรับปรุงประสิทธิภาพและผลิตผล ลดค่าใช้จ่ายในการปฏิบัติงาน เป็นต้น
- **ระดับความสำเร็จที่คาดหวัง**ว่า AI จะเข้ามาช่วยให้องค์กรบรรลุเป้าหมายในการดำเนินธุรกิจ หรือความสำเร็จตามตัวชี้วัดที่องค์กรกำหนด (Key Performance Indicator: KPI) เช่น สามารถผลิตสินค้าได้มากขึ้น 500 ชิ้น/วัน สามารถช่วยลดค่าใช้จ่ายลงได้ 20% เป็นต้น
- **เทคโนโลยีและวิธีการที่จะนำ AI มาประยุกต์ใช้**
- **ขอบเขตการดำเนินงาน**ที่ AI จะเข้าไปเกี่ยวข้องกับการปฏิบัติงาน
- **ข้อมูลและทรัพยากรที่จำเป็น**ต้องใช้ในการดำเนินการ เช่น งบประมาณ บุคลากร โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ เป็นต้น
- **ผลกระทบจากการนำ AI ไปประยุกต์ใช้** เช่น การปรับเปลี่ยนกระบวนการหรือขั้นตอนปฏิบัติ ผลกระทบต่อผู้มีส่วนได้เสีย ความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประยุกต์ใช้ AI และมาตรการในการควบคุมความเสี่ยงและผลกระทบดังกล่าว เป็นต้น
- **ข้อจำกัดหรือความท้าทายในการประยุกต์ใช้ AI** เช่น กฎหมายและข้อกำหนดที่ต้องปฏิบัติตาม ข้อจำกัดด้านทรัพยากร ปริมาณและคุณภาพของข้อมูลที่มีอยู่ในปัจจุบัน เป็นต้น

โดยในการวิเคราะห์กระบวนการหรือขั้นตอนปฏิบัติต่าง ๆ นั้น ควรมีการทำงานร่วมกันระหว่างผู้เชี่ยวชาญด้าน AI และทีมงานด้านธุรกิจหรือผู้ที่เกี่ยวข้องกับการปฏิบัติงานโดยตรง เพื่อสะท้อนมุมมองในทางปฏิบัติและวิเคราะห์ความเป็นไปได้ในการที่จะนำ AI มาประยุกต์ใช้

กำหนดเป้าหมายในการประยุกต์ใช้ AI

ภายหลังจากทำการวิเคราะห์กระบวนการหรือขั้นตอนปฏิบัติเพื่อมองหาโอกาสและความเป็นไปได้ที่จะนำ AI มาประยุกต์ใช้นั้น **องค์กรอาจพบว่ามีกระบวนการหรือขั้นตอนปฏิบัติจำนวนมาก หลากหลาย และอาจไม่สามารถดำเนินการไปพร้อมกันได้ทั้งหมด** ด้วยเหตุนี้ **องค์กรจึงจำเป็นต้องจัดลำดับความสำคัญในการดำเนินงาน** โดยอาจพิจารณาจากปัจจัยต่าง ๆ ได้แก่

- **ประโยชน์ที่องค์กรจะได้รับ** จากการนำ AI มาประยุกต์ใช้ในกระบวนการหรือขั้นตอนปฏิบัตินั้น
- **ระดับความสำเร็จที่คาดหวัง**ว่า AI จะเข้ามาช่วยให้บรรลุตามเป้าหมายขององค์กร เป้าหมายในการดำเนินธุรกิจ หรือความสำเร็จตามตัวชี้วัดที่องค์กรกำหนด (Key Performance Indicator: KPI)
- **หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนด**ที่ต้องออกแบบและพัฒนาระบบให้สอดคล้อง
- **ความพร้อมของทรัพยากร** ที่จำเป็นต้องใช้ในการดำเนินการ เช่น งบประมาณ ข้อมูล บุคลากร โครงสร้างพื้นฐานเทคโนโลยี สารสนเทศ เป็นต้น
- **ความพร้อมในการกำกับดูแลและการปฏิบัติงาน**เพื่อเปลี่ยนผ่านไปสู่การนำ AI มาประยุกต์ใช้จริง รวมถึงการรับมือความเสี่ยงและผลกระทบที่อาจเกิดขึ้น
- **ความซับซ้อนและเวลาที่ใช้**ในการดำเนินการ

ซึ่งการจัดลำดับความสำคัญในการดำเนินงานดังกล่าว จะช่วยให้องค์กรสามารถเลือกเป้าหมายในการประยุกต์ใช้งาน AI ตามลำดับความสำคัญ และสามารถจัดสรรทรัพยากรได้อย่างมีประสิทธิภาพ

กำหนดกลยุทธ์ในการบริหารจัดการข้อมูลเพื่อสนับสนุนการประยุกต์ใช้ AI

เนื่องจาก AI จำเป็นต้องใช้ข้อมูลในการประมวลผล ด้วยเหตุนี้ องค์กรจึงจำเป็นต้องมีการ**กำหนดกลยุทธ์ในการบริหารจัดการข้อมูล อย่างเหมาะสม ตั้งแต่กระบวนการสรรหาแหล่งข้อมูลที่เหมาะสม การจัดเตรียมข้อมูลให้อยู่ในรูปแบบที่พร้อมใช้งานและเพียงพอสำหรับ AI ในการประมวลผล ไปจนถึงการพัฒนาอัลกอริทึม ให้สามารถทำงานได้อย่างมีประสิทธิภาพบนพื้นฐานของข้อมูลที่มีอยู่**

เพื่อให้มั่นใจได้ว่าองค์กรจะมีข้อมูลที่เหมาะสมและเพียงพอต่อการสนับสนุนการประยุกต์ใช้ AI ให้บรรลุตามเป้าหมายที่กำหนด **องค์กรควรมีการสรรหาแหล่งข้อมูลที่เหมาะสม** โดยอาจพิจารณาจากคุณภาพของข้อมูล ความน่าเชื่อถือในการเก็บรวบรวมข้อมูล ความสามารถในการเข้าถึงข้อมูลได้โดยสะดวก ข้อมูลอยู่ในรูปแบบหรือประเภทที่ตรงตามความต้องการใช้งาน ข้อมูลมีความหลากหลายและครอบคลุมตัวอย่างที่ต้องการ มีขนาดของข้อมูลหรือขนาดของกลุ่มตัวอย่างที่เหมาะสม ข้อมูลมีการปรับปรุงให้ทันสมัยอยู่เสมอ เป็นต้น

นอกจากนี้องค์กรยังจำเป็นต้องมีการ**เตรียมความพร้อมในด้านบุคลากร เครื่องมือและกระบวนการอย่างเหมาะสม** เพื่อจัดเตรียมข้อมูลที่เหมาะสมสำหรับการพัฒนา ทดสอบและใช้งาน AI (ซึ่งจะกล่าวถึงในหัวข้อ 7.1) รวมถึง**ควรมีการกำกับดูแลโดยนำหลักการธรรมาภิบาลข้อมูล (Data Governance) มาปรับใช้** เพื่อให้มั่นใจได้ว่าข้อมูลมีคุณภาพตรงตามความต้องการในการใช้งาน

ข้อมูล คือ อาหารของ AI หากองค์กรใช้ข้อมูลที่ไม่มีคุณภาพในการสอน AI ผลลัพธ์จากการทำงานหรือการตัดสินใจของ AI ก็จะไม่มีคุณภาพเช่นกัน

จัดทำแผนปฏิบัติงาน (Roadmap) ในการประยุกต์ใช้ AI

ภายหลังจากที่องค์กรสามารถกำหนดเป้าหมายในการประยุกต์ใช้งาน AI รวมถึงแนวทางการบริหารจัดการข้อมูลที่สอดคล้องตามกลยุทธ์ที่วางไว้แล้ว **องค์กรควรจัดทำแผนปฏิบัติงานตามลำดับความสำคัญ พร้อมทั้งกำหนดขั้นตอนการดำเนินงานและระยะเวลาในการดำเนินงานของแต่ละเป้าหมาย** เช่น การจัดเตรียมข้อมูล การพัฒนา ทดสอบ และการนำ AI ไปใช้งาน เป็นต้น

นอกจากนี้ **องค์กรอาจกำหนดให้มีการจัดทำระบบต้นแบบ (Prototype) ก่อนนำไปขยายผลเพื่อใช้งานจริง** เพื่อทดสอบและประเมินประสิทธิภาพในการทำงานของ AI พร้อมทั้งประเมินความคุ้มค่าในการลงทุน วิเคราะห์ปัญหาและอุปสรรคที่อาจเกิดขึ้นเมื่อนำ AI ไปประยุกต์ใช้ในสภาพแวดล้อมการใช้งานจริง



6.2 การบริหารจัดการความเสี่ยงจากการประยุกต์ใช้ AI

(AI Risk Management)

การประยุกต์ใช้ AI อาจนำมาซึ่งโอกาสใหม่ในการดำเนินธุรกิจหรือสร้างประโยชน์ให้แก่องค์กร แต่ในขณะเดียวกันการประยุกต์ใช้ AI ก็อาจก่อให้เกิดผลกระทบเชิงลบต่อบุคคลที่เกี่ยวข้อง องค์กร และสังคมโดยกว้างได้เช่นกัน ด้วยเหตุนี้ ในระหว่างการกำหนดกลยุทธ์และเป้าหมายในการประยุกต์ใช้ AI นั้น **องค์กรจึงจำเป็นต้องมีการประเมินความเสี่ยงเพื่อให้เห็นถึงความไม่แน่นอนหรือโอกาสที่การประยุกต์ใช้ AI จะไม่เป็นไปตามเป้าหมายที่กำหนด รวมถึงเห็นผลกระทบเชิงลบที่อาจเกิดขึ้น**

ทั้งนี้ ความเสี่ยงจากการประยุกต์ใช้ AI นั้น มีความหลากหลายและแตกต่างกันไปตามบริบทของการประยุกต์ใช้ AI ตัวอย่างเช่น

- **ความเสี่ยงด้านคุณภาพข้อมูล (Data Quality)** – เป็นความเสี่ยงที่ข้อมูลขององค์กรมีคุณภาพไม่เพียงพอ จนส่งผลให้การทำงานของ AI ไม่มีประสิทธิภาพตามเป้าหมายที่กำหนดหรือทำงานผิดพลาด เป็นต้น

- **ความเสี่ยงด้านความไม่เป็นธรรมและการเลือกปฏิบัติ (Unfairness and Discrimination)** – เป็นความเสี่ยงที่ผลลัพธ์จากการทำงานของ AI นำไปสู่ความไม่เป็นธรรมและการเลือกปฏิบัติ ซึ่งอาจเกิดจากอคติที่มาจากการออกแบบและสร้างโมเดล (Bias Introduced by Engineering Decisions) หรือเกิดจากอคติที่มาจากข้อมูล (Data Bias) เช่น การใช้ข้อมูลที่ไม่มีความหลากหลายหรือเอนเอียงมาสอน AI เป็นต้น

- **ความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cyber Attack)** – เป็นความเสี่ยงที่ AI ถูกโจมตี โดยมีวัตถุประสงค์ให้ AI ทำงานผิดพลาด หยุดการทำงาน หรือเกิดการรั่วไหลของข้อมูล เป็นต้น โดยอาศัยช่องโหว่ (Vulnerability) ของระบบ AI หรือ โจมตีข้อมูลที่ใช้ในการสอน AI โดยทำให้ข้อมูลปนเปื้อนด้วยข้อมูลที่ทำให้เกิดช่องโหว่

- **ความเสี่ยงด้านการคุ้มครองความเป็นส่วนตัว (Privacy)** – เป็นความเสี่ยงที่ข้อมูลส่วนบุคคลถูกละเมิด โดยอาจเกิดจากการมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เหมาะสม ความผิดพลาดในการปฏิบัติงาน หรือถูกโจมตีโดยผู้ประสงค์ร้าย เป็นต้น
- **ความเสี่ยงด้านการไม่ปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง (Non-compliance)** – เป็นความเสี่ยงที่ผลลัพธ์จากการทำงานของ AI นำไปสู่การละเมิดกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง
- **ความเสี่ยงด้านความน่าเชื่อถือหรือชื่อเสียง (Trust and Reputation)** – เป็นความเสี่ยงที่เกิดจากการทำงานหรือการตัดสินใจของ AI ทำงานผิดพลาดหรือก่อให้เกิดผลกระทบเชิงลบ เช่น AI ทำงานผิดพลาดเมื่ออยู่ในสถานการณ์ที่ไม่เคยถูกทดสอบหรือต้องตัดสินใจบนพื้นฐานข้อมูลที่ไม่เคยได้รับการสอนมาก่อน เป็นต้น

เพื่อลดความเสี่ยงและผลกระทบเชิงลบจากการประยุกต์ใช้ AI ดังกล่าว **องค์กรจึงจำเป็นต้องมีการบริหารจัดการความเสี่ยง (Risk Management) เพื่อควบคุมความเสี่ยงในทุกกิจกรรมตลอดวงจรชีวิตของ AI (AI Lifecycle) ให้อยู่ในขอบเขตที่ยอมรับได้**



