RISK MANAGEMENT MANUAL -2022-

คำนำ

คู่มือ “การบริหารความเสี่ยง (Risk Management Manual)” ฉบับนี้ จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อให้ผู้มีส่วนเกี่ยวข้องในการจัดทำแผนบริหารความเสี่ยงภายในองค์กร มีความเข้าใจหลักการการบริหารความเสี่ยง ความสำคัญและประโยชน์ของการบริหารความเสี่ยง กระบวนการและขั้นตอนการบริหารความเสี่ยง ซึ่งสามารถนำไปประยุกต์ใช้ภายในหน่วยงานได้อย่างเหมาะสม

การนำกระบวนการบริหารความเสี่ยงมาปฏิบัติใช้จริงจะช่วยเป็นหลักประกันในระดับหนึ่งได้ว่าการดำเนินการต่างๆ ขององค์กร หน่วยธุรกิจ และหน่วยปฏิบัติงาน จะสามารถบรรลุผลตามเป้าหมายที่กำหนดไว้ นอกจากนี้ การนำกระบวนการบริหารความเสี่ยงมาเสริมร่วมกับการปฏิบัติงานจะช่วยป้องกันโอกาสที่จะเกิดความเสี่ยงและปัญหาที่จะเป็นอุปสรรคต่อการดำเนินงาน ที่ส่งผลกระทบให้เกิดความเสียหายต่อองค์กรและหน่วยธุรกิจได้

ฝ่ายกลยุทธ์และบริหารการลงทุน

มิถุนายน 2565

สารบัญ

สารบัญภาพ

หน้า

สารบัญตาราง

หน้า

คู่มือการบริหารความเสี่ยง (Risk Management Manual)

นิยาม นโยบายและวัตถุประสงค์การบริหารความเสี่ยงองค์กร

ความเสี่ยง (Risk) หมายถึง ความเป็นไปได้ของเหตุการณ์ที่อาจเกิดขึ้น และส่งผลกระทบต่อการบรรลุกลยุทธ์และวัตถุประสงค์ทางธุรกิจ ทั้งในด้านกลยุทธ์ การปฏิบัติงาน การเงิน และการบริหาร โดยความเสี่ยงนี้จะถูกวัดด้วยผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

รูป 1 แสดงคำนิยามของความเสี่ยง

ความเสี่ยงมี 3 ความหมายสำคัญที่เกี่ยวข้อง ดังนี้

1. เหตุการณ์ (Event)

เหตุการณ์ที่เกิดขึ้นทางด้านลบที่ส่งผลต่อภารกิจองค์กร เกิดได้ทั้งจากปัจจัยภายในและภายนอกองค์กร เช่น ความเสียหายจากเพลิงไหม้ การเสียลูกค้ารายใหญ่ หรือการมีคู่แข่งรายใหม่

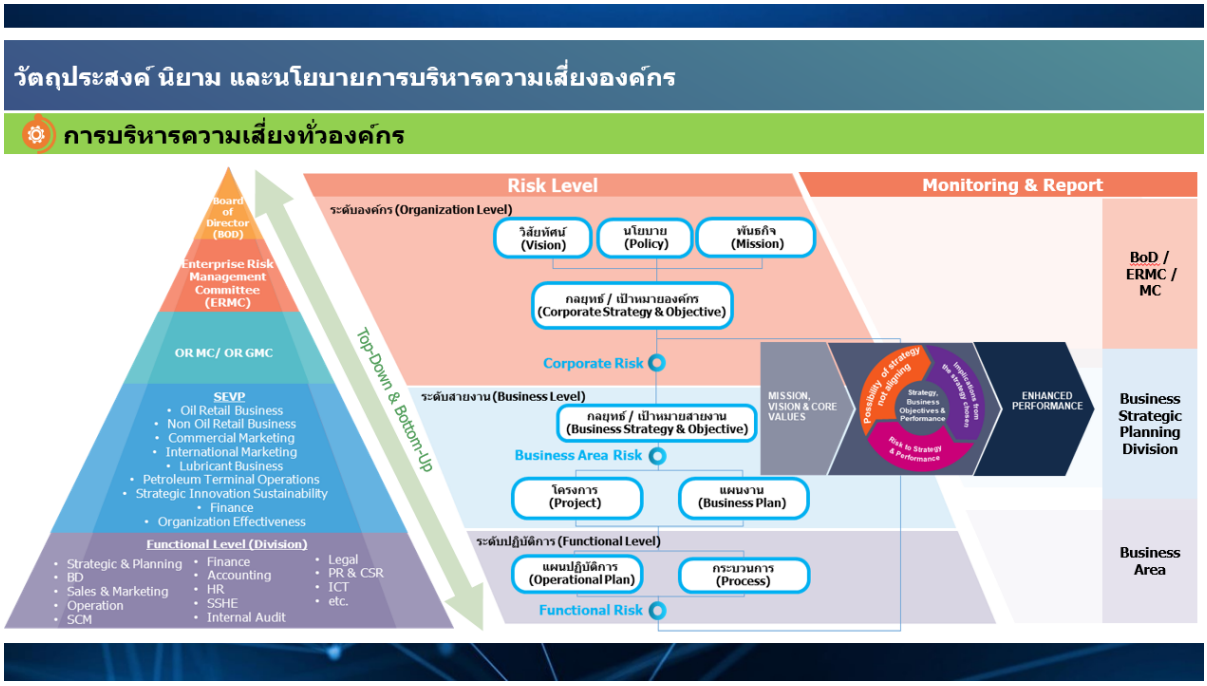
2. ความไม่แน่นอน (Uncertainty)

สถานการณ์ในอนาคตที่ไม่สามารถทำนายสภาวะล่วงหน้า ไม่คาดคิดว่าจะเกิดขึ้นหรือไม่ หรือปรากฏขึ้นอย่างไร

3. ความรุนแรง (Severity)

การประเมินว่าแต่ละเหตุการณ์นั้นมีโอกาสที่จะเกิดมากน้อยเพียงใด และหากเกิดขึ้นแล้วจะส่งผลกระทบต่อองค์กรรุนแรงเพียงใด และนำมาจัดลำดับว่าปัจจัยเสี่ยงใดมีความสำคัญมากน้อยกว่ากัน

การบริหารความเสี่ยงทั่วองค์กร (Enterprise Risk Management) หมายถึง กระบวนการที่คณะกรรมการ ผู้บริหาร และบุคลากร ร่วมในการคิด วิเคราะห์ และคาดการณ์ถึงเหตุการณ์ หรือความเสี่ยงที่อาจจะเกิดขึ้น รวมทั้งการระบุแนวทางในการจัดการกับความเสี่ยงดังกล่าวให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้ เพื่อช่วยให้องค์กรบรรลุในวัตถุประสงค์ที่ต้องการ ตามกรอบวิสัยทัศน์และพันธกิจขององค์กร



รูป 2 แสดงภาพรวมกระบวนการบริหารความเสี่ยงองค์กร

นโยบายการบริหารความเสี่ยงองค์กร การบริหารความเสี่ยงที่มีประสิทธิภาพและประสิทธิผล มีความสำคัญเป็นอย่างยิ่งต่อความยั่งยืนขององค์กร เพื่อให้มั่นใจว่าบริษัทฯ มีความยืดหยุ่นและคล่องตัวเพียงพอในการตอบสนองต่อการเปลี่ยนแปลงของสภาพแวดล้อมทางธุรกิจ และสามารถป้องกันความสูญเสียที่อาจเกิดขึ้น บริษัทฯ จึงกำหนดนโยบายบริหารความเสี่ยง ดังนี้

1. บริษัทฯ กำหนดกระบวนการบริหารความเสี่ยงตามมาตรฐานสากลของ COSO (The Committee of Sponsoring Organizations of the Treadway Commission) และหลักการกำกับดูแลกิจการที่ดีสำหรับบริษัทจดทะเบียนของตลาดหลักทรัพย์แห่งประเทศไทย โดยบูรณาการเข้ากับนโยบายกลยุทธ์ และการดำเนินธุรกิจของบริษัทฯ ให้มีความเชื่อมโยงกันในทุกระดับตลอดทั้งห่วงโซ่คุณค่า สร้างวัฒนธรรมด้านการบริหารความเสี่ยงให้เป็นวิถีปกติของการดำเนินธุรกิจ มีการทบทวนกระบวนการบริหารความเสี่ยงตามรอบระยะเวลาที่เหมาะสม หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

2. บริษัทฯ ถือเป็นหน้าที่ของทุกหน่วยงานในการปฏิบัติตามกระบวนการบริหารความเสี่ยง เพื่อให้บริษัทฯ สามารถบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้อย่างทันต่อเหตุการณ์ และกำหนดให้มีการรายงานผลการบริหารความเสี่ยงตามลำดับชั้นต่อคณะกรรมการจัดการและคณะกรรมการบริษัทตามรอบระยะเวลาที่เหมาะสม หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อสนับสนุนให้บริษัทฯ บรรลุต่อวิสัยทัศน์ พันธกิจ และเป้าหมายที่กำหนดไว้

3. บริษัทฯ ให้ความสำคัญเป็นอย่างยิ่งต่อกระบวนการบริหารความเสี่ยง โดยจัดสรรทรัพยากรที่เกี่ยวข้องและจำเป็นเพื่อสนับสนุนให้การบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

วัตถุประสงค์การบริหารความเสี่ยง เพื่อต้องการให้องค์กรมีกระบวนการหรือระบบในการค้นหา ประเมิน และจัดการกับความเสี่ยงหรือเหตุการณ์ที่ไม่พึงประสงค์ ซึ่งมีโอกาสที่จะเกิดและส่งผลกระทบต่อการดำเนินธุรกิจในภาพรวมขององค์กร ทำให้ไม่บรรลุวัตถุประสงค์ที่วางไว้ โดยการส่งเสริมให้พนักงานทุกคนมีความรู้และความเข้าใจถึงแนวทางในการบริหารความเสี่ยง และให้มีการนำขั้นตอนการบริหารความเสี่ยงไปปฏิบัติทั่วทั้งองค์กร เพื่อการบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ลดโอกาสและความรุนแรงของความเสี่ยง

ตามหลักการ The Committee of Sponsoring Organizations of the Treadway Commission (COSO) ยังให้ความเห็นเพิ่มเติมเกี่ยวกับวัตถุประสงค์ของการบริหารความเสี่ยงอีกว่า องค์กรที่จัดทำระบบบริหารความเสี่ยงได้อย่างมีประสิทธิผลจะช่วยให้บรรลุวัตถุประสงค์ใน 4 ด้าน คือ

1. วัตถุประสงค์ด้านกลยุทธ์ (Strategic) กล่าวคือ การบริหารความเสี่ยงจะช่วยให้องค์กรบรรลุเป้าหมายตามยุทธศาสตร์ ซึ่งสอดคล้องและสนับสนุนพันธกิจหลักขององค์กร

2. วัตถุประสงค์ด้านการปฏิบัติงาน (Operations) การบริหารความเสี่ยงจะช่วยให้องค์กรพิจารณาความคุ้มค่าในการใช้ทรัพยากรต่าง ๆ ในการปฏิบัติงาน รวมถึงพิจารณาประสิทธิภาพและประสิทธิผลของการดำเนินงานด้วย

3. วัตถุประสงค์ด้านการรายงาน (Reporting) การบริหารความเสี่ยงที่มีประสิทธิผลจะช่วยให้ผู้มีส่วนได้ส่วนเสียทุกกลุ่มมีความเชื่อมั่นข้อมูลในรายงานประเภทต่างๆ ขององค์กร โดยเฉพาะรายงานทางการเงิน (Financial Report)

4. วัตถุประสงค์ด้านการปฏิบัติตามกฎระเบียบ (Compliance) โดยเฉพาะการจัดทำระบบควบคุมภายในเพื่อลดความเสี่ยง ส่วนการจัดการความเสี่ยงด้วยวิธีอื่นๆ องค์กรก็สามารถใช้กฎระเบียบต่างๆ เป็นเครื่องมือได้ด้วยเช่นกัน ดังนั้นการบริหารความเสี่ยงจึงส่งเสริมให้หน่วยงานต่างๆ ภายในองค์กร ปฏิบัติตามกฎระเบียบอย่างเคร่งครัดมากยิ่งขึ้น

<u>กรอบและหลักการบริหารความเสี่ยง</u>

กรอบการบริหารความเสี่ยง องค์กรมีการกำหนดกรอบการบริหารความเสี่ยงที่สอดคล้องกับหลักเกณฑ์ของ The Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM 2017 ประกอบด้วยหลักการสำคัญ 5 หลักการและมี 20 องค์ประกอบ โดยองค์กรนำหลักการและองค์ประกอบต่างๆ ไปใช้ในการบริหารความเสี่ยงทั่วทั้งองค์กร สำหรับความเสี่ยงในระดับองค์กรจะมีการบริหารจัดการผ่านคณะกรรมการบริหารความเสี่ยงองค์กร ตามขอบเขตและหน้าที่รับผิดชอบอย่างเป็นระบบ ความเสี่ยงในระดับหน่วยธุรกิจและระดับสายปฏิบัติงานจะอยู่ภายใต้การกำกับดูแลของผู้บริหารที่รับผิดชอบ โดยถือเป็นหน้าที่รับผิดชอบของทุกหน่วยงานในการบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

รูป 3 กรอบการบริหารความเสี่ยง COSO ERM 2017

หลักการบริหารความเสี่ยง หลักการสำคัญของการบริหารความเสี่ยงตามแนวคิดของ COSO ERM 2017 แบ่งออกเป็น 5 หลักการ หลักการเหล่านี้ต้องเกี่ยวเนื่องและมีความสัมพันธ์ต่อกันเพื่อให้เกิดการบรรลุวัตถุประสงค์ของการบริหารความเสี่ยง หลักการสำคัญทั้ง 5 หลักการ ได้แก่

1. การกำกับดูแลกิจการและวัฒนธรรมองค์กร
2. กลยุทธ์และการกำหนดวัตถุประสงค์
3. ผลการดำเนินงาน
4. การทบทวนและปรับปรุงกระบวนการบริหารความเสี่ยง
5. การรายงานผลการบริหารความเสี่ยง

<u>หลักการสำคัญที่ 1. การกำกับดูแลกิจการและวัฒนธรรมองค์กร (Governance and Culture)</u>

การกำกับดูแลกิจการและวัฒนธรรมองค์กรเป็นพื้นฐานขององค์ประกอบทั้งหมดในการบริหารความเสี่ยงเนื่องจากการกำกับดูแลกิจการจะเป็นสิ่งกำหนดแนวทางขององค์กรในการให้ความสำคัญและสร้างความรับผิดชอบเกี่ยวกับการบริหารความเสี่ยง วัฒนธรรมองค์กรจะเกี่ยวข้องกับค่านิยมทางจริยธรรมพฤติกรรมที่พึงประสงค์ และความเข้าใจเกี่ยวกับความเสี่ยงขององค์กร ซึ่งจะสะท้อนผ่านการตัดสินใจต่างๆ COSO ถือว่าการกำกับดูแลกิจการและวัฒนธรรมองค์กรเป็นองค์ประกอบที่สำคัญยิ่ง เป็นองค์ประกอบพื้นฐานหลักให้องค์ประกอบอื่นๆ เกิดขึ้นหรือเสมือนเป็นรากฐานสำคัญให้เกิดการบริหารความเสี่ยงขึ้นในองค์กร

OR ได้กำหนดวิสัยทัศน์ พันธกิจ และค่านิยมขององค์กร แสดงให้เห็นถึงความมุ่งมั่นที่ต้องปฏิบัติตาม และมีการแต่งตั้งคณะกรรมการบริหารความเสี่ยงองค์กรเพื่อทำหน้าที่ในการกำหนดนโยบายกรอบการบริหารความเสี่ยง กำกับดูแลและสนับสนุนให้การดำเนินงานด้านการบริหารความเสี่ยงองค์กรสอดคล้องกับกลยุทธ์และเป้าหมายทางธุรกิจ และให้ข้อคิดเห็นในการนำไปปรับปรุงประสิทธิภาพของการบริหารจัดการความเสี่ยงอย่างไม่หยุดนิ่ง เพื่อตอบสนองต่อความเสี่ยงได้อย่างทันท่วงทีและสร้างความพร้อมในการรองรับความเสี่ยงของธุรกิจในทุกด้าน

<u>วิสัยทัศน์องค์กร</u>

OR เติมเต็มโอกาส เพื่อทุกการเติบโต ร่วมกัน

<u>พันธกิจองค์กร</u>

- Seamless Mobility

  สร้างความแข็งแกร่งให้กับธุรกิจพลังงานแบบผสมผสานเพื่อการเคลื่อนที่อย่างไร้รอยต่อ

- All Lifestyles

  มุ่งมั่นสร้างทางเลือกสำหรับการดำเนินชีวิตแบบครบวงจรเพื่อตอบโจทย์การใช้ชีวิตทุกรูปแบบ

- Global Market

  ขยายฐานธุรกิจเพื่อสร้างความสำเร็จและการยอมรับในตลาดโลก

- OR Innovation

  แก้ปัญหาสังคมและสิ่งแวดล้อมเพื่อยกระดับสู่นวัตกรรมในแบบฉบับ OR

รูป 4 แสดงวิสัยทัศน์และพันธกิจขององค์กรในด้านต่าง ๆ

<u>ค่านิยมองค์กร</u>

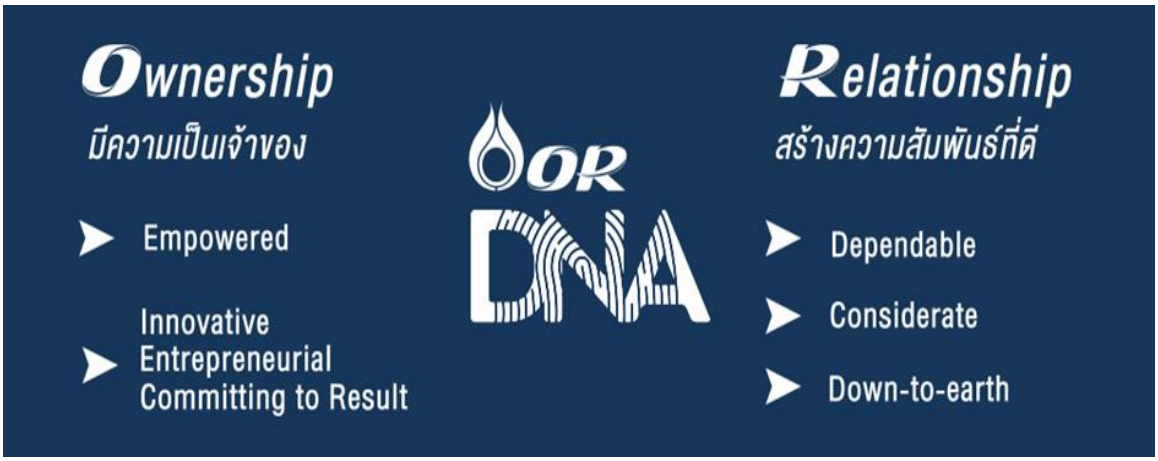
OR มุ่งเน้นการเสริมสร้างและปลูกฝังวัฒนธรรมองค์กร OR DNA เพื่อเป็นพื้นฐานที่สำคัญในการหล่อหลอมให้ผู้บริหารและพนักงานมีแนวคิดและวิถีการทำงานที่สอดคล้องกับวิสัยทัศน์ พันธกิจ ทิศทางกลยุทธ์ ทั้งยังเป็นปัจจัยสำคัญที่ช่วยเสริมสร้างพฤติกรรมการทำงานของพนักงานและผู้บริหาร ช่วยขับเคลื่อนการดำเนินธุรกิจของ OR ให้บรรลุเป้าหมายที่ตั้งไว้และสะท้อนวัฒนธรรมที่เข้มแข็งของ OR พร้อมทั้งสามารถสะท้อนความเป็น OR ผ่านศักยภาพของพนักงาน

OR ดำเนินการเชื่อมโยง OR DNA สู่การพัฒนาบุคลากร ผ่านการกำหนดความสามารถ (Competencies) ที่จะช่วยขับเคลื่อนการดำเนินธุรกิจที่มีการปรับเปลี่ยนในอนาคตให้บรรลุเป้าหมาย

ที่ตั้งไว้ และนำไปสู่การพัฒนาและหมุนเวียนงานตาม Success Profile เพื่อพัฒนาความสามารถ (Competencies) และประสบการณ์ตามเส้นทางความก้าวหน้าในอาชีพ (Career Path) อย่างเป็นระบบ อีกทั้งยังสร้างความตระหนักรู้ให้กับพนักงานผ่านการสื่อสารช่องทางต่างๆ เช่น อีเมล์ (E-mail) และส่งเสริมให้ผู้บริหารประพฤติตนเป็นแบบอย่างที่ดี (Role Model) ภายใต้วิถีการทำงานแบบ OR DNA ซึ่งผู้บริหารเป็นผู้ที่มีบทบาทสำคัญในการผลักดันและส่งเสริมให้พนักงานเกิดความตระหนักรู้ถึงความสำคัญของวัฒนธรรมองค์กร OR DNA และนำไปสู่การปฏิบัติต่อไป

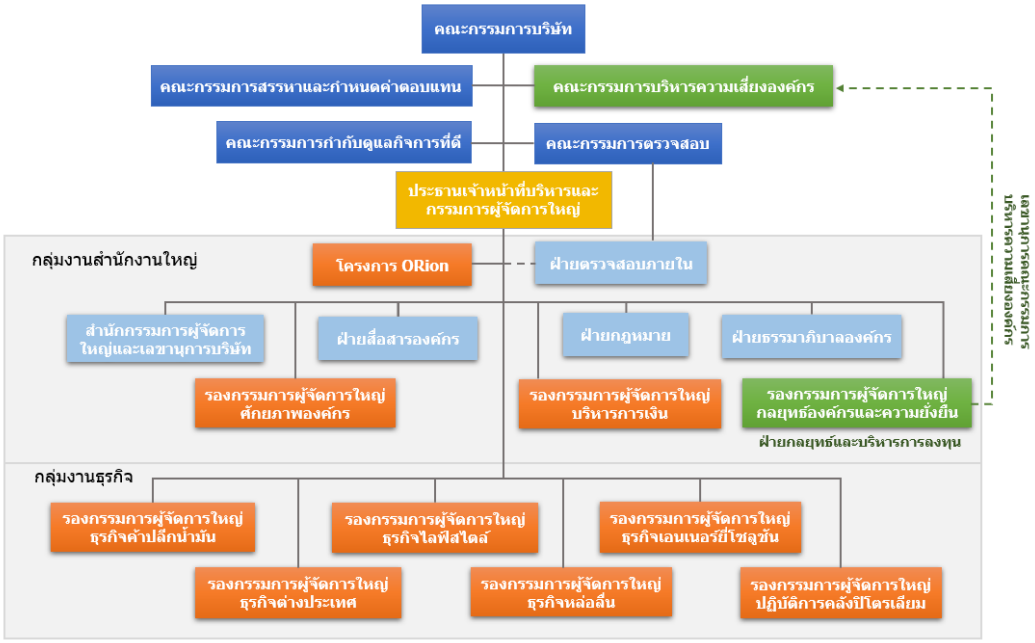
โดย OR DNA นี้จะเป็นพฤติกรรมพึงประสงค์ที่ OR คาดหวังให้พนักงานตลอดจนผู้บริหารทุกคนแสดงออก ซึ่งประกอบไปด้วย 5 ข้อ ได้แก่