ในการบริหารจัดการความเสี่ยงนั้น องค์กรจำเป็นต้องมีการ**กำหนดนโยบาย กระบวนการ ขั้นตอนปฏิบัติ และมาตรการเพื่อควบคุมความเสี่ยงที่อาจเกิดขึ้นในแต่ละกิจกรรมตลอดวงจรชีวิตของ AI ซึ่งกระบวนการในการบริหารจัดการความเสี่ยงนั้น** ประกอบด้วย 6 กระบวนการหลัก ได้แก่

1. การสื่อสารและหารือร่วมกัน (Communication and Consultation) ระหว่างบุคลากรภายในองค์กรและผู้มีส่วนได้เสียที่เกี่ยวข้องกับการประยุกต์ใช้ AI

2. การทำความเข้าใจขอบเขตและบริบทของการประยุกต์ใช้ AI รวมถึงกำหนดเกณฑ์ในการประเมินความเสี่ยง (Risk Criteria)

3. การประเมินความเสี่ยง (Risk Assessment) เพื่อให้องค์กรมองเห็นความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประยุกต์ใช้ AI รวมถึงมาตรการในการควบคุมความเสี่ยงดังกล่าว

4. การกำหนดมาตรการที่เหมาะสมในการควบคุมและแก้ไขความเสี่ยง (Risk Treatment) รวมถึงจัดทำแผนการดำเนินการเพื่อควบคุมและแก้ไขความเสี่ยง (Risk Treatment Plan) ดังกล่าว เพื่อควบคุมความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้ นอกจากนี้ การกำหนดมาตรการในการควบคุมและแก้ไขความเสี่ยงจะต้องครอบคลุมถึงการปฏิบัติงานของหน่วยงานภายนอก เช่น หน่วยงานที่รับจ้างพัฒนาระบบ (Vendor) ผู้ให้บริการโซลูชั่นด้าน AI (AI Solution Provider) เป็นต้น และครอบคลุมถึงเครื่องมือหรือผลิตภัณฑ์ AI ที่ใช้งาน เพื่อควบคุมความเสี่ยงที่อาจเกิดขึ้นจากบุคคลหน่วยงานภายนอก

5. การเฝ้าติดตามและทบทวน (Monitoring and Review) ประสิทธิภาพในการควบคุมและแก้ไขความเสี่ยงที่เกิดขึ้น

6. การบันทึกและรายงานผลการบริหารจัดการความเสี่ยง (Recording & Reporting) ต่อคณะกรรมการกำกับดูแลฯ บุคลากร และผู้มีส่วนได้เสียที่เกี่ยวข้อง เพื่อประเมินผลการปฏิบัติงาน (Evaluation) และปรับปรุงประสิทธิภาพในการบริหารจัดการและควบคุมความเสี่ยง

ตัวอย่างกรอบแนวทางการบริหารจัดการความเสี่ยงจากการประยุกต์ใช้ AI (AI Risk Management Framework)

จากกระบวนการในการบริหารจัดการความเสี่ยงข้างต้น องค์กรอาจพิจารณานำกรอบแนวทางการบริหารจัดการความเสี่ยงที่ประกาศโดยหน่วยงานด้านมาตรฐานสากลมาปรับใช้ โดยในปี 2023 องค์กร International Organization for Standardization (ISO) ซึ่งเป็นองค์กรระหว่างประเทศด้านมาตรฐาน และสถาบัน National Institute of Standards and Technology (NIST) ซึ่งเป็นสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา ได้มีการประกาศมาตรฐาน

1) **ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management ซึ่งเป็นส่วนขยาย (Extension) จากมาตรฐาน ISO 31000:2018 Risk management** — Guidelines ที่อธิบายรายละเอียดเพิ่มเติมในส่วนของการบริหารจัดการความเสี่ยงจากการประยุกต์ใช้ AI

2) **Artificial Intelligence Risk Management Framework (AI RMF 1.0)** โดย NIST

ซึ่งทั้ง 2 มาตรฐานดังกล่าว ได้มีการวางแนวปฏิบัติในการบริหารจัดการความเสี่ยงจากการประยุกต์ใช้ AI เป็นการเฉพาะ เพื่อให้องค์กรมีความเข้าใจและตระหนักถึงความเสี่ยงรูปแบบใหม่ที่เกิดจากการประยุกต์ใช้ AI รวมถึงใช้เป็นแนวทางในการรับมือกับความเสี่ยงที่จะมาเปลี่ยนแปลงสังคมและบริบทของการดำรงชีวิตของมนุษย์ในอนาคต

ระดับการมีส่วนร่วมของมนุษย์ (Level of Human Involvement)

เนื่องจาก บริบทของการประยุกต์ใช้ AI นั้นมีความหลากหลาย **ความผิดพลาดในการทำงานหรือการตัดสินใจของ AI อาจก่อให้เกิดผลกระทบเชิงลบในระดับที่แตกต่างกันไปตามบริบทของการประยุกต์ใช้** ตัวอย่างเช่น

- ความผิดพลาดของระบบวินิจฉัยโรค อาจส่งผลให้คนไข้ไม่ได้รับการรักษาอย่างทันท่วงทีและอาจนำไปสู่อันตรายต่อชีวิต
- ระบบควบคุมคุณภาพสินค้า (Quality Control) วิเคราะห์คุณภาพสินค้าผิดพลาด ทำให้สินค้าถูกส่งคืนและส่งผลให้องค์กรสูญเสีย ชื่อเสียง และความน่าเชื่อถือ
- ระบบช่วยตอบคำถามลูกค้า (Chatbot) ไม่สามารถตอบคำถามลูกค้าได้อย่างถูกต้อง จนทำให้ลูกค้าส่วนใหญ่ไม่พอใจในการให้บริการ
- แพลตฟอร์มขายของออนไลน์แนะนำสินค้าตามพฤติกรรมหรือประวัติการซื้อสินค้าที่ผ่านมา ทำให้ผู้ซื้อไม่สามารถเห็นสินค้าประเภทอื่นที่ตนสนใจได้

ซึ่งจากกรณีตัวอย่างข้างต้น **ผลกระทบเชิงลบที่อาจเกิดขึ้นมีความแตกต่างกันตามบริบทของการประยุกต์ใช้ AI** เช่น ผลกระทบต่อชีวิตและร่างกาย ทรัพย์สิน ความพึงพอใจของลูกค้า ความน่าเชื่อถือและชื่อเสียงขององค์กร เป็นต้น **นอกจากนี้ ขนาดของผู้ได้รับผลกระทบอาจแตกต่างกันไปตามบริบทด้วยเช่นกัน** โดยในบางกรณีอาจส่งผลกระทบเป็นรายบุคคลหรือองค์กร แต่ในบางกรณีนั้นอาจส่งผลกระทบถึงกลุ่มบุคคลและสังคมโดยกว้างได้เช่นกัน

ด้วยเหตุนี้ การอนุญาตให้ AI ทำงานหรือตัดสินใจในบริบทที่อาจส่งผลกระทบต่อชีวิตและร่างกาย หรือก่อความเสียหายแก่ทรัพย์สินที่มีมูลค่าสูง รวมถึงในกรณีที่อาจส่งผลกระทบต่อกลุ่มบุคคลหรือสังคมในวงกว้าง อาจทำให้ผู้ใช้งานหรือผู้มีส่วนได้เสียที่เกี่ยวข้องเกิดความกังวล และไม่เชื่อมั่นในการประยุกต์ใช้ AI ขององค์กร

ดังนั้น **การเข้ามามีส่วนร่วมของมนุษย์ในการควบคุมการทำงานหรือตัดสินใจของ AI จึงเป็นหนึ่งในมาตรการที่จะช่วยควบคุมและแก้ไขความเสี่ยง (Risk Treatment) รวมถึงบรรเทาผลกระทบเชิงลบที่อาจเกิดขึ้น อีกทั้งยังเป็นการสร้างความเชื่อมั่นในการประยุกต์ใช้ AI และสร้างการยอมรับจากบุคคลที่เกี่ยวข้องได้**

การเข้ามามีส่วนร่วมของมนุษย์ในการควบคุมการทำงาน หรือตัดสินใจของ AI นั้นอาจแบ่งออกได้เป็น 3 ระดับ ได้แก่

Human-in-the-loop

เป็นระดับการมีส่วนร่วมที่มนุษย์ควบคุมการทำงานหรือตัดสินทั้งหมด โดยมี AI ทำหน้าที่ในการให้คำแนะนำหรือข้อมูล แต่ไม่สามารถทำงานหรือตัดสินใจในการดำเนินการใด ๆ ได้ โดยปราศจากมนุษย์

ตัวอย่างเช่น

ในกรณีของการวินิจฉัยโรคนั้น AI จะช่วยวิเคราะห์โอกาสการเป็นโรค พร้อมทั้งนำเสนอข้อมูลที่เป็นประโยชน์แก่แพทย์ในการวินิจฉัยและกำหนดแนวทางการรักษาต่อไป

ซึ่งจากกรณีดังกล่าว หาก AI วินิจฉัยโรคผิดพลาด การวินิจฉัยของแพทย์จะช่วยลดโอกาสและผลกระทบที่อาจนำไปสู่อันตรายต่อชีวิต ซึ่งเป็นความเสียหายที่ไม่อาจแก้ไขให้กลับคืนมาเหมือนเดิมได้

Human-over-the-loop

เป็นระดับการมีส่วนร่วมที่ AI สามารถทำงานหรือตัดสินใจได้โดยอัตโนมัติ (ไม่ต้องรอการตัดสินใจจากมนุษย์) แต่ยังคงจำเป็นต้องมีมนุษย์ในการกำกับดูแล อีกทั้งมนุษย์ยังสามารถเข้าควบคุมหรือระงับการทำงานได้ หากพบความผิดพลาดหรือเกิดเหตุการณ์ที่อาจก่อให้เกิดผลกระทบเชิงลบ

ตัวอย่างเช่น

กรณีของระบบควบคุมคุณภาพสินค้านั้น AI สามารถคัดแยกสินค้าที่ไม่ผ่านคุณภาพได้โดยไม่ต้องรอการตัดสินใจจากมนุษย์ แต่ระบบยังคงอนุญาตให้มนุษย์สามารถระงับการทำงานได้ หากพบว่าระบบไม่สามารถคัดแยกสินค้าที่ไม่ผ่านคุณภาพได้ตามที่กำหนด โดยในกรณีดังกล่าว การทำงานของ AI ยังคงอยู่ภายใต้การกำกับดูแลของมนุษย์ อีกทั้ง ยังสามารถระงับเหตุเพื่อแก้ไขปัญหาและคัดแยกสินค้าที่ไม่ได้คุณภาพก่อนส่งถึงมือลูกค้าได้

Human-out-of-the-loop

เป็นระดับการมีส่วนร่วมที่ AI ควบคุมการทำงานหรือตัดสินทั้งหมดได้ โดยมนุษย์ไม่สามารถเข้าควบคุม แทรกแซง หรือระงับการทำงานได้

ตัวอย่างเช่น

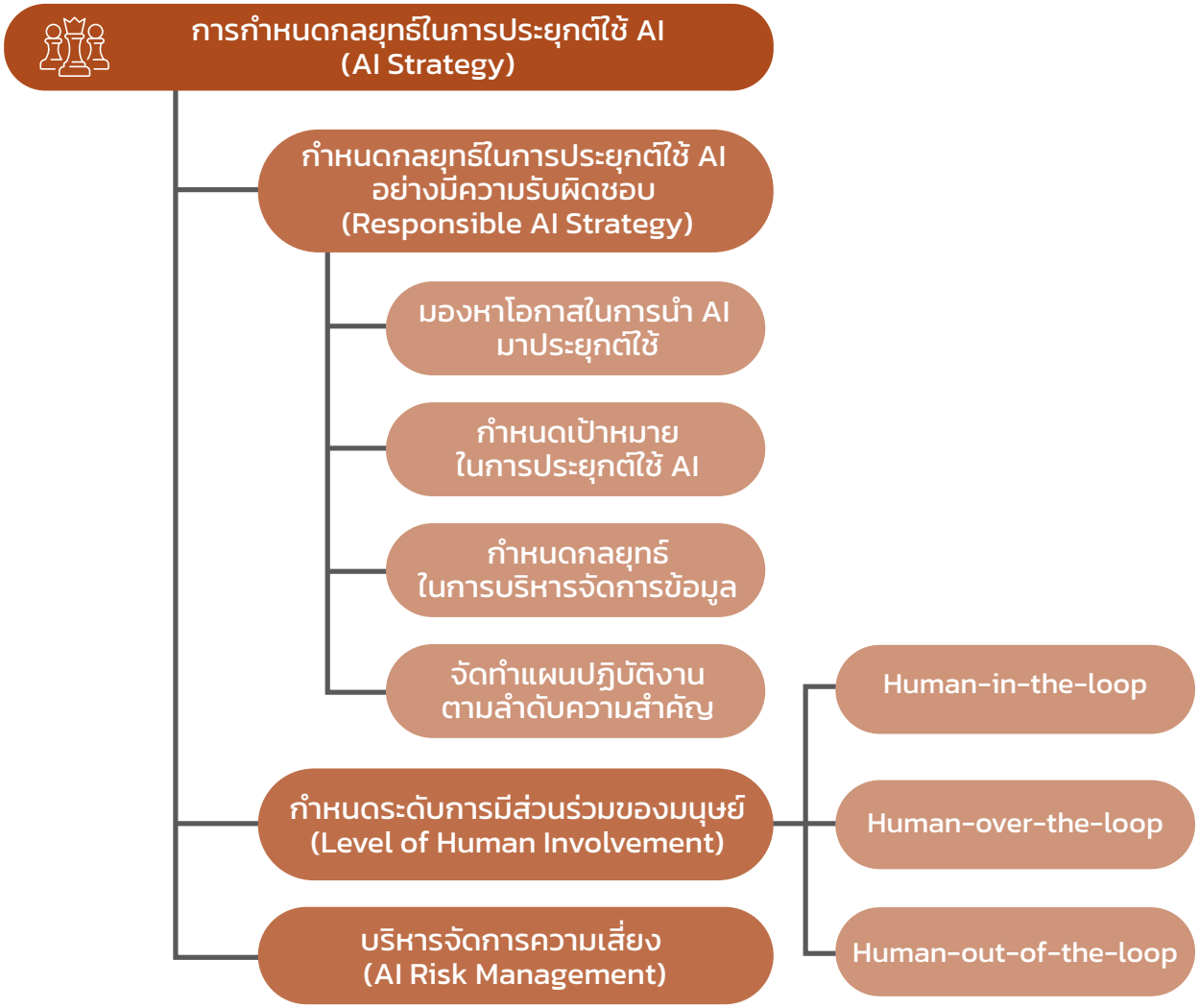
ในกรณีของระบบช่วยตอบคำถามลูกค้า (Chatbot) และการแนะนำสินค้าบนแพลตฟอร์มขายของออนไลน์นั้น องค์กรมีความประสงค์ที่จะประยุกต์ใช้ AI เพื่อตอบสนองความต้องการของลูกค้าได้อย่างทันท่วงที โดยไม่จำเป็นต้องรอการตัดสินใจจากมนุษย์