1. เชื่อมั่นในศักยภาพ กล้าตัดสินใจ และเปิดโอกาสให้พนักงานลงมือทำ แนะนำเพื่อพัฒนา (Empowerment)
2. มีความคิดสร้างสรรค์พร้อมจิตวิญญาณในความเป็นเจ้าของ และมุ่งมั่นสู่ผลลัพธ์ (Innovative Entrepreneur Committing to Result)
3. มีความน่าเชื่อถือ ไว้วางใจได้ และยืนหยัดทำในสิ่งที่ถูกต้อง (Dependability)
4. ใส่ใจ คิดถึงผู้อื่น และไม่เอาตัวเองรอด (Consideration)
5. เข้าถึงได้ง่าย และไม่ถือตัว (Down to Earth)



รูป 5 แสดงค่านิยมขององค์กร

คณะกรรมการบริหารความเสี่ยงองค์กร



รูป 6 แสดงผังการบริหารขององค์กร

คณะกรรมการ บริษัท ปตท. น้ำมันและการค้าปลีก จำกัด (มหาชน) ให้ความสำคัญอย่างยิ่งต่อการบริหารความเสี่ยงที่มีประสิทธิภาพ เพื่อสร้างความเชื่อมั่นต่อการบรรลุเป้าหมายองค์กรในการเติบโตอย่างยั่งยืนภายใต้สภาพแวดล้อมและความไม่แน่นอนในการดำเนินธุรกิจ จึงได้อนุมัติแต่งตั้งคณะกรรมการบริหารความเสี่ยงองค์กร (Enterprise Risk Management Committee : ERMC) เมื่อวันที่ 15 พฤษภาคม 2562 โดยมีหน้าที่และความรับผิดชอบ ในการกำหนดนโยบาย กรอบการบริหารความเสี่ยง กำกับดูแลการดำเนินงานด้านการบริหารความเสี่ยงองค์กรให้สอดคล้องกับกลยุทธ์และเป้าหมายองค์กร รวมทั้งให้ข้อเสนอแนะแนวทางการบริหารความเสี่ยงให้เกิดประสิทธิภาพทั้งในด้านกลยุทธ์ ด้านการปฏิบัติการและธุรกิจ ด้านการปฏิบัติตามกฎหมาย/กฎระเบียบ ด้านการเงิน และด้านเทคโนโลยีสารสนเทศ

หลักการสำคัญที่ 2. กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy and Objective-Setting)

การบริหารความเสี่ยงสามารถบูรณาการเข้ากับแผนยุทธศาสตร์ขององค์กรผ่านกระบวนการกำหนดกลยุทธ์และวัตถุประสงค์ทางธุรกิจ โดยองค์กรควรกำหนดความเสี่ยงที่ยอมรับได้ให้สอดคล้องกับการกำหนดกลยุทธ์ นอกจากนี้ วัตถุประสงค์ทางธุรกิจจะเป็นสิ่งที่กำหนดแนวทางปฏิบัติตามกลยุทธ์

การดำเนินงานทั่วไป ปัจจัยที่องค์กรให้ความสำคัญ ทั้งยังเป็นพื้นฐานในการระบุ ประเมิน และการตอบสนองต่อความเสี่ยง

การบริหารความเสี่ยงที่มีประสิทธิภาพเป็นเครื่องมือที่สำคัญของบริษัทฯ เพื่อสร้างความเชื่อมั่นว่า บริษัทฯ สามารถบรรลุวิสัยทัศน์ พันธกิจ และเป้าหมายของบริษัทฯ โดยกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) เพื่อเป็นกรอบในการดำเนินงานภายใต้ความไม่แน่นอนของสภาพแวดล้อมทางธุรกิจ เพื่อให้มั่นใจได้ว่าบริษัทฯ มีการติดตามการดำเนินธุรกิจอย่างเหมาะสม มีความยืดหยุ่นและความคล่องตัวเพียงพอในการปรับเปลี่ยนการบริหารจัดการให้สอดคล้องกับระดับความเสี่ยงที่บริษัทฯ มีอยู่และอยู่ในระดับที่ยอมรับได้ ดังนี้

1. บริษัทฯ ไม่ยอมรับความเสี่ยงของการลงทุนโดยรวมที่มีผลตอบแทนจากการลงทุนต่ำกว่าต้นทุนของเงินทุนถัวเฉลี่ยถ่วงน้ำหนัก (Weighted Average Cost of Capital : WACC) ในระยะยาว ยกเว้นการลงทุนที่มีเป้าหมายเชิงกลยุทธ์ เพื่อขยายโอกาสทางธุรกิจใหม่และสร้างมูลค่าเพิ่มให้กับกิจการในอนาคตทั้งในประเทศและต่างประเทศ โดยเป็นไปตามแนวทางการดำเนินธุรกิจอย่างยั่งยืนตามมาตรฐานสากลและ Triple Bottom Line ทั้งด้านสังคม ชุมชน (People) สิ่งแวดล้อม (Planet) และผลประกอบการ (Performance)

2. บริษัทฯ ให้ความสำคัญเป็นอย่างยิ่งต่อชื่อเสียงและภาพลักษณ์องค์กร หลีกเลี่ยงการดำเนินธุรกิจที่อาจนำมาซึ่งการเสื่อมเสียชื่อเสียงหรือส่งผลกระทบต่อภาพลักษณ์องค์กร และดำเนินธุรกิจตามแนวทางการบริหารจัดการความยั่งยืน มีระบบปฏิบัติการที่เป็นไปตามกฎหมายและมาตรฐานสากล ให้ความสำคัญกับความมั่นคง ความปลอดภัย อาชีวอนามัย และสิ่งแวดล้อม โดยไม่ยอมรับอุบัติการณ์ใหญ่หลวงตามนิยามด้านความปลอดภัย (No Catastrophic Accident)

3. บริษัทฯ กำหนดกลยุทธ์ด้านเทคโนโลยีสารสนเทศเพื่อสนับสนุนการดำเนินธุรกิจให้มีประสิทธิภาพ มีการรักษาความมั่นคงและความปลอดภัยด้านไซเบอร์ที่เหมาะสม โดยไม่ยอมรับการรั่วไหลของข้อมูลตามที่กฎหมายกำหนด หรือการรั่วไหลของข้อมูลที่จะส่งผลกระทบต่อการดำเนินธุรกิจอย่างมีนัยสำคัญ

4. บริษัทฯ กำหนดให้มีกระแสเงินสด (Cash Flow) และสภาพคล่องทางการเงิน (Financial Liquidity) ในระดับที่เพียงพอต่อการชำระหนี้ ภาระผูกพัน และการลงทุน โดยมีอัตราส่วนทางการเงิน (Financial Ratio) เป็นไปตามนโยบายทางการเงินของกลุ่ม ปตท.

5. บริษัทฯ คำนึงถึงความต้องการและความคาดหวังของผู้มีส่วนได้เสียทุกกลุ่ม มุ่งมั่นสร้างคุณค่าร่วมให้เกิดแก่ผู้มีส่วนได้เสียทุกกลุ่มอย่างสมดุล ยึดมั่นในการดำเนินธุรกิจตามกฎหมาย มี

จริยธรรม ด้วยความโปร่งใส เป็นธรรม เท่าเทียม ไม่ยอมรับการทุจริตคอร์รัปชันทุกรูปแบบ โดยกำหนดนโยบายการกำกับดูแลกิจการที่ดีที่สอดคล้องกับหลักการกำกับดูแลกิจการที่ดีสำหรับบริษัทจดทะเบียนของตลาดหลักทรัพย์แห่งประเทศไทย เพื่อให้บุคลากรทุกระดับและผู้มีส่วนได้เสียทุกกลุ่มยึดถือเป็นบรรทัดฐานในการปฏิบัติงานและดำเนินธุรกิจร่วมกัน

หลักการสำคัญที่ 3. ผลการดำเนินงาน (Performance)

ในการประเมินผลการดำเนินงานขององค์กร เริ่มจากการระบุและประเมินความเสี่ยงในระดับหน่วยธุรกิจที่อาจส่งผลต่อความสามารถในการบรรลุกลยุทธ์และวัตถุประสงค์ทางธุรกิจก่อน และค่อยรวบรวมมาเป็นความเสี่ยงองค์กร โดยจัดลำดับความสำคัญของความเสี่ยงตามโอกาสและผลกระทบที่อาจเกิดขึ้น และพิจารณาความเสี่ยงที่องค์กรยอมรับได้ จากนั้นองค์กรจะเลือกตอบสนองต่อความเสี่ยงด้วยวิธีต่างๆ รวมถึงพิจารณาปริมาณความเสี่ยงในภาพรวมและตรวจสอบผลการดำเนินงานเพื่อเปลี่ยนแปลงแก้ไขซึ่งจะพัฒนามุมมองในภาพรวมเกี่ยวกับปริมาณความเสี่ยงที่องค์กรอาจเผชิญในการบรรลุเป้าหมายกลยุทธ์และวัตถุประสงค์ทางธุรกิจในระดับองค์กร

3.1 การระบุความเสี่ยง

การระบุความเสี่ยงเป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องกับการดำเนินงาน เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยงที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ โดยต้องคำนึงถึงปัจจัยเสี่ยงที่กระทบต่อองค์กรซึ่งสามารถแบ่งออกได้เป็น 2 ประเภท

1. ปัจจัยภายใน เช่น โครงสร้างองค์กร กระบวนการและวิธีการปฏิบัติงาน วัฒนธรรมองค์กร ปรัชญาการบริหารความเสี่ยงและระดับความเสี่ยงที่ยอมรับได้ของผู้บริหาร
2. ปัจจัยภายนอก เช่น ภาวะเศรษฐกิจ การเมืองทั้งในประเทศและต่างประเทศ ความก้าวหน้าทางเทคโนโลยี กฎเกณฑ์การกำกับดูแลของหน่วยงานที่เกี่ยวข้อง

เนื่องจากความเสี่ยงมีมากมายหลายเรื่อง หลายแหล่งที่มา การรวบรวมความเสี่ยงเป็นประเภทต่างๆ จะทำให้สามารถระบุความเสี่ยงที่ส่งผลกระทบต่อองค์กรได้อย่างชัดเจนและครอบคลุม จึงแบ่งความเสี่ยงออกเป็น 5 ประเภท ได้แก่

1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) เป็นความเสี่ยงที่เกิดขึ้นจากปัจจัยเสี่ยงต่างๆ ที่ส่งผลต่อวัตถุประสงค์เชิงกลยุทธ์ หรือเกิดจากการกำหนดแผนกลยุทธ์ แผนดำเนินงานที่นำไปปฏิบัติไม่เหมาะสมหรือไม่สอดคล้องกับปัจจัยภายในและสภาพแวดล้อมภายนอก อันส่งผลกระทบต่อการบรรลุวิสัยทัศน์และพันธกิจ
2. ความเสี่ยงด้านปฏิบัติการและธุรกิจ (Operational and Business Risk) เป็นความเสี่ยงที่เกิดจากการกระบวนการปฏิบัติงาน ซึ่งส่งผลให้องค์กรไม่สามารถบรรลุวัตถุประสงค์และเป้าหมายที่กำหนด อันเนื่องมาจากการขาดการกำกับดูแลหรือขาดการควบคุมภายในที่เหมาะสม
3. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) เป็นความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินธุรกิจ ส่งผลกระทบต่อระบบหรือการปฏิบัติงานของบริษัท รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์
4. ความเสี่ยงด้านการเงิน (Financial Risk) เป็นความเสี่ยงที่เกิดการบริหารจัดการทางการเงิน สภาพคล่องและงบการเงินขององค์กร
5. ความเสี่ยงด้านการปฏิบัติตามกฎหมาย/กฎระเบียบ (Compliance Risk) เป็นความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามกฎหมาย กฎระเบียบ ข้อบังคับ ซึ่งครอบคลุมถึงกฎระเบียบของทั้งหน่วยงานภายในและภายนอก

รูป 7 แสดงถึงประเภทความเสี่ยง คำจำกัดความ และตัวอย่างความเสี่ยงแต่ละประเภท

การระบุสาเหตุของความเสี่ยงสามารถทำได้หลายวิธี ดังนี้

1. การระดมความคิด (Brainstorming) ถือเป็นวิธีหนึ่งที่ฝ่ายบริหารและผู้ที่เกี่ยวข้องสามารถช่วยกันระบุสาเหตุความเสี่ยงต่างๆ ที่ทำให้องค์กร/หน่วยธุรกิจไม่สามารถบรรลุวัตถุประสงค์นั้นๆ ได้ การระดมความคิดจะประสบความสำเร็จได้ หากมีการระดมความคิดจากตัวแทนหลายๆ ฝ่ายในองค์กร/หน่วยธุรกิจ เพราะตัวแทนเหล่านั้นจะสามารถสะท้อนความคิดเห็นออกมาในมุมมองที่หลากหลาย อีกทั้งยังสามารถบอกได้ว่า หากความเสี่ยงนั้นเกิดขึ้นจริงจะกระทบแต่ละฝ่ายอย่างไร

2. การวิเคราะห์ข้อมูลและเหตุการณ์ในอดีต สิ่งหนึ่งที่จะทำให้การระดมความคิดมีประสิทธิภาพมากยิ่งขึ้นก็คือ การนำเข้าข้อมูลเหตุการณ์ความเสี่ยงที่เคยเกิดขึ้นในอดีต หรือข้อมูลที่ส่งผลเสียหายต่อองค์กร/หน่วยธุรกิจมาพิจารณาร่วมกัน จึงถือเป็นเครื่องมือที่จะช่วยให้ฝ่ายบริหารและผู้ที่เกี่ยวข้องคำนึงถึงความเสี่ยงได้ครบถ้วน ล่วงรู้ถึงสาเหตุที่ความเสี่ยงเหล่านั้นอาจเกิดขึ้นได้

3. การสัมภาษณ์และการประเมินตนเอง (Interviews and Self-Assessment) วิธีนี้เป็นการผสมผสาน 2 วิธีเข้าด้วยกัน โดยวิธีแรกคือ การให้แต่ละคนในหน่วยงานปฏิบัติการ ประเมินว่าในหน้าที่ความรับผิดชอบของตนเองว่ามีความเสี่ยงใดบ้างที่จะทำให้ตนไม่สามารถทำได้ตามแผนหรือวัตถุประสงค์ที่กำหนดไว้และความเสี่ยงเหล่านั้นเกิดจากสาเหตุใด อีกหนึ่งวิธีที่จะช่วยให้ได้ข้อมูลที่ละเอียดมากขึ้นจากผู้ที่ปฏิบัติงานเกี่ยวกับความเสี่ยงก็คือ การสัมภาษณ์ ซึ่งวิธีนี้จะได้ข้อมูลที่ตรงกับความต้องการมากขึ้น

4. การทดลองปฏิบัติการ (Facilitated Workshop) ภายหลังจากที่ได้ข้อมูลความเสี่ยงแล้ว การที่ผู้บริหารและผู้ที่เกี่ยวข้องเข้ามามีส่วนร่วมในการทดลองปฏิบัติการ โดยการหารือและวิเคราะห์จากการจำลองเหตุการณ์ หากเกิดความเสี่ยงขึ้นจริงจะให้ช่วยเห็นภาพของความเสี่ยงองค์กร/หน่วยธุรกิจมากขึ้น

5. การวิเคราะห์สถานการณ์ (Scenario Analysis) วิธีนี้เป็นวิธีที่มีประโยชน์ในการช่วยระบุสาเหตุความเสี่ยงทางด้านกลยุทธ์ โดยเฉพาะในสถานการณ์ที่ยากจะระบุได้ กล่าวคือ เป็นวิธีเดียวที่จะสามารถค้นพบความเสี่ยงที่มีผลกระทบต่อองค์กร/หน่วยธุรกิจสูง แต่มีโอกาสเกิดขึ้นน้อยนั่นเอง

<u>3.2 เกณฑ์การประเมินระดับความรุนแรงของความเสี่ยง</u>

การกำหนดเกณฑ์สำหรับการประเมินระดับความรุนแรงของความเสี่ยง เป็นองค์ประกอบที่สำคัญเนื่องจากจะใช้ในการจัดลำดับความสำคัญความเสี่ยงต่อไป เกณฑ์ที่จะใช้ประกอบการประเมิน

ระดับความรุนแรงความเสี่ยงนั้นประกอบด้วย 2 องค์ประกอบ ได้แก่ ระดับโอกาสที่ความเสี่ยงอาจเกิดขึ้น (Likelihood) และระดับความรุนแรงของผลกระทบที่เกิดขึ้นจากความเสี่ยง (Impact) แบ่งออกได้เป็น 2 ลักษณะ ได้แก่ ผลกระทบที่เป็นตัวเงิน (Financial Impact) และผลกระทบที่ไม่เป็นตัวเงิน (Non-Financial Impact) โดยใช้ฐานข้อมูลในอดีต หรือการคาดการณ์ในอนาคต ตัวอย่างผลกระทบที่เป็นตัวเงิน ได้แก่ ผลกระทบต่อประมาณการรายได้และค่าใช้จ่ายหรือการลดลงของเป้าหมายกำไรของกิจการ ตัวอย่างผลกระทบที่ไม่ใช่ตัวเงิน ได้แก่ ภาพลักษณ์และชื่อเสียงของกิจการ เกณฑ์การประเมินค่าความเสี่ยงจะขึ้นอยู่กับค่าระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite)

1. ระดับโอกาสที่ความเสี่ยงอาจเกิดขึ้น (Likelihood) เป็นการพิจารณาความเป็นไปได้ที่จะเกิดเหตุการณ์ความเสี่ยงในช่วงเวลาหนึ่ง หรือจะเรียกว่า ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงก็ได้

<u>เกณฑ์การวัดระดับโอกาสในการเกิดความเสี่ยง</u>

ตาราง 1 แสดงเงื่อนไขการประเมินระดับโอกาสในการเกิดความเสี่ยง

หัวข้อ	ความถี่โดยเฉลี่ย			
	4 น่าจะเกิด Likely	3 เป็นไปได้ที่จะเกิด Possible	2 ไม่น่าจะเกิด Unlikely	1 ยากที่จะเกิด Rare
โอกาสเกิดเหตุการณ์	คาดว่าเหตุการณ์นี้มีโอกาสเกิดขึ้นสูงมากในทุกสถานการณ์ มีโอกาสเกิดเหตุการณ์มากกว่า 90% ภายในระยะเวลา 12 เดือนข้างหน้า	คาดว่าเหตุการณ์นี้อาจจะเกิดขึ้นได้ในสภาพการณ์ส่วนใหญ่มีโอกาสเกิด 50-90% ภายในระยะเวลา 12 เดือนข้างหน้า	คาดว่าเหตุการณ์นี้อาจจะเกิดขึ้นได้ในบางเวลาเท่านั้น มีโอกาสเกิด 10-50% ภายในระยะเวลา 12 เดือนข้างหน้า	คาดว่าเหตุการณ์นี้อาจจะเกิดขึ้นได้เมื่อเกิดสภาพการณ์ผิดปกติเท่านั้น มีโอกาสเกิดน้อยกว่า 10% ภายในระยะเวลา 12 เดือนข้างหน้า
ความถี่ของการเกิดเหตุการณ์ (Quality, Safety, Environment)	โอกาสเกิดปีละ 12 ครั้ง หรือเกิดทุกเดือน	โอกาสเกิดปีละ 7-11 ครั้ง	โอกาสเกิดปีละ 2-6 ครั้ง	โอกาสเกิดปีละ 1 ครั้ง

2. ระดับความรุนแรงของผลกระทบที่เกิดขึ้นจากความเสี่ยง (Impact) ระดับความรุนแรงของผลเสียหายที่เกิดขึ้นจากความเสี่ยงและมีผลกระทบต่อองค์กรซึ่งอาจเป็นได้ทั้งในด้านบวกและด้านลบ โดยสามารถแบ่งเป็นผลกระทบทางด้านการเงินและผลกระทบที่ไม่ใช่ทางการเงิน

เกณฑ์การวัดระดับความรุนแรงของผลกระทบด้านการเงิน (Financial Impact)

ตาราง 2 แสดงเงื่อนไขการประเมินระดับความรุนแรงของผลกระทบด้านการเงิน

หัวข้อ	ระดับความรุนแรง			
	4 รุนแรง	3 สูง	2 ปานกลาง	1 น้อย
OPEX เพิ่มขึ้น (% ของค่าใช้จ่ายเทียบจากแผน)	$> 0.5\%$	$> 0.25\%$ ถึง $\leq 0.5\%$	$> 0.125\%$ ถึง $\leq 0.25\%$	$\leq 0.125\%$
EBITDA ลดลง (%ของ EBITDA เทียบจากแผน)	$> 5\%$	$> 2.5\%$ ถึง $\leq 5\%$	$> 1.25\%$ ถึง $\leq 2.5\%$	$\leq 1.25\%$

เกณฑ์การวัดระดับความรุนแรงของผลกระทบที่ไม่ใช่ด้านการเงิน (Non-Financial Impact)

ตาราง 3 เกณฑ์การวัดระดับความรุนแรงของผลกระทบที่ไม่ใช่ด้านการเงิน (Non-Financial Impact)

หัวข้อ	ระดับความรุนแรง			
	4 รุนแรง	3 สูง	2 ปานกลาง	1 น้อย
กระบวนการและขั้นตอนการดำเนินงาน	กระบวนการหลักไม่เกิดประสิทธิผล หรือเกิดความล่าช้าในการดำเนินงานมากกว่า 50% เทียบแผนงาน	กระบวนการหลักไม่มีประสิทธิภาพค่อนข้างมาก เกิดความล่าช้าในการดำเนินงานมากกว่า 25% เทียบแผนงาน	กระบวนการหลักไม่มีประสิทธิภาพปานกลาง เกิดความล่าช้าในการดำเนินงานมากกว่า 10% เทียบแผนงาน	กระบวนการหลักไม่มีประสิทธิภาพเล็กน้อย เกิดความล่าช้าในการดำเนินงานไม่เกิน 10% เทียบแผนงาน
	-	-	กระบวนการที่ไม่ใช่กระบวนการหลักไม่เกิดประสิทธิผล หรือเกิดความล่าช้าในการดำเนินงานมากกว่า 50%	กระบวนการที่ไม่ใช่กระบวนการหลักไม่มีประสิทธิภาพ เกิดความล่าช้าในการดำเนินงานน้อยกว่า 50% เทียบแผนงาน
เทคโนโลยี	กระทบต่อกระบวนการทำงานหลัก ทำให้ข้อมูลรั่วไหลออกสู่ภายนอกองค์กร และก่อให้เกิดความเสียหาย	กระทบต่อกระบวนการทำงานหลัก ทำให้ข้อมูลรั่วไหลออกสู่ภายนอกองค์กร และไม่ก่อให้เกิดความเสียหาย	กระทบต่อกระบวนการทำงานหลัก	กระทบต่อกระบวนการปฏิบัติงานทั่วไป