โดยทั้ง 2 กรณีข้างต้น มนุษย์อาจไม่สามารถเข้าไปแทรกแซงการทำงานของ AI และไม่สามารถติดต่อกับลูกค้าหรือผู้ซื้อโดยตรงได้ ดังนั้น เพื่อลดผลกระทบจากความไม่พอใจต่อระบบช่วยตอบคำถาม องค์กรจึงควรมีการเปิดให้มีช่องทางอื่นเพื่อให้ลูกค้าสามารถติดต่อพนักงานที่เป็นมนุษย์ได้โดยตรง หรือในกรณีที่ผู้ซื้อไม่สามารถเห็นสินค้าประเภทอื่นที่สนใจได้นั้น องค์กรอาจลดผลกระทบดังกล่าวโดยอนุญาตให้ผู้ซื้อปิดฟังก์ชันการนำเสนอสินค้าได้ด้วยตนเอง

จากตัวอย่างของการมีส่วนร่วมของมนุษย์ทั้ง 3 ระดับ จะพบว่า**ปัจจัยในการพิจารณาเลือกระดับการมีส่วนร่วมของมนุษย์นั้น มีความหลากหลายแตกต่างกันไปตามบริบทของการประยุกต์ใช้ AI ซึ่งองค์กรจำเป็นต้องมีการพิจารณาเลือกระดับการมีส่วนร่วมของมนุษย์อย่างเหมาะสม** โดยอาจพิจารณาจากปัจจัย ดังต่อไปนี้

1. ระดับความเสี่ยงที่อาจส่งผลกระทบเชิงลบ
2. ความรุนแรงของผลกระทบเชิงลบที่อาจเกิดขึ้น
3. ผลกระทบที่เกิดขึ้นนั้นสามารถย้อนกลับไปแก้ไขได้หรือไม่
4. ความเป็นไปได้หรือความเหมาะสมในการเข้าไปแทรกแซงการทำงานโดยมนุษย์

ภาพสรุปองค์ประกอบสำคัญของการกำหนดกลยุทธ์ในการประยุกต์ใช้ AI (AI Strategy)





07

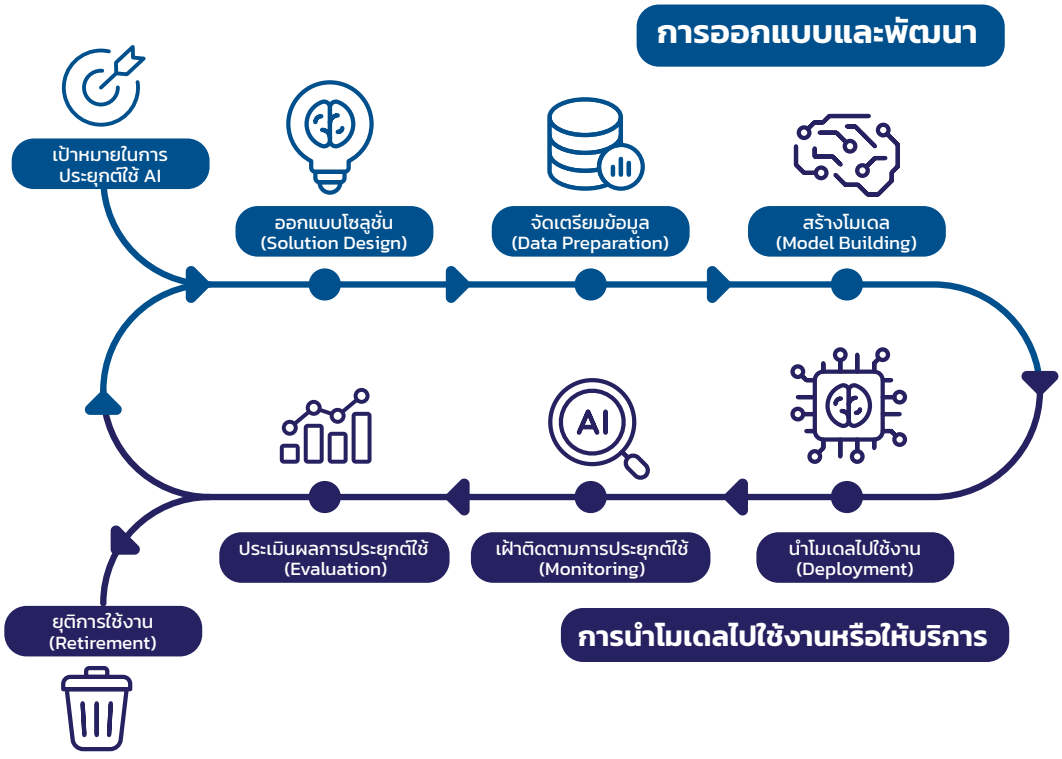
การกำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับ AI

(AI Operation)

7.1 การกำกับดูแลตลอดวงจรชีวิตของ AI (AI Lifecycle)

ความสามารถของ AI ที่หลากหลายนั้นมีเบื้องหลังมาจากความสามารถของโมเดลปัญญาประดิษฐ์ (AI Model) (ซึ่งต่อไปในเอกสารนี้จะเรียกว่า "โมเดล") ที่สร้างขึ้นจากอัลกอริทึมและข้อมูลที่สอนโดยมนุษย์ (เฉพาะในกรณีของ AI ประเภท Machine Learning เท่านั้น ที่จำเป็นต้องมีการเรียนรู้จากข้อมูลที่สอนโดยมนุษย์) ด้วยเหตุนี้ **ประสิทธิภาพในการประมวลผลของ AI เช่น ระดับความถูกต้อง (Accuracy) ความแม่นยำ (Precision) และระดับความน่าเชื่อถือในการตัดสินใจ (Level of Confidence) เป็นต้น จึงขึ้นอยู่กับประสิทธิภาพของอัลกอริทึมและคุณภาพของข้อมูลที่ใช้ในการสอน AI** เป็นสำคัญ

ด้วยเหตุนี้ **การกำกับดูแลการประยุกต์ใช้ AI ตลอดวงจรชีวิต (AI Lifecycle) ตั้งแต่ระยะเริ่มต้นของการออกแบบและพัฒนาไปจนถึงการนำโมเดลไปใช้งานหรือให้บริการ** จึงมีความสำคัญอย่างยิ่งในการทำให้ AI มีประสิทธิภาพสอดคล้องตามเป้าหมายที่กำหนดและมีความรับผิดชอบ ซึ่งในการกำกับดูแลนั้นควรมีการกำกับดูแลการปฏิบัติงานในกระบวนการต่าง ๆ ได้แก่ กระบวนการออกแบบโซลูชั่น จัดเตรียมข้อมูล สร้างโมเดล นำโมเดลไปใช้งาน เฝ้าติดตามและประเมินผลการประยุกต์ใช้ AI ไปจนถึงยุติการใช้งาน



ออกแบบโซลูชั่น (Solution Design)

เพื่อให้การประยุกต์ใช้ AI บรรลุตามเป้าหมายอย่างมีความรับผิดชอบต่อบุคคลที่เกี่ยวข้อง องค์กร และสังคมโดยกว้าง **องค์กรจำเป็นต้องวิเคราะห์ (1) เป้าหมายในการประยุกต์ใช้ AI (2) หลักการจริยธรรมปัญญาประดิษฐ์ (3) กฎหมายและข้อกำหนดที่เกี่ยวข้อง และ (4) มาตรการในการควบคุมและแก้ไขความเสี่ยง เพื่อมาเปลี่ยนเป็นข้อกำหนดความต้องการในการพัฒนาระบบ AI (AI Requirement) พร้อมทั้งเลือกใช้เครื่องมือหรือผลิตภัณฑ์ที่สามารถตอบสนองความต้องการดังกล่าวได้**

แต่เนื่องจากบริบทในการประยุกต์ใช้ AI และความพร้อมด้านบุคลากรที่แตกต่างกันในแต่ละองค์กร การเลือกใช้เครื่องมือหรือผลิตภัณฑ์ในแต่ละองค์กรจึงมีความแตกต่างกัน โดยบางองค์กรอาจเลือกใช้ผลิตภัณฑ์ AI ที่พร้อมใช้งาน (Off-the-shelf AI Product) หรือว่าจ้างหน่วยงานภายนอกมาดำเนินการทั้งหมด แต่ในขณะที่บางองค์กรอาจมีความต้องการที่จะสร้างและนำโมเดลไปใช้งานด้วยบุคลากรของตนเอง จึงทำให้แนวทางในการสร้างและนำโมเดลไปใช้งานในปัจจุบัน อาจแบ่งออกเป็น 4 แนวทางหลัก

แนวทางในการสร้างและนำโมเดลไปใช้งานในปัจจุบัน

1. **สร้างและนำโมเดลไปใช้งานด้วยบุคลากรภายในองค์กร**
   สำหรับองค์กรที่มีความพร้อมด้านบุคลากรในด้าน AI อาจทำการสร้างโมเดลและนำโมเดลไปใช้งานกับระบบหรือบริการด้วยบุคลากรภายในองค์กรเอง โดยในกรณีดังกล่าวองค์กรจำเป็นต้องดำเนินการตั้งแต่กระบวนการสร้าง สอน ตรวจสอบ และทดสอบโมเดล รวมถึงจัดเตรียมข้อมูลสำหรับกระบวนการดังกล่าวด้วยตนเองทั้งหมด ซึ่งแนวทางการสร้างและนำโมเดลไปใช้งานในรูปแบบนี้ จะช่วยให้องค์กรได้ระบบหรือบริการที่ตรงตามความต้องการ แต่จำเป็นต้องลงทุนด้านบุคลากรและเวลามากกว่าแนวทางอื่น

2. **นำโมเดลในรูปแบบโอเพนซอร์ส (Open-source Model) มาปรับใช้**
   การนำโมเดลในรูปแบบโอเพนซอร์สมาปรับใช้จะช่วยลดเวลาในการสร้างโมเดล แต่อย่างไรก็ตาม องค์กรยังคงมีหน้าที่ในการสอน ตรวจสอบ และทดสอบโมเดล รวมถึงจัดเตรียมข้อมูลสำหรับกระบวนการดังกล่าว อีกทั้งยังต้องทำการทดสอบประสิทธิภาพและความสอดคล้องตามข้อกำหนดความต้องการในการพัฒนาระบบ AI (AI Requirement)

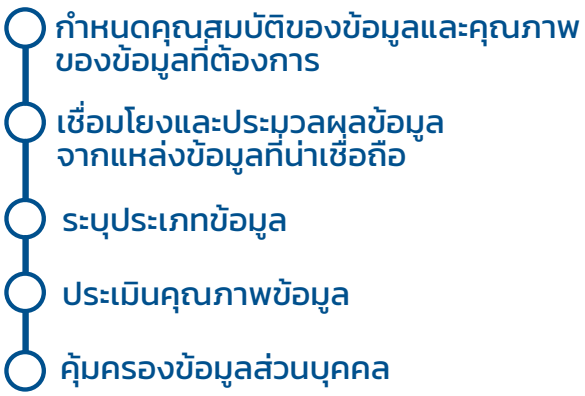
3. **เลือกใช้โมเดลที่ได้รับการสอนแล้ว (Pre-trained Model) มาปรับใช้**
   การเลือกใช้โมเดลที่ได้รับการสอนแล้ว (Pre-trained Model) จากผู้ให้บริการโซลูชั่นด้าน AI หรือหน่วยงานภายนอกมาปรับใช้นั้น เป็นอีกหนึ่งแนวทางที่ช่วยลดเวลาและภาระในกระบวนการสร้าง สอน และตรวจสอบโมเดล แต่อย่างไรก็ตามองค์กรยังคงมีหน้าที่ในการจัดเตรียมข้อมูล รวมถึงทดสอบประสิทธิภาพและความสอดคล้องตามข้อกำหนดความต้องการในการพัฒนาระบบ AI (AI Requirement)

4. **เลือกใช้ผลิตภัณฑ์ AI ที่พร้อมใช้งาน (Off-the-shelf AI Product)**
   การเลือกใช้ผลิตภัณฑ์ AI ที่พร้อมใช้งานในท้องตลาดจะช่วยลดเวลาและความซับซ้อนในการพัฒนาระบบ อีกทั้งยังช่วยลดภาระขององค์กรในการสร้างบุคลากรด้าน AI แต่อย่างไรก็ตาม องค์กรยังคงมีความจำเป็นที่จะต้องจัดเตรียมข้อมูลและดำเนินการทดสอบเช่นเดียวกันกับแนวทางข้างต้น

จากแนวทางการดำเนินการที่ 2-4 จะพบว่าองค์กรมีการใช้โมเดลหรือผลิตภัณฑ์ AI ที่สร้างโดยหน่วยงานภายนอก รวมถึงอาจมีการว่าจ้างหน่วยงานภายนอกเพื่อนำโมเดลหรือผลิตภัณฑ์ AI มาปรับใช้ร่วมกับกระบวนการหรือขั้นตอนปฏิบัติต่าง ๆ ให้แก่องค์กร

โดยในกรณีที่มีความเสียหายหรือผลกระทบเชิงลบซึ่งเกิดความผิดพลาดของหน่วยงานภายนอก รวมถึงความผิดพลาดจากการทำงานของโมเดลหรือผลิตภัณฑ์ AI (ตามแนวทางที่ 2-4) นั้น **องค์กรยังคงต้องรับผิดชอบต่อความเสียหายหรือผลกระทบเชิงลบเช่นเดียวกันกับการดำเนินการตามแนวทางการดำเนินการที่ 1 ด้วยเหตุนี้ องค์กรจึงจำเป็นต้องมีการกำกับดูแลการปฏิบัติงานของหน่วยงานภายนอกให้สอดคล้องตามนโยบายและขั้นตอนปฏิบัติขององค์กร รวมถึงจัดให้มีการทดสอบอย่างเหมาะสม** เพื่อให้มั่นใจได้ว่าโมเดลหรือผลิตภัณฑ์ AI ที่ใช้งานมีประสิทธิภาพและสอดคล้องตามข้อกำหนดความต้องการในการพัฒนาระบบ AI (AI Requirement)

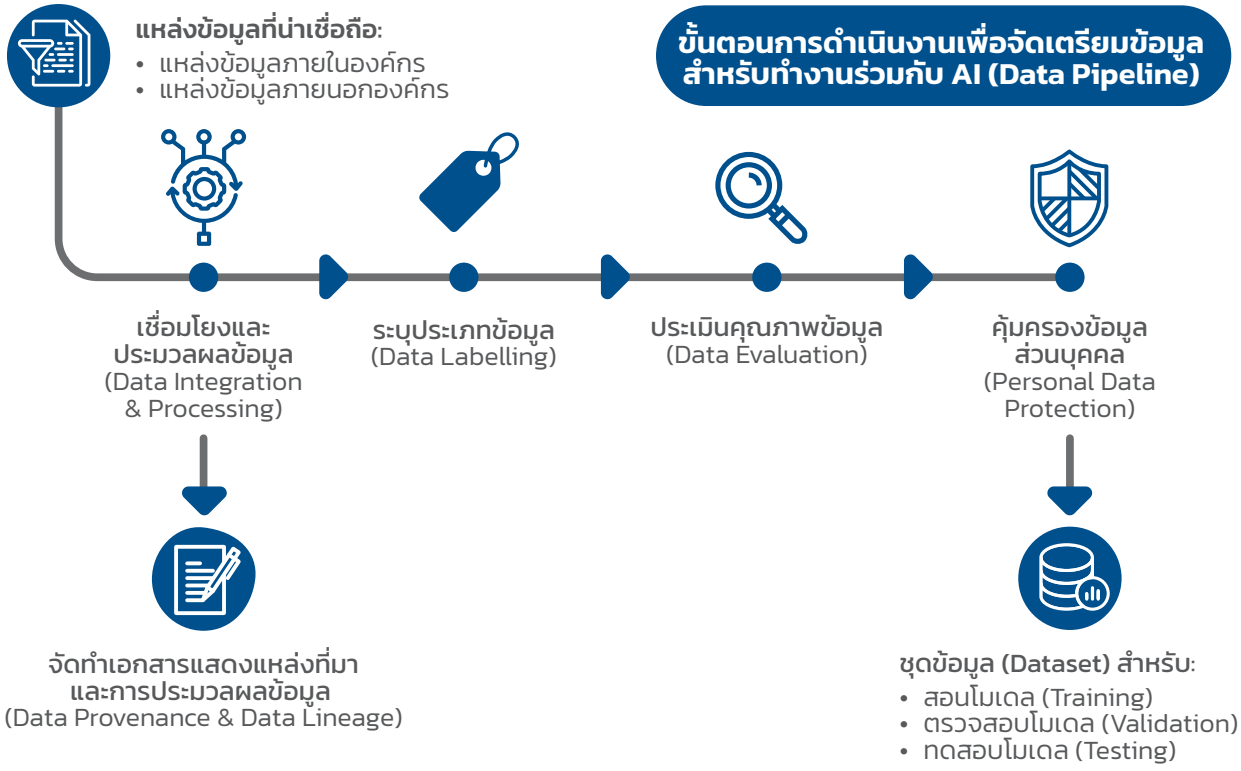
จัดเตรียมข้อมูล (Data Preparation)



เนื่องจาก AI จำเป็นต้องใช้ข้อมูลในการเรียนรู้และประมวลผลในการทำงาน ด้วยเหตุนี้ **องค์กรจึงควรมีการกำหนดคุณสมบัติและคุณภาพของข้อมูลที่เหมาะสม เพื่อให้ AI สามารถทำงานได้อย่างมีประสิทธิภาพตามเป้าหมายที่กำหนด** โดยในการกำหนดคุณสมบัติและคุณภาพนั้น อาจพิจารณาจากประเภทของข้อมูลที่จำเป็นต้องใช้ในการประมวลผล ขนาดของข้อมูล ความถูกต้องของข้อมูล ข้อมูลมีการจัดเก็บภายในช่วงเวลาที่ต้องการ (Time Series Data) มีการปรับปรุงข้อมูลเป็นประจำสม่ำเสมอ เป็นต้น **อีกทั้งองค์กรควรมีการสรรหาแหล่งข้อมูลที่น่าเชื่อถือเพื่อนำมาใช้งานร่วมกับ AI**

นอกจากนี้ องค์กรยัง**ควรมีการพิจารณาคุณสมบัติของข้อมูลในด้านอื่นเพื่อลดการเกิดอคติที่มาจากข้อมูล (Data Bias)** เช่น ข้อมูลมีความหลากหลาย ข้อมูลมีความครอบคลุมทุกกลุ่มประชากรโดยไม่เอนเอียงไปยังกลุ่มใดกลุ่มหนึ่ง ขนาดของกลุ่มตัวอย่างสามารถสะท้อนหรือเป็นตัวแทนของประชากรได้อย่างสมเหตุสมผล เป็นต้น **รวมถึงพิจารณาความน่าเชื่อถือของการเก็บรวบรวมข้อมูล เพื่อลดการเกิดอคติที่เกิดจากความคลาดเคลื่อนในการวัดหรือความผิดพลาดจากเครื่องมือวัด (Measurement Bias)**

โดยภายหลังจากทำการเชื่อมโยงเพื่อรวบรวมข้อมูลจากแหล่งต่าง ๆ (Data Integration) เรียบร้อยแล้ว ไม่ว่าจะเป็นแหล่งที่มาจากภายในหรือภายนอกองค์กร **ควรมีการจัดทำเอกสารเพื่อแสดงแหล่งที่มาของข้อมูล (Data Provenance) รวมถึงรายละเอียดการประมวลผลหรือการเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นกับข้อมูลตลอดกระบวนการจัดเตรียมข้อมูล (Data Lineage) เพื่อประโยชน์ในการตรวจสอบย้อนกับ (Traceability)** ในกรณีที่ AI ทำงานผิดพลาด



เนื่องจากในการสร้างโมเดลจำเป็นต้องใช้ข้อมูลในการดำเนินการ โดยเฉพาะอย่างยิ่ง AI ประเภท Supervised Machine Learning จำเป็นต้องเรียนรู้จากข้อมูลที่สอนโดยมนุษย์ เพื่อให้สามารถวิเคราะห์คาดการณ์ ให้คำแนะนำ ตัดสินใจ หรือดำเนินการใด ๆ แทนมนุษย์ได้ ด้วยเหตุนี้ **ในการจัดเตรียมข้อมูลสำหรับการสอน ตรวจสอบ และทดสอบโมเดล จำเป็นต้องมีการระบุประเภทของข้อมูล (Data Labelling) อย่างถูกต้อง เพื่อให้ AI มีข้อมูลและสามารถรับรู้ความหมายของข้อมูลได้อย่างถูกต้อง** ซึ่งในการระบุประเภทของข้อมูลสามารถทำได้ทั้งในรูปแบบรูปภาพ ข้อความ และเสียง ตัวอย่างเช่น การระบุรูปคน สัตว์ และสิ่งของต่าง ๆ เพื่อให้ AI สามารถเข้าใจรูปภาพหรือวิดีโอในแบบเดียวกับที่มนุษย์มองเห็น หรือการระบุอารมณ์และความรู้สึกของแต่ละข้อความหรือเสียง เพื่อให้ AI สามารถเข้าใจได้ว่า ผู้ที่แสดงความคิดเห็นดังกล่าวมีความรู้สึกอย่างไร เป็นต้น

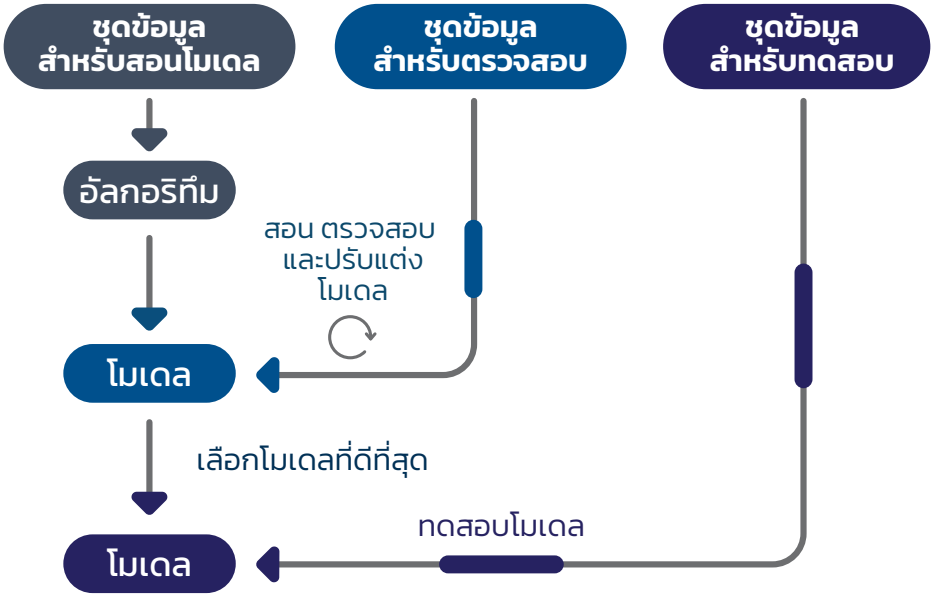
โดย**ก่อนที่จะนำชุดข้อมูล (Dataset) ไปใช้สำหรับการสอน ตรวจสอบ และทดสอบ องค์กรจำเป็นต้องมีการประเมินคุณภาพของข้อมูล (Data Evaluation) และอาจทำการปรับปรุงข้อมูลให้มีคุณภาพตามหลักเกณฑ์ที่องค์กรกำหนด** เช่น ข้อมูลมีความถูกต้อง (Accuracy) เนื้อหาข้อมูลครบถ้วน (Completeness) ตรงตามความต้องการ (Relevancy) มีรูปแบบของข้อมูล (Data Format) ตามที่กำหนด และมีการปรับปรุงให้เป็นปัจจุบัน (Timeliness) เป็นต้น **เพื่อให้มั่นใจได้ว่า AI มีความสามารถและประสิทธิภาพเป็นไปตามเป้าหมายที่กำหนด**

นอกจากนี้ ในกรณีที่มีการใช้ข้อมูลส่วนบุคคลในการประมวลผล รวมถึงกรณีที่มีการประมวลผลข้อมูลที่มีความอ่อนไหว (Sensitive Data) ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (เช่น เชื้อชาติ เผ่าพันธุ์ ข้อมูลสุขภาพ ข้อมูลชีวภาพ เป็นต้น) องค์กร**ควรมีการเก็บรักษาข้อมูลส่วนบุคคลอย่างมั่นคงปลอดภัยและจัดให้มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม** เช่น การควบคุมการเข้าถึง (Access Control) การเข้ารหัสลับข้อมูล (Encryption) การทำข้อมูลส่วนบุคคลให้เป็นข้อมูลนิรนาม (Anonymization) เป็นต้น **เพื่อลดความเสี่ยงที่จะทำให้ข้อมูลส่วนบุคคลรั่วไหล (Data Breach) และป้องกันผลกระทบที่อาจเกิดขึ้นจากการรั่วไหลของข้อมูล**