หัวข้อ	ระดับความรุนแรง			
	4 รุนแรง	3 สูง	2 ปานกลาง	1 น้อย
กฎหมาย	โทษอาญาจำคุก ผู้แทนนิติบุคคล	โทษอาญาจำคุกผู้กระทำ	โทษปรับ	ไม่มีโทษทางอาญา และไม่มีโทษปรับ
	เพิกถอนใบอนุญาต	ต้องหยุดปฏิบัติงานชั่วคราว		
	ความผิดเกี่ยวกับการทุจริต	-	-	-
กฎระเบียบภายในองค์กร	ไม่ปฏิบัติตามกฎระเบียบภายในองค์กร ถือเป็นความผิดร้ายแรง ถูกพักงานโดยไม่จ่ายค่าจ้าง หรือ ถูกเลิกจ้างโดยจ่ายค่าชดเชย หรือไม่จ่ายค่าชดเชย แล้วแต่กรณีหรือสาเหตุแห่งการกระทำความผิด	ไม่ปฏิบัติตามกฎระเบียบภายในองค์กร ถือเป็นความผิดปานกลาง ถูกงดขึ้นเงินเดือนในปีถัดไป แต่ไม่เกิน 6 เดือน	ไม่ปฏิบัติตามกฎระเบียบภายในองค์กร ถือเป็นความผิดเล็กน้อย ถูกตักเตือนเป็นลายลักษณ์อักษร	ไม่ปฏิบัติตามกฎระเบียบภายในเล็กน้อย ไม่มีความผิดทางวินัย
ความพึงพอใจและชื่อเสียง	ผู้มีส่วนได้ส่วนเสียเกิดความไม่พึงพอใจ จนอาจเกิดการประท้วงหรือฟ้องร้ององค์กร และ/หรือ ต่อต้านการใช้สินค้าและบริการของ OR	ผู้มีส่วนได้ส่วนเสียเกิดความไม่พึงพอใจ โดยแสดงความคิดเห็นผ่านทางโซเชียลมีเดีย และ/หรือ เลิกใช้สินค้าและบริการของ OR	ผู้มีส่วนได้ส่วนเสียเกิดความไม่พึงพอใจ โดยดำเนินการร้องเรียนต่อองค์กร และ/หรือ ลดการใช้สินค้าและบริการของ OR	ผู้มีส่วนได้ส่วนเสียเกิดความไม่พึงพอใจ โดยมีการเสนอแนะเพื่อปรับปรุง และ/หรือ ยังคงใช้สินค้าและบริการของ OR
ความปลอดภัย	เกิดอันตรายถึงชีวิตหรือทุพพลภาพ	ได้รับบาดเจ็บ ต้องหยุดรักษาและถูกจำกัดลักษณะงาน	ได้รับบาดเจ็บ ต้องหยุดรักษา แต่ไม่ถูกจำกัดลักษณะงาน	ได้รับบาดเจ็บเล็กน้อย และทำการปฐมพยาบาล
สิ่งแวดล้อม	สิ่งแวดล้อมได้รับผลกระทบสูง และต้องใช้เวลาในการแก้ไข/ฟื้นฟูมากกว่า 1 ปี	สิ่งแวดล้อมได้รับผลกระทบสูง และต้องใช้เวลาในการแก้ไข/ฟื้นฟูไม่เกิน 1 ปี	สิ่งแวดล้อมได้รับผลกระทบปานกลางและแก้ไขได้ในระยะเวลาสั้นไม่เกิน 1 เดือน	สิ่งแวดล้อมได้รับผลกระทบเล็กน้อย แก้ไขได้ทันที
บุคลากร	พนักงานไม่พึงพอใจในระดับรุนแรง เช่น นัดหยุดงานหรือลาออกเป็นจำนวนมาก หรือ Turnover rate มากกว่า 10%	พนักงานไม่พึงพอใจอย่างมาก เช่น เกิดการประท้วง หรือ Turnover rate มากกว่า 5%	พนักงานไม่พึงพอใจในระดับปานกลาง เช่น เกิดการเสียขวัญและกำลังใจในการทำงาน หรือ Turnover rate มากกว่า 3-5%	พนักงานไม่พึงพอใจเล็กน้อย เช่น กระทบต่อประสิทธิภาพในการทำงานเล็กน้อย หรือ Turnover rate น้อยกว่า 3%

ทั้งนี้ หน่วยธุรกิจสามารถกำหนดเกณฑ์การประเมินโอกาสในการเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของความเสี่ยง (Impact) และ Risk Matrix ให้เหมาะสมกับวัตถุประสงค์และระดับความเสี่ยงที่หน่วยธุรกิจนั้นยอมรับได้

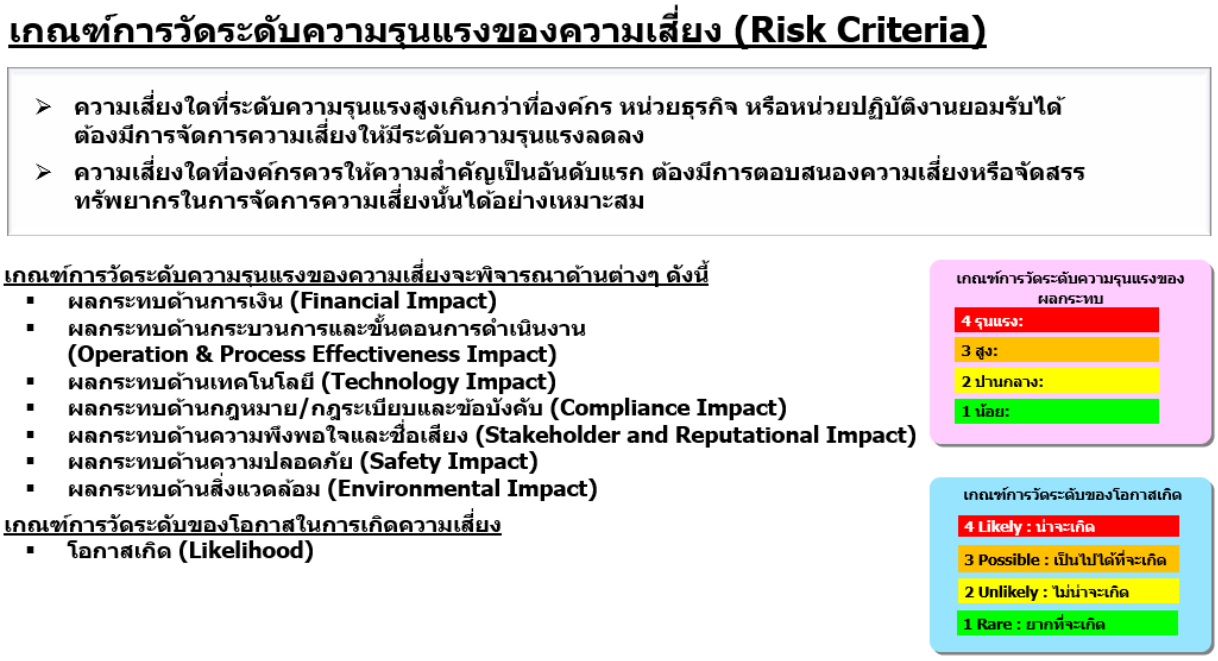
3.3 เกณฑ์การจัดลำดับความสำคัญของความเสี่ยง

การนำความเสี่ยงที่ประเมินได้มาจัดลำดับความสำคัญ ซึ่งมีอยู่ 4 ระดับคือ ต่ำ ปานกลาง สูง และสูงมาก เพื่อให้ผู้บริหารตัดสินใจเลือกจัดการกับความเสี่ยงที่มีระดับความสำคัญมากกว่าก่อน

ในการประเมินความเสี่ยง มีเกณฑ์ในการประเมินร่วมกัน 2 เกณฑ์ คือ

1. เกณฑ์การจัดระดับความรุนแรงของผลกระทบ (Impact) ถูกแบ่งออกเป็น 4 ระดับ คือ (1) น้อย (2) ปานกลาง (3) สูง และ (4) รุนแรง

2. เกณฑ์การวัดโอกาสในการเกิดความเสี่ยง (Likelihood) ถูกแบ่งออกเป็น 4 ระดับเช่นกัน คือ (1) Rare ยากที่จะเกิด (2) Unlikely ไม่น่าจะเกิด (3) Possible เป็นไปได้ที่จะเกิด และ (4) Likely น่าจะเกิดขึ้นอย่างแน่นอน

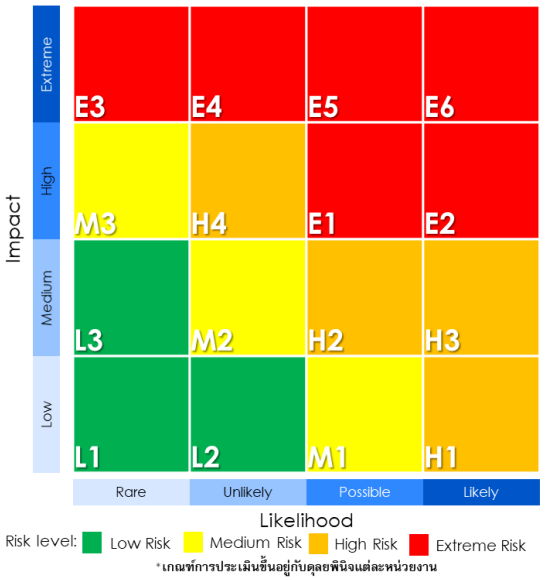


รูป 8 แสดงเกณฑ์การวัดระดับความรุนแรงของความเสี่ยง

การประเมินความเสี่ยงลงในเมทริกซ์ความเสี่ยง (Risk Matrix) แสดงการวิเคราะห์ความสัมพันธ์ของระดับโอกาสที่จะเกิดความเสี่ยงและระดับความรุนแรงของผลกระทบจากความเสี่ยงของแต่ละปัจจัยเสี่ยงที่ได้ระบุไว้ สามารถชี้ให้เห็นว่าความเสี่ยงใดเป็นความเสี่ยงสำคัญที่หน่วยธุรกิจควรให้ความใส่ใจ

เป็นอันดับแรกๆ โดยความเสี่ยงที่ตกอยู่ในพื้นที่สีแดง ถือว่าเป็นความเสี่ยงสำคัญอันดับแรกๆ ตามมาด้วยความเสี่ยงที่ตกอยู่ในพื้นที่สีส้ม สีเหลือง และสีเขียว ตามลำดับ การประเมินทำโดยการนำค่าเกณฑ์การจัดระดับความรุนแรงของผลกระทบ คูณกับเกณฑ์การวัดระดับโอกาสในการเกิดความเสี่ยง

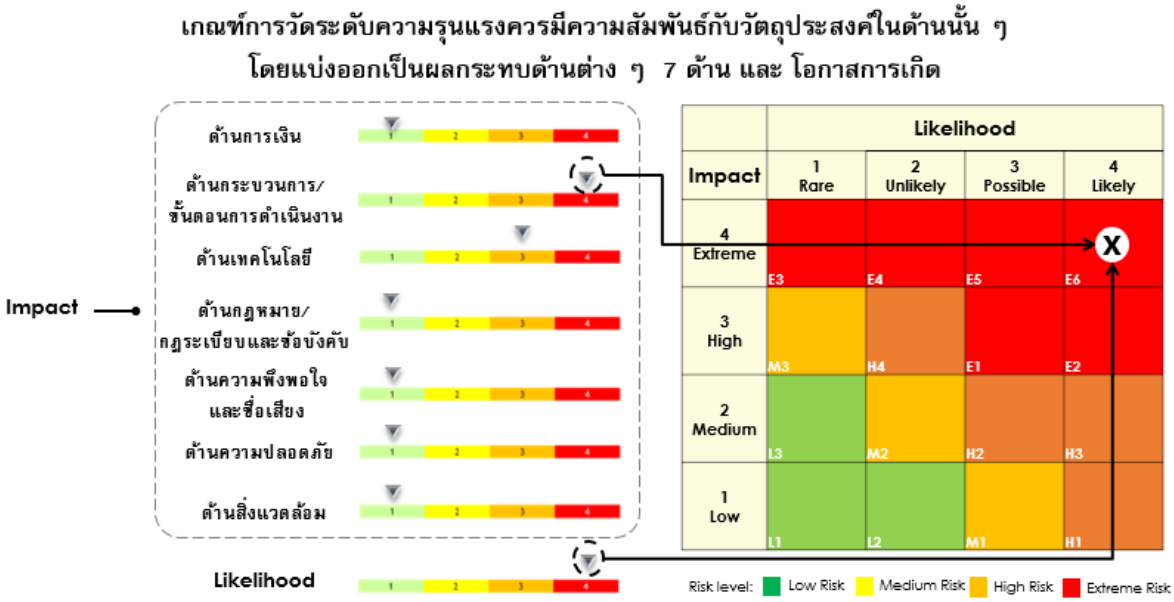
ระดับความเสี่ยง = ระดับความรุนแรงของผลกระทบ x ระดับโอกาสในการเกิดความเสี่ยง