สร้างโมเดลปัญญาประดิษฐ์ (Model Building)

การสร้างโมเดลนั้นประกอบด้วยขั้นตอนพื้นฐาน 4 ขั้นตอน โดยเริ่มจากการจัดเตรียมอัลกอริทึมสำหรับสร้างโมเดล ซึ่งในขั้นตอนนี้องค์กรอาจพัฒนาอัลกอริทึมขึ้นเองหรืออาจนำอัลกอริทึมที่มีการเปิดเผยซอร์สโค้ด (Open Source) มาใช้งาน โดย**ในกรณีที่องค์กรสร้างโมเดลประเภท Machine Learning นั้น องค์กรจำเป็นต้องทำการสอนโมเดลด้วยชุดข้อมูลสำหรับสอนโมเดล (Training Dataset) จากนั้นจึงนำโมเดลไปตรวจสอบประสิทธิภาพ โดยใช้ชุดข้อมูลสำหรับตรวจสอบโมเดล (Validation Dataset)** ซึ่งหาก AI ยังไม่สามารถทำงานได้ตามประสิทธิภาพที่กำหนด **โมเดลดังกล่าวจะต้องถูกปรับแต่ง (Tuning) และนำกลับไปตรวจสอบจนกว่าประสิทธิภาพในการทำงานจะเป็นไปตามเป้าหมายที่กำหนด โดยโมเดลที่ดีที่สุดจะถูกนำไปทดสอบด้วยชุดข้อมูลสำหรับทดสอบโมเดล (Testing Dataset) ในขั้นตอนสุดท้ายก่อนนำไปใช้งาน (Deployment)** ซึ่งชุดข้อมูลสำหรับทดสอบโมเดลนี้จะต้องเป็นชุดข้อมูลที่ไม่เคยถูกใช้ในขั้นตอนการสอนและตรวจสอบโมเดลมาก่อน

- สร้างโมเดลปัญญาประดิษฐ์
- สอนโมเดลปัญญาประดิษฐ์
- ตรวจสอบและเลือกโมเดลปัญญาประดิษฐ์
- ทดสอบโมเดลปัญญาประดิษฐ์



ภาพขั้นตอนพื้นฐานในการสร้างโมเดลปัญญาประดิษฐ์ประเภท Machine Learning [1]

[1]Adapt from "Train, Validate, and Test" PRIMO.ai, accessed April 13, 2023, http://primo.ai/index.php?title=Train,_Validate,_and_Test

สำหรับองค์กรที่เลือกใช้โมเดลจากผู้ให้บริการโซลูชั่นด้าน AI (AI Solution Provider) ถึงแม้ว่าองค์กรจะไม่จำเป็นต้องทำการสร้างโมเดลด้วยตนเอง แต่องค์กรยังคงมีหน้าที่ในการทดสอบว่าโมเดลสามารถทำงานได้อย่างมีประสิทธิภาพและสามารถบรรลุตามเป้าหมายที่กำหนด พร้อมทั้ง มีหน้าที่ในการ**พิจารณาและตรวจสอบความเหมาะสมของกระบวนการสร้างโมเดล** เช่น ขั้นตอนและข้อมูลที่เกี่ยวข้องกับกระบวนการสร้าง สอน และทดสอบโมเดล รวมถึงมาตรการต่าง ๆ ที่เกี่ยวข้อง เป็นต้น

นอกเหนือจากการควบคุมกระบวนการสร้างโมเดลข้างต้นเพื่อให้ AI มีประสิทธิภาพและสามารถบรรลุเป้าหมายตามที่กำหนด **องค์กรยังจำเป็นต้องจัดให้มีมาตรการควบคุมเพื่อให้มั่นใจได้ว่า การทำงานของ AI สอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ รวมถึงกฎหมายและข้อกำหนดที่เกี่ยวข้อง**

โดยในการพิจารณาว่าการทำงานของ AI ควรสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ใดนั้น **องค์กรควรพิจารณาจากบริบทของการนำ AI ไปประยุกต์ใช้ ความเสี่ยง และผลกระทบที่อาจเกิดขึ้น โดยไม่จำเป็นต้องดำเนินการให้สอดคล้องกับทุกหลักการจริยธรรมปัญญาประดิษฐ์ที่กล่าวถึงในเอกสารนี้**

ความน่าเชื่อถือ (Reliability)

เพื่อให้การทำงานของ AI มีความน่าเชื่อถือ องค์กรควรมีการกำหนดมาตรการและควบคุมกระบวนการสร้างและทดสอบโมเดล เพื่อให้มั่นใจได้ว่า**โมเดลสามารถสร้างผลลัพธ์ได้เหมือนเดิมทุกครั้ง (Reproducibility) เมื่ออยู่ภายใต้สถานการณ์หรือได้รับข้อมูลที่เหมือนกัน อีกทั้งยังสามารถทนทาน (Robustness) ต่อเหตุการณ์ที่อาจเกิดความผิดพลาดหรือสร้างผลกระทบเชิงลบได้**

โดยในการทดสอบความทนทานต่อเหตุการณ์ที่อาจเกิดความผิดพลาดหรืออาจสร้างผลกระทบเชิงลบนั้น องค์กรจำเป็นต้องทำการทดสอบโดยใช้ข้อมูลที่อยู่นอกเหนือจากขอบเขตที่ออกแบบไว้ (Exceptions) รวมถึงทำการทดสอบภายใต้สถานการณ์หรือข้อมูลที่ไม่เคยถูกสอนมาก่อน เพื่อให้มั่นใจได้ว่า AI ยังคงสามารถทำงานได้อย่างถูกต้องตามที่ออกแบบไว้หรือสามารถรับมือกับเหตุการณ์ที่เกิดขึ้นโดยไม่ส่งผลกระทบเชิงลบต่อบุคคล องค์กร และสังคมโดยกว้าง

นอกจากนี้ในการทดสอบความทนทาน องค์กรยังจำเป็นต้องเฝ้าติดตามและนำผลลัพธ์การทำงานของ AI มาปรับปรุงอย่างต่อเนื่อง เพื่อให้ AI สามารถทำงานได้อย่างมีประสิทธิภาพภายใต้สภาพแวดล้อมการใช้งานจริงและอยู่ในขอบเขตที่ยอมรับได้

ความเท่าเทียม หลากหลาย ครอบคลุม และเป็นธรรม (Fairness)

ผลลัพธ์จากการทำงานของ AI ไม่ว่าจะอยู่ในรูปแบบของการวิเคราะห์คาดการณ์ การให้คำแนะนำ การตัดสินใจ หรือการดำเนินการใด ๆ นั้น **อาจส่งผลกระทบให้เกิดความไม่เป็นธรรม (Unfairness) จนนำไปสู่การเลือกปฏิบัติ (Discrimination) ซึ่งผลกระทบดังกล่าวนั้นอาจเกิดจากอคติที่มาจากข้อมูล (Data Bias) หรืออคติที่มาจากการออกแบบและสร้างโมเดล (Bias Introduced by Engineering Decisions)**

เพื่อป้องกันความไม่เป็นธรรมซึ่งเกิดจากอคติที่มาจากการออกแบบและสร้างโมเดล (Bias Introduced by Engineering Decisions) นั้น **บุคลากรที่เกี่ยวข้องกับกระบวนการสร้างและการทดสอบโมเดลจึงควรมีความรู้และมีความหลากหลาย รวมถึงจัดให้มีผู้เชี่ยวชาญในด้านที่เกี่ยวข้องกับการประยุกต์ใช้ AI คอยให้คำปรึกษา** เพื่อให้องค์กรมองเห็นอคติที่อาจเกิดขึ้นและกำหนดกลยุทธ์ในการลดอคติดังกล่าว

สำหรับ**อคติที่มาจากข้อมูล (Data Bias) นั้น อาจเกิดจากการมีข้อมูลที่เอนเอียง ไม่ครอบคลุมทุกกลุ่มประชากร หรือมีขนาดของกลุ่มตัวอย่างที่ไม่เหมาะสม ทำให้เกิดความไม่เป็นธรรม (ซึ่งเรียกว่า "Selection Bias")** ตัวอย่างเช่น AI คัดเลือกใบสมัครจากผู้สมัครงานเพศชายมากกว่าเพศหญิง เนื่องจากข้อมูลส่วนใหญ่ที่ใช้สอนโมเดลนั้นเป็นข้อมูลของเพศชาย จึงทำให้ AI ให้น้ำหนักในการคัดเลือกผู้สมัครงานเพศชายเพื่อเข้ารับการสัมภาษณ์มากกว่าผู้สมัครเพศหญิง เป็นต้น อีกทั้งในบางกรณีอาจเกิดจาก**อคติที่มาจากความคลาดเคลื่อนในการวัดหรือความผิดพลาดจากเครื่องมือวัด (Measurement Bias)** เช่น อุปกรณ์วัดระดับมลพิษทางอากาศบางพื้นที่แจ้งระดับมลพิษต่ำกว่าความเป็นจริง ทำให้พื้นที่ดังกล่าวไม่ได้รับการแก้ไขปัญหา จนนำไปสู่ปัญหาสุขภาพของประชาชนในพื้นที่ เป็นต้น

องค์กรอาจพิจารณาเลือกใช้มาตรการดังต่อไปนี้เพื่อลดอคติที่มาจากข้อมูล ตัวอย่างเช่น

1. เลือกใช้ข้อมูลจากแหล่งข้อมูลที่มีความน่าเชื่อถือและมีการเก็บรวบรวมข้อมูลอย่างถูกต้อง
2. ข้อมูลมีความหลากหลายและครอบคลุมทุกกลุ่มประชากร อีกทั้งมีการรวบรวมมาจากแหล่งข้อมูลที่หลากหลาย (หากเป็นไปได้)
3. ขนาดของกลุ่มตัวอย่างสามารถสะท้อนหรือเป็นตัวแทนของประชากรได้อย่างสมเหตุสมผล

4. ระมัดระวังในการเลือกใช้ข้อมูลเฉพาะกลุ่มประชากรกลุ่มใดกลุ่มหนึ่ง รวมถึงข้อมูลที่มีความอ่อนไหว (Sensitive Data) ตัวอย่างเช่น เพศ เชื้อชาติ ศาสนา ประวัติการรักษาพยาบาล ประวัติอาชญากรรม เป็นต้น

5. พิจารณากำหนดชุดข้อมูลสำหรับทดสอบแต่ละชุดให้มีความแตกต่างกันของกลุ่มประชากร เพื่อตรวจสอบว่า AI ยังคงตัดสินใจได้อย่างถูกต้อง ไม่เอนเอียงไปตามกลุ่มประชากรกลุ่มใดกลุ่มหนึ่ง

6. อาจพิจารณาสุ่มข้อมูลที่คาดว่าจะส่งผลให้เกิดอคติ เพื่อค้นหาความผิดพลาด พร้อมทั้งเก็บรวบรวมข้อมูลดังกล่าวสำหรับใช้ในครั้งต่อไป

ความโปร่งใส (Transparency)

ความสามารถในการอธิบายรายละเอียดเกี่ยวกับ AI (Explainability) เป็นหนึ่งในมาตรการสำคัญที่จะช่วยให้เกิดความโปร่งใสในการประยุกต์ใช้ AI โดย**องค์กรจำเป็นต้องมีการจัดทำเอกสารเพื่ออธิบายพฤติกรรมการทำงานของ AI และเหตุผลเบื้องหลังการทำงาน รวมถึงอธิบายกระบวนการในการสร้างและทดสอบโมเดล** ซึ่งจะช่วยให้ผู้ที่เกี่ยวข้องรับทราบและเข้าใจถึงกระบวนการทำงานของ AI อีกทั้งยังเป็นการสร้างความเชื่อมั่นและการยอมรับจากบุคคลที่เกี่ยวข้องอีกด้วย

นอกจากนี้ เพื่อให้เกิดความโปร่งใสในการประยุกต์ใช้ AI **องค์กรควรมีการดำเนินการเพื่อให้สามารถตรวจสอบย้อนกลับ (Traceability)** ในกรณีที่พบความผิดปกติหรือความผิดพลาดได้ **โดยทำการเก็บรวบรวมข้อมูลและรายละเอียดที่เกี่ยวข้องกับกระบวนการในการสร้างและทดสอบโมเดล** เช่น

- แหล่งที่มาของข้อมูล (Data Provenance)
- การประมวลผลหรือการเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นกับข้อมูลตลอดกระบวนการจัดเตรียมข้อมูล (Data Lineage)
- รายละเอียดการออกแบบและการทำงานของอัลกอริทึม
- ชุดข้อมูลที่ใช้และผลลัพธ์ในการสอน ตรวจสอบ และทดสอบโมเดล
- ผลการประเมินความเสี่ยงและมาตรการการรับมือ

ความมั่นคงปลอดภัยและความเป็นส่วนตัว (Security and Privacy)

ในด้านการรักษาความมั่นคงปลอดภัยและการคุ้มครองความเป็นส่วนตัวนั้น การปฏิบัติตามแนวปฏิบัติที่ดีในการพัฒนาซอฟต์แวร์ (เช่น การควบคุมเวอร์ชัน การทดสอบ และการควบคุมคุณภาพของซอร์สโค้ด เป็นต้น) อาจจะไม่เพียงพอต่อการรักษาความมั่นคงปลอดภัยและคุ้มครองความเป็นส่วนตัว เนื่องจาก **AI อาจมีช่องโหว่ที่เปิดโอกาสให้ผู้ประสงค์ร้ายโจมตีข้อมูลที่ใช้ในการสอนโมเดลและโจมตีที่โมเดลโดยตรง** ตัวอย่างเช่น

- Poisoning Attack เป็นการโจมตีโดยทำให้ข้อมูลที่ใช้ในการสอนโมเดลปนเปื้อนด้วยข้อมูลที่ทำให้โมเดลเกิดช่องโหว่ (Adversarial Manipulation) เพื่อให้ผู้ประสงค์ร้าย (Attacker) สามารถบรรลุเป้าหมายที่ต้องการ
- Evasion Attack เป็นการโจมตีโมเดลโดยตรง โดยส่งข้อมูลที่ทำให้โมเดลประมวลผลแล้วทำงานผิดพลาดหรือหยุดการทำงาน (Adversarial Input)

เพื่อป้องกันภัยคุกคามข้างต้นจึงจำเป็นต้องมีความร่วมมือกันระหว่างนักพัฒนา AI (AI Developer) นักวิทยาศาสตร์ข้อมูล (Data Scientist) นักวิเคราะห์ข้อมูล (Data Analyst) ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย รวมถึงผู้มีส่วนได้เสียที่เกี่ยวข้อง ในการจัดทำมาตรการเพื่อป้องกันภัยคุกคามที่อาจเกิดขึ้น โดยปฏิบัติตามมาตรฐานหรือแนวทางการรักษาความมั่นคงปลอดภัย เช่น มาตรฐานที่ประกาศโดย The ETSI Technical Committee on Securing Artificial Intelligence (TC SAI) และมาตรฐาน ISO/IEC 27090 Cybersecurity — Artificial Intelligence — Guidance for addressing security threats and failures in artificial intelligence systems ซึ่งกำลังจะประกาศใช้โดยหน่วยงาน International Organization for Standardization (ISO) นอกจากนี้ควรติดตามข่าวสารเกี่ยวกับภัยคุกคามจากแหล่งข้อมูลต่าง ๆ เช่น The Open Worldwide Application Security Project (OWASP) และ Adversarial Threat Landscape for Artificial-Intelligence System (MITRE ATLAS)

นอกจากนี้ ในการคุ้มครองความเป็นส่วนตัว **ควรมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access) รวมถึงจัดให้มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม** ซึ่งได้กล่าวมาแล้วในหัวข้อการจัดเตรียมข้อมูล (Data Preparation)


week 1
week 2
week 3
week 4
week 5
week 6
M T W Th F
Main Project
TimeLine total Use : 30 day

นำโมเดลไปใช้งาน (Deployment)

ก่อนนำโมเดลไปใช้งานจริง **องค์กรควรมีการนำโมเดลไปติดตั้งและทดสอบการทำงานภายใต้สภาพแวดล้อมเสมือนจริง (Pre-Production Environment) เพื่อทดสอบการทำงานร่วมกับขั้นตอนปฏิบัติงานที่เกี่ยวข้อง พร้อมทั้งทดสอบความสามารถในการรองรับปริมาณการใช้งาน (Workload) และความสามารถในการตอบสนองภายในระยะเวลาที่ยอมรับได้ (Acceptable Latency Time)** ซึ่งการติดตั้งและทดสอบในสภาพแวดล้อมดังกล่าว จะช่วยให้องค์กรพบปัญหาและสามารถป้องกันปัญหาที่อาจเกิดขึ้นก่อนนำโมเดลไปใช้งานจริง อีกทั้งยังเป็นการสร้างความน่าเชื่อถือ (Reliability) ให้แก่ระบบหรือบริการ

- ทดสอบการทำงานของโมเดลใน Pre-production Environment
- บริหารจัดการความเปลี่ยนแปลง (Change Management)
- รักษาความมั่นคงปลอดภัยและคุ้มครองข้อมูลส่วนบุคคล
- จัดให้มีมาตรการรับมือประเด็นปัญหาและเหตุการณ์ผิดปกติ

นอกจากนี้ ก่อนนำโมเดลไปใช้งานจริงองค์กรควรมีการ**ออกแบบสถาปัตยกรรมที่เกี่ยวข้องกับการประยุกต์ใช้ AI (AI Architecture) ที่มีประสิทธิภาพและสามารถรองรับปริมาณการใช้งานได้อย่างเพียงพอ เพื่อให้การประยุกต์ใช้ AI บรรลุตามเป้าหมายที่กำหนด พร้อมทั้งอาจพิจารณาออกแบบสถาปัตยกรรมให้มีความยืดหยุ่น**เพื่อรองรับความต้องการที่เพิ่มขึ้นหรือการขยายขอบเขตการใช้งานในอนาคตได้

เพื่อให้องค์กรมีความพร้อมในการทำงานหรือให้บริการอย่างต่อเนื่อง องค์กรจึงควร**มีการบริหารจัดการความเปลี่ยนแปลง (Change Management) เพื่อลดผลกระทบที่อาจเกิดขึ้นจากการนำโมเดลไปใช้งานร่วมกับขั้นตอนปฏิบัติงานจริง** นอกจากนี้ ในการบริหารจัดการความเปลี่ยนแปลงดังกล่าว ยังจำเป็นต้องครอบคลุมถึงกรณีที่มีการปรับปรุงแก้ไขโมเดลและการยุติการใช้งานโมเดลด้วยเช่นกัน เพื่อไม่ให้การเปลี่ยนแปลงใด ๆ ที่เกี่ยวข้องกับโมเดลส่งผลกระทบต่อการทำงานหรือการให้บริการ

เนื่องจาก AI เป็นเทคโนโลยีสารสนเทศประเภทหนึ่งที่ต้องทำงานร่วมกับระบบเทคโนโลยีสารสนเทศที่หลากหลาย เช่น ระบบปฏิบัติการ (Operating System) ระบบเครือข่าย (Network) ระบบบริการคลาวด์ (Cloud Computing) ระบบบริหารจัดการข้อมูล (Data Management System) เป็นต้น ดังนั้น ผลกระทบใด ๆ ที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศดังกล่าวย่อมส่งผลกระทบต่อการทำงานของ AI ด้วยเช่นกัน ด้วยเหตุนี้ **องค์กรจึงควรมี**

มาตรการในการรักษาความมั่นคงปลอดภัยสารสนเทศและคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม เพื่อควบคุมความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้ และป้องกันผลร้ายที่อาจเกิดขึ้น เช่น การโจรกรรมข้อมูลสำคัญขององค์กร ข้อมูลส่วนบุคคลรั่วไหล การโจมตีช่องโหว่ของโมเดลเพื่อให้ระบบบริการหยุดชะงักหรือใช้ประโยชน์จากความผิดพลาดเพื่อเข้าถึงระบบ เป็นต้น

นอกจากนี้ เพื่อให้องค์กรสามารถรับมือกับเหตุการณ์ผิดปกติและลดผลกระทบที่อาจเกิดขึ้นได้อย่างทันท่วงที องค์กรจึงควร**จัดให้มีช่องทางรับข้อคิดเห็น (Feedback) ประเด็นปัญหา (Issue) ความผิดพลาด (Error) จากการปฏิบัติงานและการให้บริการ พร้อมทั้งจัดให้มีมาตรการในการบริหารจัดการเหตุการณ์ผิดปกติ (Incident Management) เพื่อรับมือและแก้ไขปัญหาที่เกิดขึ้น** อีกทั้งยังเป็นการลดผลกระทบที่อาจเกิดขึ้นต่อบุคคล องค์กร หรือสังคมโดยกว้าง

เฝ้าติดตามการประยุกต์ใช้ (Monitoring)

ภายหลังจากนำโมเดลไปใช้งานในระบบบริการจริง องค์กร**ควรมีการเฝ้าติดตามประสิทธิภาพ (Performance) ของการประยุกต์ใช้ AI ในด้านความสำเร็จตามเป้าหมายและประสิทธิภาพในการทำงานของ AI พร้อมทั้งปรับแต่งค่า (Model Tuning) เมื่อมีความจำเป็น** เพื่อให้มั่นใจได้ว่าโมเดลยังสามารถทำงานได้ตามเป้าหมายที่องค์กรกำหนด พร้อมทั้งจัดให้มีกระบวนการในการ**เฝ้าติดตามว่ามีข้อมูลใหม่ที่ควรนำมาใช้ในการสอนโมเดลเพื่อปรับปรุงประสิทธิภาพของ AI** หรือไม่ นอกจากนี้ การเฝ้าติดตามยัง**รวมถึงการปฏิบัติงานตามนโยบายขององค์กร หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้องอย่างสม่ำเสมอ**

โดยในการเฝ้าติดตามประสิทธิภาพของการประยุกต์ใช้ AI นั้น อาจดำเนินการโดยพิจารณาจากผลลัพธ์จากการทำงาน ระดับความถูกต้องในการตัดสินใจ (Accuracy Rate) ข้อคิดเห็น (Feedback) ประเด็นปัญหา (Issue) และความผิดพลาดที่เกิดขึ้น (Error) เป็นต้น ทั้งนี้ หากองค์กรมีเครื่องมือที่ช่วยในการเฝ้าติดตามและมีการรายงานผลโดยอัตโนมัติ ไม่ว่าจะอยู่ในรูปแบบของการรายงานผ่านหน้าจอสรุปข้อมูล (Dashboard) หรือมีการแจ้งเตือนผ่านช่องทางต่าง ๆ จะช่วยเพิ่มประสิทธิภาพในการเฝ้าติดตาม อีกทั้งยังช่วยลดภาระในการเฝ้าติดตามและรายงานผลคณะกรรมการกำกับดูแลฯ เพื่อรับทราบ

ประเมินผลการประยุกต์ใช้ (Evaluation)

การประเมินผลการประยุกต์ใช้ AI **เป็นการนำผลลัพธ์จากการประยุกต์ใช้ในปัจจุบันมาพิจารณาเพื่อกำหนดแนวทางการดำเนินการในอนาคต** โดยอาจพิจารณาในด้านต่าง ๆ เช่น

- ประสิทธิภาพ (Performance) ของการประยุกต์ใช้ AI ในด้านความสำเร็จตามเป้าหมายและประสิทธิภาพในการทำงานของ AI ที่ผ่านมา เมื่อเทียบกับเป้าหมายที่กำหนด ความสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้อง

- พิจารณาปรับปรุงเป้าหมายในการประยุกต์ใช้ AI หากพบว่าการประยุกต์ใช้ AI ไม่สามารถช่วยให้องค์กรบรรลุตามเป้าหมายที่กำหนดได้ หรือมีเหตุจำเป็นที่ต้องปรับปรุงเป้าหมาย

- ปรับปรุงข้อกำหนดความต้องการในการพัฒนาระบบ AI (AI Requirement) หากพบว่าข้อกำหนดความต้องการไม่ถูกต้อง หรือยกเลิกข้อกำหนดในบางเรื่องหากพบว่าไม่มีความจำเป็น