รูป 9 แสดงเมทริกซ์ความเสี่ยง

ตาราง 4 แสดงการจัดลำดับความเสี่ยง (Degree of Risk)

ระดับความเสี่ยง	แทนด้วยแถบสี	ความหมาย
สูงมาก (Extreme: E)		ระดับที่ไม่สามารถยอมรับได้จะเป็นต้องเร่งจัดการบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที โดยเร่งดำเนินการความเสี่ยงที่มีคะแนนสูงไปต่ำ ตามลำดับ
สูง (High: H)		ระดับที่พอยอมรับได้ โดยต้องจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ต่อไป โดยดำเนินการความเสี่ยงที่มีคะแนนสูงไปต่ำ ตามลำดับ
ปานกลาง (Medium: M)		ระดับที่ยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
ต่ำ (Low: L)		ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการบริหารจัดการเพิ่มเติม

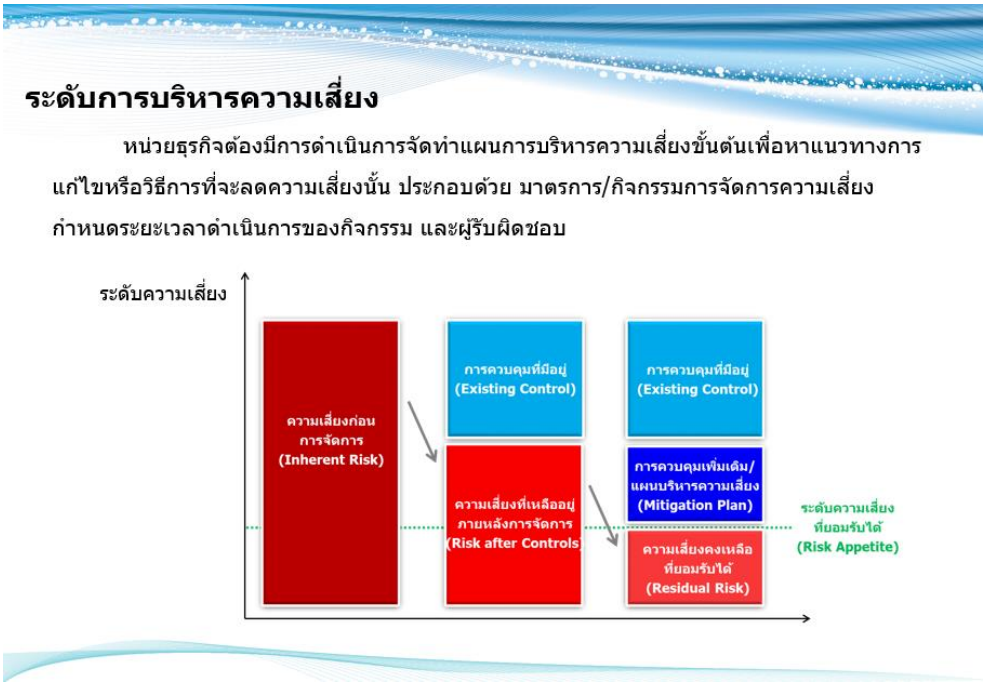


รูป 10 แสดงการประเมินความเสี่ยงตามเกณฑ์การวัดระดับความรุนแรง

เมื่อหน่วยธุรกิจมีการสรุปผลความเสี่ยงของกิจกรรมในแต่ละระดับแล้ว หน่วยธุรกิจต้องวางแผนการควบคุมกิจกรรมที่มีความเสี่ยงที่ระดับสูงมากและสูง ซึ่งถือว่ามีนัยสำคัญ อาจเรียกได้ว่าเป็นความเสี่ยงขั้นต้น (Gross Risk) สำหรับกิจกรรมที่มีความเสี่ยงที่ระดับปานกลางและต่ำ เมื่อพิจารณาจากระดับความเสี่ยงแล้วเห็นว่าหน่วยธุรกิจสามารถดำเนินการได้ด้วยตนเองจึงไม่ต้องรายงานแต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้

3.4 แผนการบริหารความเสี่ยง

หน่วยธุรกิจต้องมีการดำเนินการจัดทำแผนการบริหารความเสี่ยงขั้นต้นเพื่อหาแนวทางการแก้ไขหรือวิธีการที่จะลดความเสี่ยงนั้น ประกอบด้วย มาตรการ/กิจกรรมการจัดการความเสี่ยง กำหนดระยะเวลาดำเนินการของกิจกรรม และผู้รับผิดชอบ กล่าวคือ Action Plan ซึ่งหลังจากมีการดำเนินการตาม Action Plan แล้ว ระดับของปัจจัยความเสี่ยงของแต่ละกิจกรรมก็จะมีการเปลี่ยนแปลงไปจากเดิมขึ้นอยู่กับระดับประสิทธิภาพของการควบคุมที่มีอยู่และจะสามารถประเมินระดับความเสี่ยงที่คงเหลือ (Residual Risk) ลงในเมทริกซ์ความเสี่ยงได้



รูป 11 แสดงระดับการบริหารความเสี่ยง

กลยุทธ์การบริหารความเสี่ยง (4T's Strategies)

องค์กร/หน่วยธุรกิจสามารถเลือกใช้กลยุทธ์การบริหารความเสี่ยงเพื่อตอบสนองความเสี่ยงได้อย่างเหมาะสม ประกอบด้วย 4T's คือ Take Treat Transfer และ Terminate ดังนี้

การยอมรับความเสี่ยง (Take)

หากพิจารณาแล้วเห็นว่าระดับความรุนแรงของความเสี่ยงนั้นยอมรับได้ หากเกิดเหตุการณ์ขึ้นจริง มาตรการที่มีอยู่ในปัจจุบันสามารถใช้การได้อย่างมีประสิทธิภาพ

การจัดการความเสี่ยง (Treat)

หากพิจารณาแล้วเห็นว่าระดับความรุนแรงของความเสี่ยงนั้นสูงกว่าที่ยอมรับได้ จำเป็นต้องมีมาตรการเพิ่มเติม เช่น มาตรการลดโอกาสเกิดของความเสี่ยงนั้น หรือมาตรการลดผลกระทบ หากความเสี่ยงนั้นเกิดขึ้นจริง หรือการกระจายความเสี่ยง

การโอนความเสี่ยง (Transfer)

เป็นการโอนความเสี่ยงให้กับบุคคลที่สาม เช่น การประกันภัย การจ้าง Outsourcing เป็นต้น

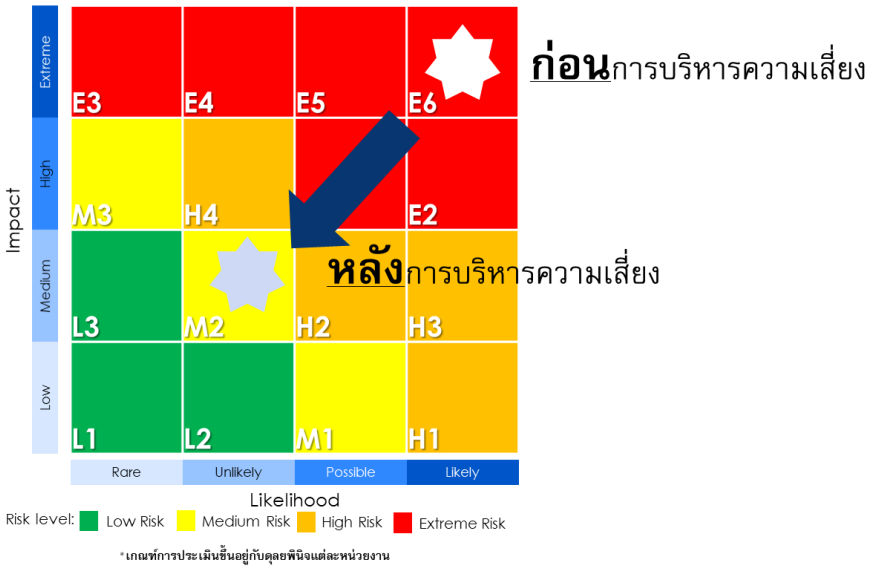
การยกเลิกความเสี่ยง (Terminate)

เป็นการเลิกหรือเปลี่ยนแปลงกิจกรรมที่ทำให้เกิดความเสี่ยงนั้นไปเป็นวิธีอื่น เพื่อหลีกเลี่ยงความเสี่ยงนั้น

รูป 12 แสดงกลยุทธ์การบริหารความเสี่ยง

รูป 13 แสดงตัวอย่างกลยุทธ์การบริหารความเสี่ยง

จากแผนบริหารความเสี่ยงของหน่วยธุรกิจจะถูกรวบรวมขึ้นมาเป็นแผนบริหารความเสี่ยงองค์กร ซึ่งเป็นการรวบรวมข้อมูลวิธีการและกิจกรรมการจัดการความเสี่ยงต่างๆ มาพิจารณาในภาพรวม เพื่อให้การบริหารความเสี่ยงองค์การมีประสิทธิภาพสูงขึ้น มีความมั่นใจต่อการบรรลุเป้าหมายหรือกลยุทธ์องค์กร ซึ่งการรวบรวมความเสี่ยงในหน่วยธุรกิจมาเป็นความเสี่ยงองค์กรนั้นจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ขององค์กรและต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับ เพื่อให้การบริหารความเสี่ยงมีประสิทธิผล อาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่งหรือหลายวิธีรวมกัน เพื่อลดระดับความรุนแรงของผลกระทบและโอกาสที่อาจจะเกิดขึ้นให้อยู่ในระดับที่องค์กรยอมรับได้ (Risk Appetite) และสอดคล้องกับกลยุทธ์องค์กร



รูป 14 แสดงการปรับระดับความเสี่ยงในเมทริกซ์ความเสี่ยง

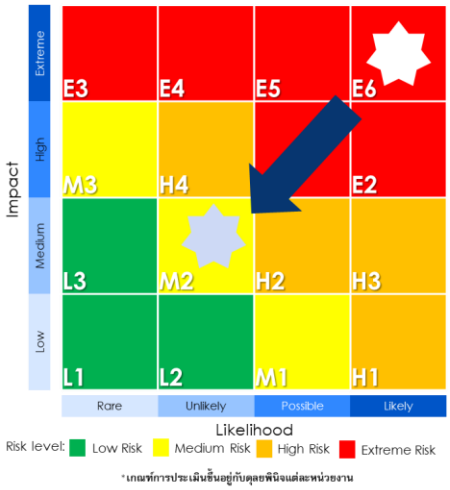
จากนั้นจัดทำเป็นทะเบียนความเสี่ยง (Risk Register) เพื่อแสดงให้เห็นถึงสถานะปัจจุบันของทุกๆ ความเสี่ยงองค์กรและเป็นข้อมูลสำคัญที่ใช้ในการพัฒนาแผนบริหารความเสี่ยงองค์กร/หน่วยธุรกิจต่อไป

โดยทะเบียนความเสี่ยงถือเป็นเครื่องมือในการบริหารความเสี่ยงทั่วไปที่นิยมใช้กัน ซึ่งนอกจากจะมีข้อมูลเกี่ยวกับความเสี่ยงแล้ว ทะเบียนความเสี่ยงที่ดีจะต้องมีพื้นที่/คอลัมน์ว่างไว้สำหรับบันทึกข้อความเกี่ยวกับเครื่องมือในการควบคุมที่ใช้ในการจัดการกับความเสี่ยงเหล่านั้นด้วย