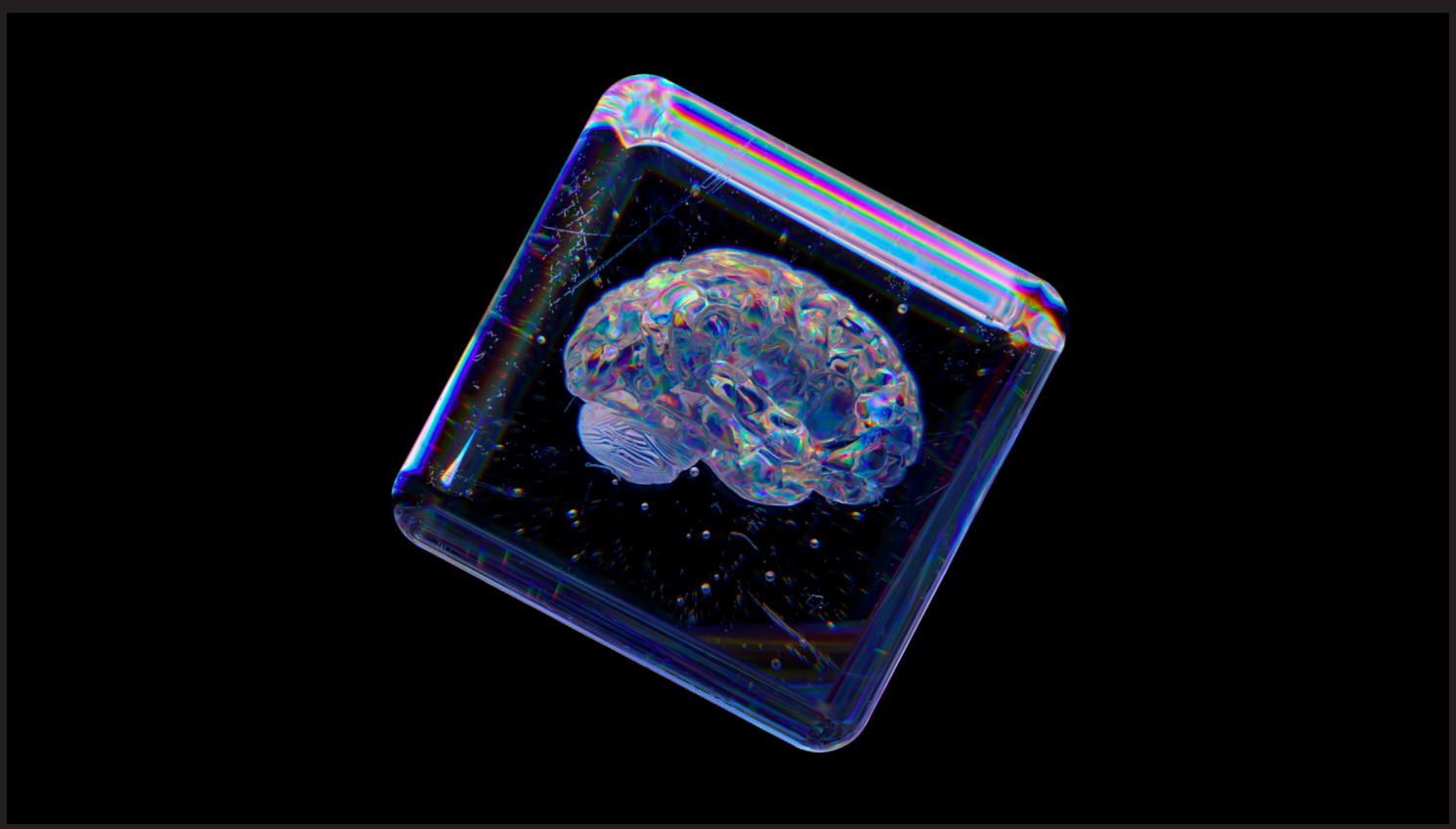
- วิเคราะห์และทบทวนความเสี่ยงจากการดำเนินงานที่ผ่านมา รวมถึงวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นในอนาคต เพื่อปรับปรุงแผนการจัดการความเสี่ยง (Risk Treatment Plan) ให้เหมาะสม

โดยในการประเมินผลการประยุกต์ใช้ AI นั้น **อาจจัดให้มีการประเมินผลโดยผู้ตรวจประเมินภายใน (Internal Auditor) หรือผู้ตรวจประเมินภายนอก (External Auditor) ตามความเหมาะสมเพื่อช่วยเพิ่มความน่าเชื่อถือ (Reliability)** ให้แก่บริการ พร้อมทั้งแจ้งผลการตรวจประเมินให้คณะกรรมการกำกับดูแลฯ รับทราบ เพื่อพิจารณาและกำหนดแนวทางการดำเนินงานในอนาคต รวมถึงสื่อสารให้แก่ผู้มีส่วนได้เสียที่เกี่ยวข้องรับทราบและดำเนินการตามแนวทางที่กำหนด

ยุติการใช้งาน (Retirement)

ในกรณีที่โมเดล ผลิตภัณฑ์ ระบบหรือบริการที่เกี่ยวข้องกับ AI **ไม่สามารถช่วยให้องค์กรบรรลุตามเป้าหมายหรือตอบโจทย์ความต้องการทางธุรกิจได้อย่างมีประสิทธิภาพ ซึ่งอาจเกิดจากเทคโนโลยีที่ใช้นั้นล้าสมัย (Obsolete) หรือผลลัพธ์จากการทำงานของ AI ในปัจจุบันไม่สามารถตอบสนองต่อความต้องการขององค์กรที่เปลี่ยนแปลงได้** ซึ่งในกรณีดังกล่าวองค์กรอาจพิจารณาดำเนินการใน 2 กรณี กล่าวคือ

1. ยุติการใช้งานโมเดล ระบบ หรือบริการที่เกี่ยวข้องกับ AI ดังกล่าว
2. นำโมเดล ผลิตภัณฑ์ ระบบหรือบริการที่เกี่ยวข้องกับ AI ใหม่ มาใช้งานทดแทนของเดิม (Replace) หากองค์กรพบว่ามีแนวทางใหม่มีประสิทธิภาพที่ดีกว่า หรือสามารถตอบสนองต่อความต้องการขององค์กรที่เปลี่ยนแปลงไปได้



7.2 การให้บริการ AI (AI Service)

การสื่อสารเพื่อสร้างความสัมพันธ์ระหว่างองค์กรและผู้ใช้งานนั้น มีความสำคัญอย่างยิ่งต่อการสร้างความโปร่งใสในการให้บริการ อีกทั้งยังเป็นการสร้างความเชื่อมั่นของผู้ใช้งานที่มีต่อบริการและองค์กร ด้วยเหตุนี้ **องค์กรจึงควรมีการสื่อสารนโยบายในการให้บริการ ข้อกำหนดในการให้บริการ และข้อมูลที่เกี่ยวข้องกับการใช้งาน AI รวมถึงการเปิดให้มีช่องทางการติดต่อสื่อสารกับผู้ใช้งานเพื่อรับฟังเสียงสะท้อนจากการใช้งานจริง** ดังตัวอย่างต่อไปนี้

การประกาศนโยบายและข้อมูลทั่วไปเกี่ยวกับการใช้งาน AI (Policy and General Disclosure)

ในการให้บริการที่เกี่ยวข้องกับ AI องค์กรควรมีการแจ้งให้ผู้ใช้งานรับทราบถึงนโยบายด้านต่าง ๆ เกี่ยวกับการให้บริการ ตัวอย่างเช่น นโยบายในการใช้งาน AI (AI Usage Policy) แนวปฏิบัติตามหลักการจริยธรรมปัญญาประดิษฐ์ (AI Ethics Principles) นโยบายด้านความมั่นคงปลอดภัย (Security Policy) นโยบายความเป็นส่วนตัว (Privacy Policy) เป็นต้น

นอกจากนี้ องค์กรยังควรมีการแจ้งผู้ใช้งานทราบว่ากำลังใช้งาน รับบริการ หรือทำงานร่วมกับ AI ผ่านการแจ้งเตือนบนแอปพลิเคชัน (In-app Notification) พร้อมทั้งควรมีการแจ้งถึงวิธีการใช้งาน ข้อห้ามในการใช้งาน ความสามารถ ข้อจำกัด ผลลัพธ์จากการตัดสินใจของ AI รวมถึงวิธีการและเหตุผลเบื้องหลังการทำงานของ AI ผ่านทางคู่มือการใช้งาน คำถามที่พบบ่อย (FAQ) และข้อตกลงการใช้บริการ (Terms and Conditions) เป็นต้น

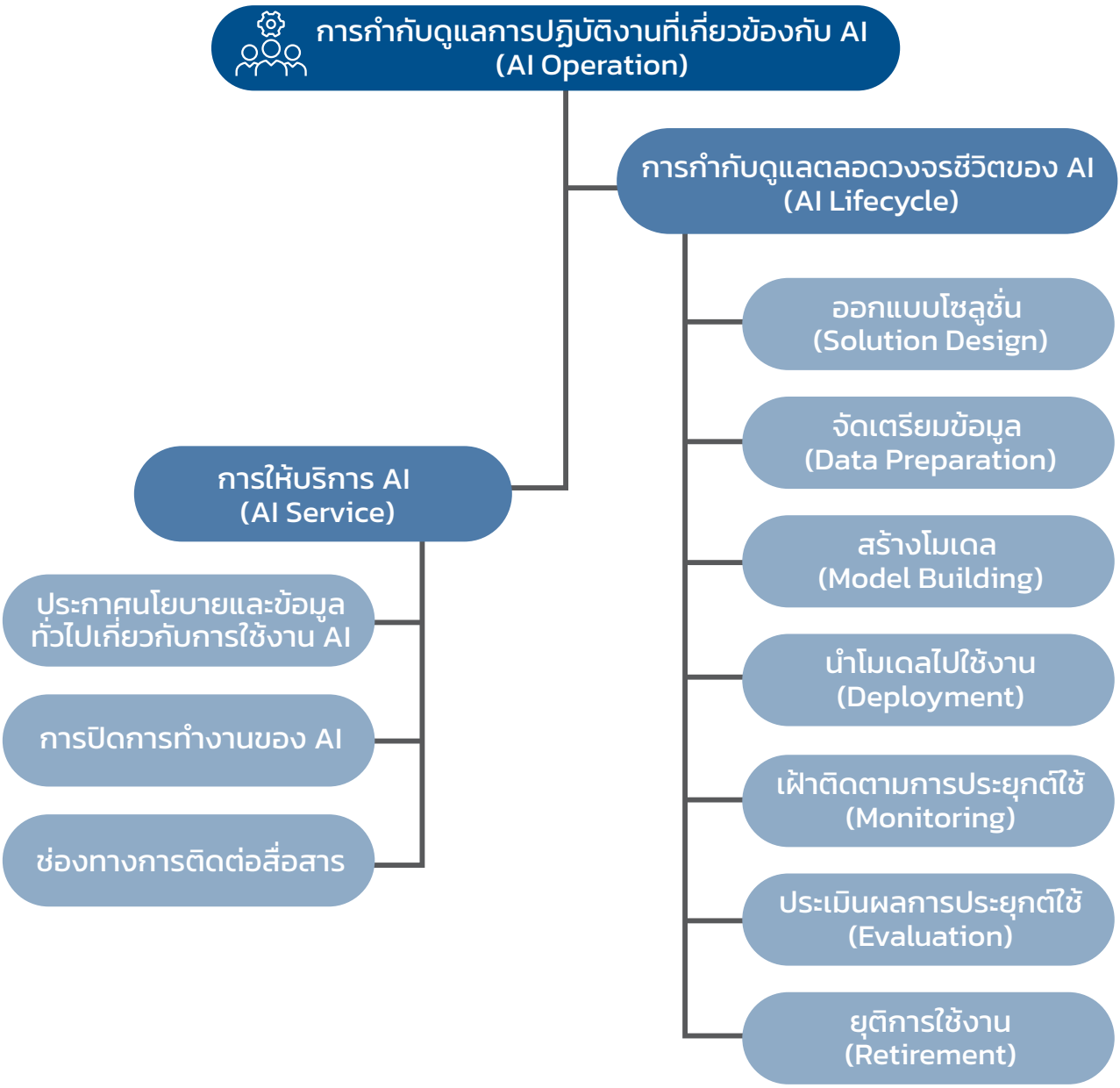
การปิดการทำงานของ AI (AI Function Opt-out)

ในกรณีที่ระบบสามารถเปิดโอกาสให้ผู้ใช้งานปิดการทำงานของ AI ได้ด้วยตนเอง เช่น รถยนต์ที่มีระบบการขับเคลื่อนอัตโนมัติด้วยตนเอง อนุญาตให้ผู้ใช้งานสามารถปิดระบบขับเคลื่อนอัตโนมัติด้วยตนเองได้ หากพบว่ารถยนต์ไม่สามารถตัดสินใจได้ถูกต้องในสภาพถนนที่ไม่เหมาะสม เป็นต้น อีกทั้ง องค์กรควรมีการสื่อสารอย่างเหมาะสมเพื่อให้ผู้ใช้งานทราบถึงขั้นตอนการปิดการทำงานดังกล่าว

ช่องทางการติดต่อสื่อสาร (Communication Channel)

การเปิดช่องทางการติดต่อสื่อสารเพื่อเปิดรับความคิดเห็น (Feedback) ประเด็นปัญหา (Issue) และความผิดพลาด (Error) ที่พบโดยผู้ใช้งานนั้นมีความสำคัญมาก เนื่องจากจะช่วยให้องค์กรสามารถปรับปรุง รวมถึงแก้ไขปัญหาและความผิดพลาดที่พบจากการให้บริการจริง อีกทั้งยังช่วยในการปรับปรุงประสบการณ์ในการให้บริการและป้องกันปัญหาหรือผลกระทบที่อาจเกิดขึ้นในอนาคต

ภาพสรุปองค์ประกอบสำคัญของการกำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับ AI (AI Operation)





08
ภาคผนวก

ภาคผนวก ก.
ตารางแสดงความสัมพันธ์ระหว่างหลักการจริยธรรมปัญญาประดิษฐ์และองค์ประกอบหลักในการสนับสนุนธรรมาภิบาลในการประยุกต์ใช้ AI

หลักการจริยธรรมปัญญาประดิษฐ์ตามแนวทางของ สดช. (ONDE's AI Ethics Principles)	องค์ประกอบในการสนับสนุนธรรมาภิบาลในการประยุกต์ใช้ AI		
	การกำหนดโครงสร้างการกำกับดูแล (AI Governance Structure)	การกำหนดกลยุทธ์ในการประยุกต์ใช้ AI (AI Strategy)	การกำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับ AI (AI Operation)
ความสามารถในการแข่งขันและการพัฒนาอย่างยั่งยืน (Competitiveness and Sustainable Development)	✅	✅	
ความสอดคล้องกับกฎหมาย จริยธรรม และมาตรฐานสากล (Laws, Ethics, and International Standards)	✅	✅	✅
ความโปร่งใสและความรับผิดชอบต่อผลของการกระทำ (Transparency and Accountability)	✅		✅
ความมั่นคงปลอดภัยและความเป็นส่วนตัว (Security and Privacy)			✅
ความเท่าเทียม หลากหลาย ครอบคลุม และเป็นธรรม (Fairness)			✅
ความน่าเชื่อถือ (Reliability)			✅