ตัวอย่าง : แผนการบริหารความเสี่ยง

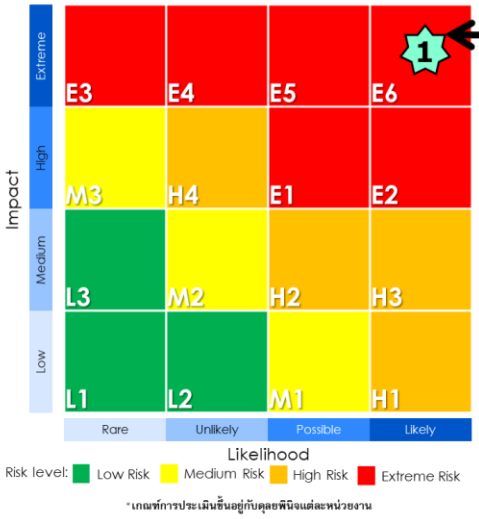
เลขที่ความเสี่ยง	XXX.-2020-XX	ประเภทความเสี่ยง	Business & Operational Risk	หน่วยงานที่รับผิดชอบ	xx

ความเสี่ยง	ผลกระทบ (Impact)	การควบคุมที่มีอยู่ (Existing Control)	ระดับความเสี่ยงขั้นต้น	การควบคุมเพิ่มเติม (Mitigation Plan)	ระดับความเสี่ยงคงเหลือ
สินค้าขาดคุณภาพและไม่เป็นตามมาตรฐานอุตสาหกรรม	1) ขาดระบบการติดตามดูแลเรื่องคุณภาพสินค้าอย่างต่อเนื่อง 2) ขาดเครื่องมืออุปกรณ์ในการตรวจคุณภาพสินค้า	• ดำเนินการตามแผนงาน • ติดตามการดำเนินงานอย่างใกล้ชิด	E6	• จัดทำระบบการติดตามดูแลทั้งในกระบวนการตรวจสอบคุณภาพสินค้าและตรวจสอบสินค้าที่ผลิตออกมาได้ก่อนจำหน่ายเป็นประจำทุกวันและรายงานต่อผู้บริหารทุกสัปดาห์	M2



รูป 15 แสดงตัวอย่างการจัดทำทะเบียนความเสี่ยง

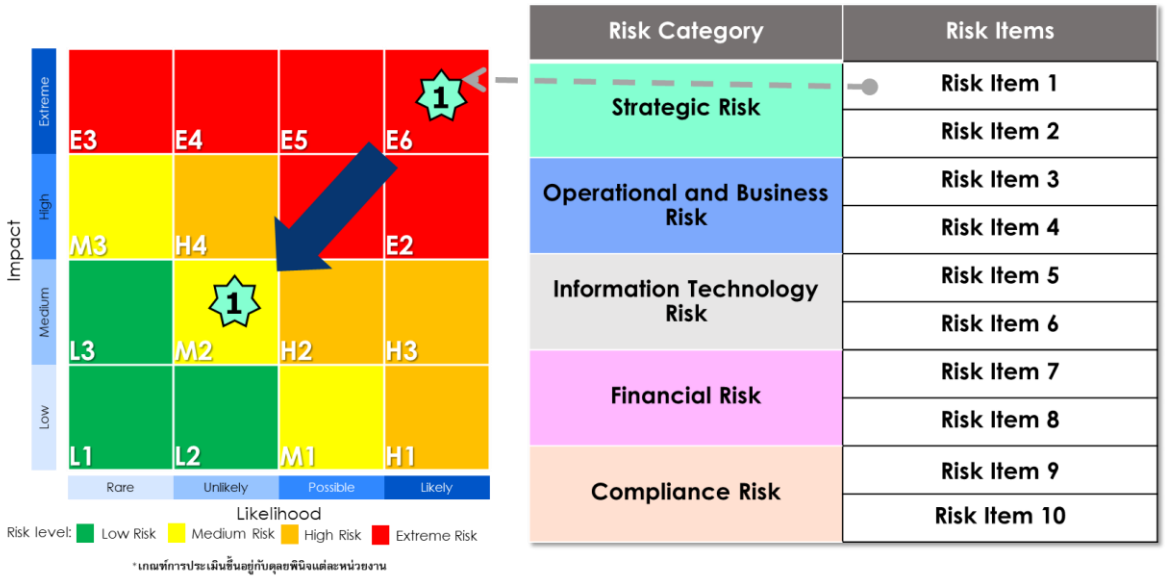
Department/Business Area Risk Profile (ก่อนการบริหารความเสี่ยง)



Risk Category	Risk Items
Strategic Risk	Risk Item 1
	Risk Item 2
Operational and Business Risk	Risk Item 3
	Risk Item 4
Information Technology Risk	Risk Item 5
	Risk Item 6
Financial Risk	Risk Item 7
	Risk Item 8
Compliance Risk	Risk Item 9
	Risk Item 10

รูป 16 แสดงการประเมินหัวข้อความเสี่ยงก่อนการบริหารความเสี่ยง

Department/Business Area Risk Profile (หลังการบริหารความเสี่ยง)



รูป 17 แสดงการประเมินหัวข้อความเสี่ยงหลังการบริหารความเสี่ยง

หลักการสำคัญที่ 4. การทบทวนและปรับปรุงกระบวนการบริหารความเสี่ยง (Review & Revision)

แผนบริหารความเสี่ยงที่จัดทำขึ้นมานี้ควรได้รับการทบทวนอย่างสม่ำเสมอทุกปี เนื่องจากสภาพแวดล้อมที่เปลี่ยนแปลงไป ย่อมทำให้ปัจจัยเสี่ยงที่มีต่อองค์กร/หน่วยธุรกิจเปลี่ยนแปลงไปด้วยเช่นกัน อีกทั้งแผนบริหารความเสี่ยงนั้นจะมีประสิทธิภาพได้ก็ต่อเมื่อองค์กร/หน่วยธุรกิจมีการติดตามแผนบริหารความเสี่ยงอยู่เสมอ โดยมีการทบทวนเพื่อให้มั่นใจว่าแต่ละโครงการหรือแผนงานได้มีการนำไปปฏิบัติจริง และมีผลการดำเนินงานอยู่ในระดับที่องค์กร/หน่วยธุรกิจคาดหวังไว้

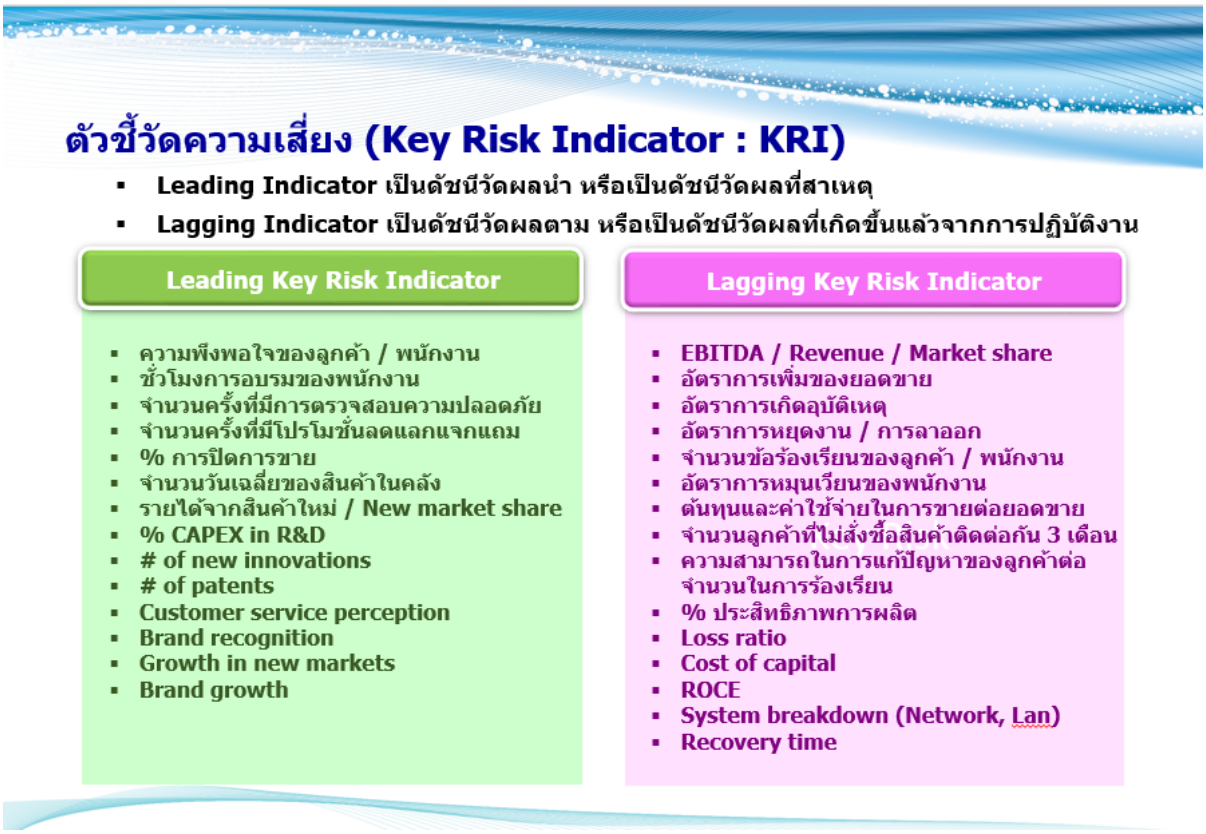
ตัวชี้วัดความเสี่ยง (KRI) คือ ปัจจัย ตัวแปร กิจกรรม เหตุการณ์ หรือสิ่งที่ใช้ในการติดตามที่สามารถใช้บ่งบอกถึงการเปลี่ยนแปลงระดับความรุนแรงของความเสี่ยงได้ หากการเปลี่ยนแปลงของปัจจัยเสี่ยงอยู่ในช่วงที่เกินกว่าที่กำหนด องค์กร/หน่วยธุรกิจสามารถตอบสนองต่อการเปลี่ยนแปลงนั้นได้อย่างมีประสิทธิภาพมากยิ่งขึ้น โดยพาะตัววัดความเสี่ยงที่เป็น Leading Indicator สามารถนำไปใช้ประโยชน์ในการวางแผนการบริหารความเสี่ยงให้มีระบบเตือนล่วงหน้า (Early Warning System)

ตัวชี้วัดความเสี่ยง (KRI) มี 2 ประเภทคือ

1. ตัวชี้วัดความเสี่ยงนำ หรือ Leading KRI คือ ปัจจัย ตัวแปร กิจกรรม เหตุการณ์ หรือสิ่งที่ใช้ในการติดตามที่สามารถใช้บ่งบอกถึงการเปลี่ยนแปลงระดับความรุนแรงของสาเหตุของความเสี่ยง

2. ตัวชี้วัดความเสี่ยงตาม หรือ Lagging KRI คือ ปัจจัย ตัวแปร กิจกรรม เหตุการณ์ หรือสิ่งที่ใช้ในการติดตามที่สามารถใช้บ่งบอกถึงการเปลี่ยนแปลงระดับความรุนแรงของความเสี่ยงซึ่งมีลักษณะเป็นผล

รูป 18 แสดงตัวอย่างตัวชี้วัดของความเสี่ยง



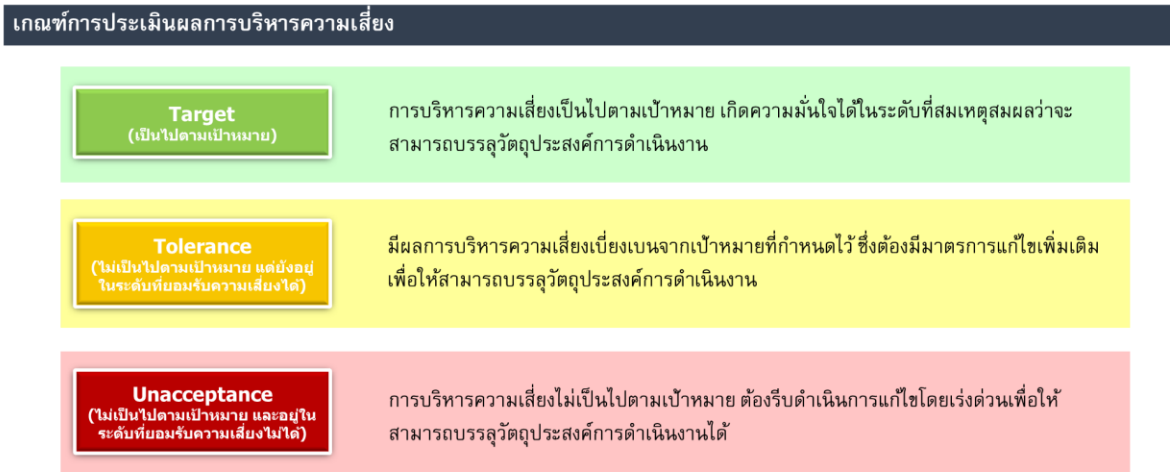
รูป 19 แสดงตัวอย่าง Leading และ Lagging KRI