ภาคผนวก ข.
ตารางสรุปแนวทางในการสร้างโมเดลและนำโมเดลไปใช้งาน

แนวทางในการสร้างโมเดลและนำโมเดลไปใช้งาน	พัฒนาอัลกอริทึม	สอนโมเดล	ตรวจสอบโมเดล	ทดสอบโมเดล	จัดเตรียมข้อมูล	หมายเหตุ
สร้างและนำโมเดลไปใช้งานด้วยบุคลากรภายในองค์กร	✅	✅	✅	✅	✅	• องค์กรสามารถได้โมเดล รวมถึงระบบงานหรือบริการที่ตรงตามความต้องการ แต่จำเป็นต้องใช้บุคลากรและเวลามากกว่าแนวทางอื่น
นำโมเดลในรูปแบบโอเพนซอร์ส (Open-source Model) มาปรับใช้	—	✅	✅	✅	✅	• องค์กรยังคงมีหน้าที่: 1. จัดเตรียมข้อมูลและทดสอบความสอดคล้องตามข้อกำหนดความต้องการในการพัฒนาระบบ AI (AI Requirement) 2. กำกับดูแลการปฏิบัติงานของหน่วยงานภายนอก (Outsource) เพื่อให้ปฏิบัติตามนโยบายขององค์กร • องค์กรยังคงมีความรับผิดชอบต่อผลของการกระทำ (Accountability) จากความผิดพลาดจากการใช้โมเดลหรือผลิตภัณฑ์ที่พัฒนาโดยหน่วยงานภายนอก/ผู้ให้บริการโซลูชั่นด้าน AI
เลือกใช้โมเดลที่ได้รับการสอนแล้ว (Pre-trained model) มาปรับใช้	—	—	—	✅	✅	
เลือกใช้ผลิตภัณฑ์ AI ที่พร้อมใช้งาน (Off-the-shelf AI Product)	—	—	—	✅	✅	

ภาคผนวก ค.
ตารางสรุปความเชื่อมโยงแนวทางการกำกับดูแลการประยุกต์ใช้ AI และมาตรฐาน ISO/IEC 42001:2023

องค์ประกอบในการสนับสนุนธรรมาภิบาลในการประยุกต์ใช้ AI		มาตรฐาน ISO/IEC 42001:2023	
		ข้อกำหนด (Clause)	มาตรการควบคุม (Control) ที่ระบุใน Annex A
1. การกำหนดโครงสร้างการกำกับดูแล (AI Governance Structure)	1.1 AI Governance Council	5.1 Leadership and commitment 5.2 AI policy 7.1 Resources 7.4 Communication 7.5 Documented information 9.3 Management review 10 Improvement	A.2 Policies related to AI A.3 Internal organization A.4 Resources for AI systems
	1.2 Roles and Responsibility	5.3 Roles, responsibilities and authorities 7.5 Documented information	A.10 Third-party and customer relationships
	1.3 AI Competency	7.2 Competence 7.3 Awareness 7.5 Documented information	A.4 Resources for AI systems
2. การกำหนดกลยุทธ์ในการประยุกต์ใช้ AI (AI Strategy)	2.1 Responsible AI Strategy	6.2 AI objectives and planning to achieve them 6.3 Planning of changes 7.5 Documented information	
	2.2 Risk Management	6.1 Actions to address risks and opportunities 7.5 Documented information 8.2 AI risk assessment 8.4 AI system impact assessment	A.5 Assessing impacts of AI systems
3. การกำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับ AI (AI Operation)	3.1 AI Lifecycle	7.5 Documented information 8.1 Operational planning and control 9.1 Monitoring, measurement, analysis and evaluation 9.2 Internal audit 10 Improvement	A.4 Resources for AI systems A.6 AI system life cycle A.7 Data for AI systems A.9 Use of AI systems
	3.2 AI Service	7.4 Communication 7.5 Documented information	A.8 Information for interested parties of AI systems

เอกสารอ้างอิง

C3 AI. n.d. "Best Practices in Developing an Enterprise AI Roadmap." C3 AI. Accessed April 24, 2023. https://c3.ai/wp-content/uploads/2020/06/Best-Practices-in-Developing-an-Enterprise-AI-Roadmap.pdf.

Concordia University and Dawson College. 2021. "ARTIFICIAL INTELLIGENCE COMPETENCY FRAMEWORK." DawsonAI. September. Accessed March 29, 2023. https://www.dawsoncollege.qc.ca/ai/wp-content/uploads/sites/180/Corrected-FINAL_PIA_ConcordiaDawson_AICompetencyFramework.pdf.

Info-Tech Researc Research Group. n.d. "AI Governance A framework for building responsible, ethical, fair, and transparent AI." Info-Tech Researc Research Group. Accessed May 20, 2023. https://www.infotech.com/research/ss/ai-governance.

International Organization for Standardization. 2022. ISO/IEC 22989:2022 Information technology — Artificial intelligence — Artificial intelligence concepts and terminology.

—. 2023. ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management.

—. 2015. ISO/IEC 38500:2015 Information technology — Governance of IT for the organization.

—. 2022. ISO/IEC 38507:2022 Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations.

—. 2021. ISO/IEC TR 24027:2021 Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making.

NASSCOM. n.d. "Responsible AI Architect's Guide Prescribing Responsible AI Best Practices Implementation Methods and Tools for Enterprise Adoption." INDIAai. Accessed April 14, 2023. https://indiaai.gov.in/responsible-ai/pdf/architect-guide.pdf.

National Institute of Standards and Technology (NIST). 2023. "Artificial Intelligence Risk Management Framework (AI RMF 1.0)." AI Risk Management Framework. January. Accessed 06 30, 2023. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

NTT Data Inc. 2022. "AI for Business Value Generation." NTT Data. June. Accessed April 1, 2023. https://es.nttdata.com/documents/whitepaper-e2e-v02.pdf.

Office of the National Digital Economy and Society Commission. 2022. "Thailand AI Ethics Guideline." February 07. https://www.onde.go.th/assets/portals/1/files/Thailand%20AI%20Ethics%20Guideline%20(White%20paper)%20Edit%20Version.pdf.

PRIMO.ai. n.d. Train, Validate, and Test. Accessed 04 13, 2023. http://primo.ai/index.php?title=Train,_Validate,_and_Test.

Scientific American. 2019. Racial Bias Found in a Major Health Care Risk Algorithm. October 24. Accessed March 22, 2023. https://www.scientificamerican.com/article/racial-bias-found-in-a-major-health-care-risk-algorithm/.

The Guardian. 2022. The Guardian. December 22. Accessed March 22, 2023. https://www.theguardian.com/technology/2022/dec/22/tesla-crash-full-self-driving-mode-san-francisco.

The Info-communications Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC). 2020. "Model Artificial Intelligence Governance Framework Second Edition." Model AI Governance Framework. January 21. Accessed April 13, 2023. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf.

The Open Worldwide Application Security Project (OWASP). n.d. "OWASP AI Security and Privacy Guide." OWASP. Accessed April 22, 2023. https://owasp.org/www-project-ai-security-and-privacy-guide/.

The World Economic Forum Centre for the Fourth Industrial Revolution, the Info-communications Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC). 2020. "Implementation and Self Assessment Guide for Organisations (ISAGO)." Accessed 04 13, 2023. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGIsago.pdf.

ภาพกระบวนการพัฒนาแนวทางการประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีธรรมาภิบาล สำหรับผู้บริหารองค์กร (AI Governance Guideline for Executives)



ที่ปรึกษา International Policy Advisory Panel

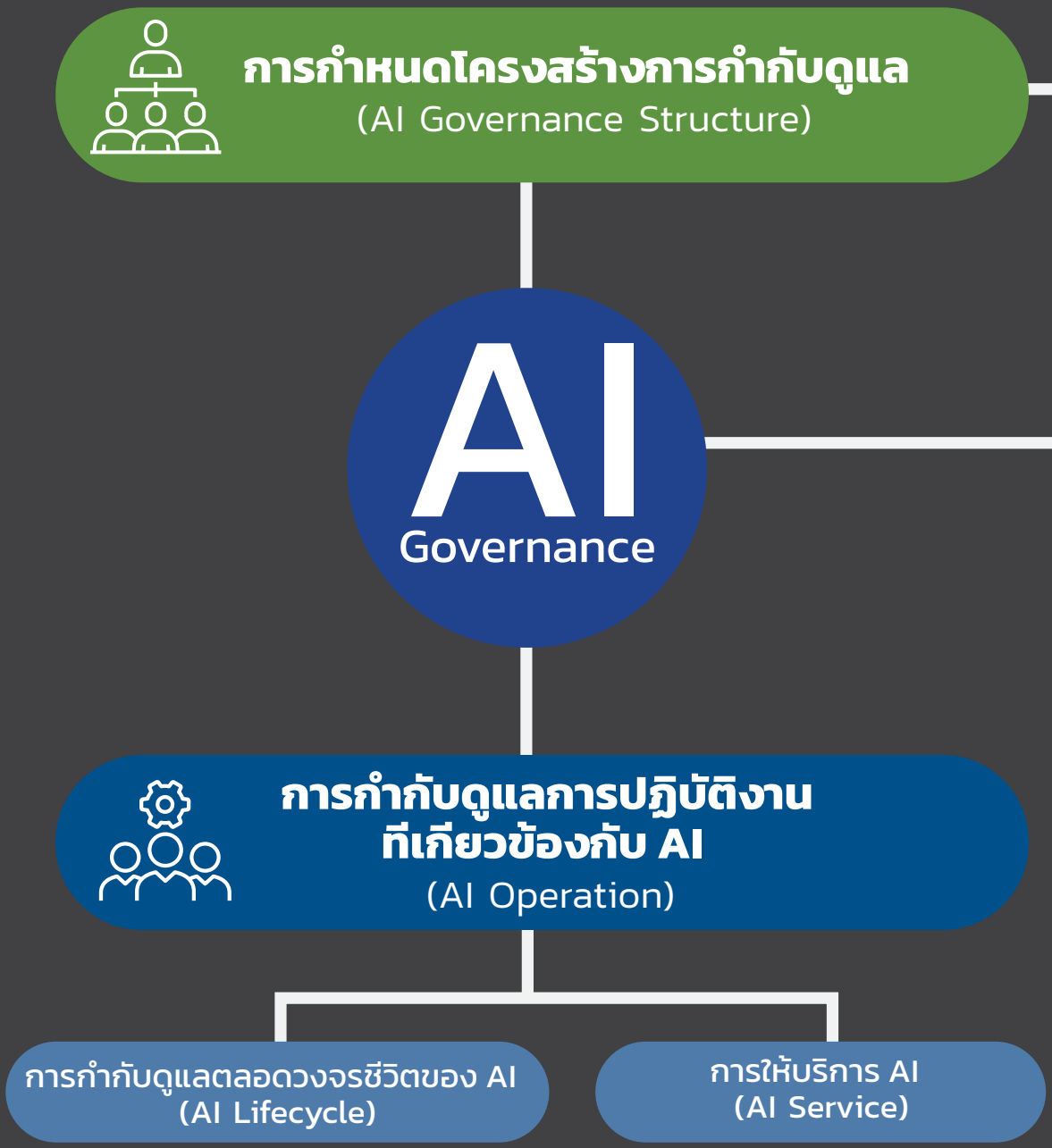
Professor Dr. Urs Gasser
Professor Dr. Christian Fieseler
Professor Dr. Kerstin Vokinger
Professor Peter Parycek
Professor Stefaan Verhulst
Professor Albert Bifet
Dr. Sandra Cortesi
Dr. Nawanan Theera-Ampornpunt
Dr. Rom Hiranpruk

ผู้บริหารสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ดร. ชัยชนะ มิตรพันธ์
ดร. ศักดิ เสกขุนทด
ดร. ชลิตดา มัธยมบุรุษ

คณะทำงาน AIGC

รจนา สำเลิศ
ธิติกร ตระกูลศิริศักดิ์
ธงชัย แสงศิริ
หทัยชนก พุทธรักษา


การกำหนดโครงสร้างการกำกับดูแล
(AI Governance Structure)
AI
Governance
การกำกับดูแลการปฏิบัติงาน
ที่เกี่ยวข้องกับ AI
(AI Operation)
การกำกับดูแลตลอดวงจรชีวิตของ AI
(AI Lifecycle)
การให้บริการ AI
(AI Service)

คณะกรรมการกำกับดูแล
การประยุกต์ใช้ AI
(AI Governance Council)

หน้าที่และความรับผิดชอบ
(Role and Responsibility)

การพัฒนาศักยภาพบุคลากร
(Competency Building)



การกำหนดกลยุทธ์ในการประยุกต์ใช้ AI
(AI Strategy)

การกำหนดกลยุทธ์ใน
การประยุกต์ใช้ AI
อย่างมีความรับผิดชอบ
(Responsible AI Strategy)

การบริหารจัดการความเสี่ยง
จากการประยุกต์ใช้ AI
(AI Risk Management)

AI GOVERNANCE GUIDELINE for EXECUTIVES





ศูนย์ปฏิบัติการด้านธรรมาภิบาล ปัญญาประดิษฐ์
AI GOVERNANCE PRACTICE CENTER (AIGPC)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
02 123 1237 aigpc@etda.or.th