ซึ่งการประเมินถึงประสิทธิผลของการบริหารความเสี่ยงที่มีอยู่ในปัจจุบันจะถูกแบ่งออกเป็น 3 ระดับ ดังนี้

Target (เป็นไปตามเป้าหมาย) : การบริหารความเสี่ยงเป็นไปตามเป้าหมาย เกิดความมั่นใจได้ในระดับที่สมเหตุสมผลว่าจะสามารถบรรลุวัตถุประสงค์การดำเนินงาน

Tolerance (ไม่เป็นไปตามเป้าหมาย แต่ยังอยู่ในระดับที่ยอมรับได้) : มีผลการบริหารความเสี่ยงเบี่ยงเบนจากเป้าหมายที่กำหนดไว้ ซึ่งต้องมีมาตรการแก้ไขเพิ่มเติมเพื่อให้สามารถบรรลุวัตถุประสงค์การดำเนินงาน

Unacceptance (ไม่เป็นไปตามเป้าหมาย และอยู่ในระดับที่ยอมรับไม่ได้) : การบริหารความเสี่ยงไม่เป็นไปตามเป้าหมาย ต้องรีบดำเนินการแก้ไขโดยเร่งด่วนเพื่อให้สามารถบรรลุวัตถุประสงค์การดำเนินงานได้



รูป 20 แสดงการประเมินผลการบริหารความเสี่ยง

<u>หลักการสำคัญที่ 5. การรายงานผลการบริหารความเสี่ยง (Information, Communication and Reporting)</u>

การรายงานด้านการบริหารความเสี่ยงควรมีการจัดการอย่างสม่ำเสมอและต่อเนื่องผ่านการผสมผสานให้เข้ากับกระบวนการต่างๆตามปกติ โดยมีผู้รับผิดชอบเพื่อดำเนินการติดตามและรายงานผลการบริหารความเสี่ยงให้กับผู้ที่มีตำแหน่งที่เกี่ยวข้อง

การบริหารจัดการความเสี่ยงอาจไม่สามารถบรรลุผลได้อย่างยั่งยืนหากปราศจากการติดตามและประเมินผลอย่างสม่ำเสมอ การติดตามผลเพื่อให้เกิดความมั่นใจว่าความเสี่ยงได้มีการควบคุมและจัดการอย่างมีประสิทธิผล จึงต้องมีการติดตามผล ประกอบด้วยข้อมูลความเสี่ยง กิจกรรมที่ควบคุม ผลลัพธ์ของการทำกิจกรรม ระยะเวลาการดำเนินงาน ความคืบหน้า ปัญหาและอุปสรรค ดังนั้น ผู้บริหารจึงสนับสนุนให้มีการจัดโครงสร้างระบบในการติดตามเรื่องความเสี่ยง โดยทั่วไปแล้ว ขั้นตอนการปฏิบัติสามารถทำได้ดังต่อไปนี้

1. มอบหมายผู้รับผิดชอบหลักในการติดตามการบริหารความเสี่ยงโดยกำหนดให้เจ้าของความเสี่ยงเป็นผู้ติดตามและรวบรวมข้อมูลเพื่อรายงานความคืบหน้าของแผนจัดการความเสี่ยงต่อผู้รับผิดชอบเป็นระยะ

2. ผู้รับผิดชอบบริหารความเสี่ยงต้องคัดกรองและวิเคราะห์ข้อมูลอย่างสม่ำเสมอตามความเหมาะสมของระดับความรุนแรงและลักษณะของข้อมูล เช่น อาจมีการรวบรวมและวิเคราะห์คัดกรองเป็นรายเดือนหรือรายไตรมาสเพื่อนำเสนอต่อที่ประชุมผู้บริหารหรือคณะกรรมการบริหารความเสี่ยงองค์กร

3. ในขั้นตอนการนำเสนอให้มุ่งเน้นภาพรวมสถานะความเสี่ยงที่สำคัญ ความคืบหน้าของแผนบริหารความเสี่ยง ความเปลี่ยนแปลงในสภาพแวดล้อมการดำเนินงาน ปัจจัยทั้งภายในและภายนอกที่อาจส่งผลต่อระดับความเสี่ยงหรือทำให้เกิดความเสี่ยงใหม่ รวมทั้งนำเสนอแนวคิด คำแนะนำในการจัดการความเสี่ยง

4. ที่ประชุมผู้บริหารหรือคณะกรรมการบริหารความเสี่ยงองค์กรพิจารณาอนุมัติหรือให้ข้อคิดเห็น/คำแนะนำในการจัดการความเสี่ยงเพิ่มเติม แล้วให้ผู้รับผิดชอบบริหารความเสี่ยงนำสิ่งที่ได้จากมติที่ประชุมไปปฏิบัติ โดยสื่อสารไปยังผู้ที่มีหน้าที่รับผิดชอบในเรื่องต่างๆ ต่อไป เช่น เจ้าของความเสี่ยง

5. ประชุมผู้บริหารหรือคณะกรรมการบริหารความเสี่ยงองค์กร ควรจะมีการประชุมอย่างสม่ำเสมอตามความเหมาะสมอย่างน้อยทุกไตรมาส เพื่อติดตามและประเมินผลการบริหารความเสี่ยงได้อย่างมีประสิทธิภาพและสามารถแก้ไขหรือควบคุมความเสี่ยงได้อย่างทันกาล

<u>การบริหารจัดการความเสี่ยงด้านข้อมูล (Data Risk Management)</u>

เนื่องจาก OR มีจุดมุ่งหมายที่จะพัฒนาไปสู่การเป็นองค์กรที่ขับเคลื่อนด้วยข้อมูล (Data Driven Organization) “ข้อมูลจึงถือเป็นสินทรัพย์ที่สำคัญ” ของ OR การวางแผนการบริหารจัดการความเสี่ยงด้านข้อมูล (Data Risk) จึงเป็นกระบวนการหนึ่งที่จะต้องมีการวางแผนอย่างชัดเจนตั้งแต่การกำหนดตัวชี้วัดความเสี่ยง, แนวทางการติดตามผลความเสี่ยง ตลอดจนแผนการรับมือกับความเสี่ยงที่จะเกิดขึ้น

ทั้งนี้ในปี 2022 นี้ OR **จะเริ่มมีการดำเนินการกำหนดตัวชี้วัดและแผนการจัดการความเสี่ยงด้านข้อมูลเบื้องต้น** โดยส่วนงานต่าง ๆ สามารถดำเนินการได้ตามแนวทางตามตารางที่ 5 และ 6

ขั้นตอนการดำเนินการเพื่อกำหนดกรอบแนวคิดกรอบแนวคิดด้านความเสี่ยงของข้อมูล มี 3 ขั้นตอน

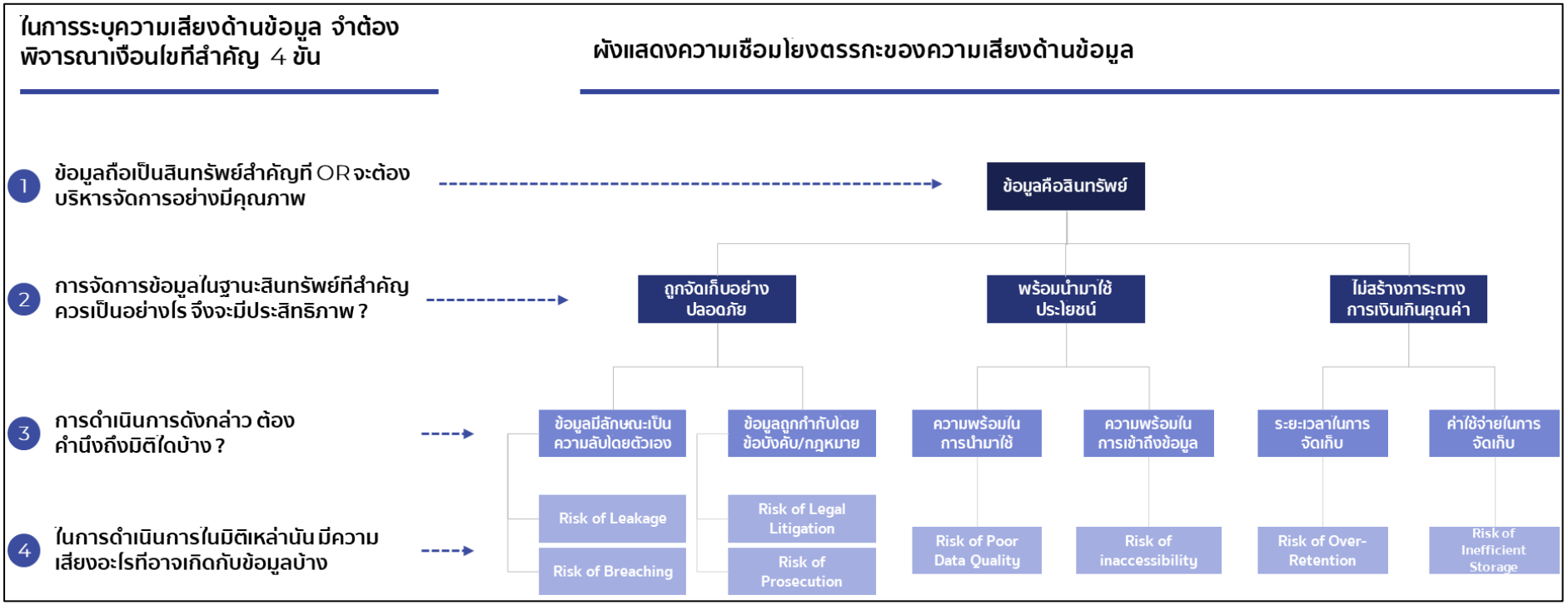
ขั้นที่ 1 – ทำความเข้าใจกรอบแนวคิดและมิติต่าง ๆ ของความเสี่ยงด้านข้อมูล (Data Risk Dimensions) – โปรดพิจารณารายละเอียดประกอบการดำเนินงานขั้นที่ 1 ในส่วนถัดไป

ขั้นที่ 2 – กำหนดตัวชี้วัดความเสี่ยงด้านข้อมูลสำหรับส่วนงาน โดยอาจพิจารณาจากตัวอย่างตัวชี้วัดภายในตามตารางที่ 5 และ 6 - โปรดพิจารณารายละเอียดประกอบการดำเนินงานขั้นที่ 2 ในส่วนถัดไป

ขั้นที่ 3 – ประเมินระดับผลกระทบของความเสี่ยงและกำหนดวิธีการบริหารจัดการความเสี่ยงเบื้องต้น ตามแนวทางที่ได้กำหนดไว้ภายในคู่มือฉบับนี้ เช่นเดียวกับความเสี่ยงประเภทอื่นๆ – โปรดพิจารณาแนวทางการดำเนินงานจากเนื้อหาหลักภายในคู่มือฉบับนี้

1

รายละเอียดประกอบการดำเนินงานขั้นที่ 1 – กรอบแนวคิดและมิติของความเสี่ยงด้านข้อมูล



รูป 21 แผนภาพเชื่อมโยงตรรกะด้านความเสี่ยงข้อมูล

จากรูปที่ 21 จะพบว่าความเสี่ยงด้านข้อมูลสามารถแบ่งออกได้เป็น 8 มิติ ตามหลักการบริหารจัดการข้อมูล 3 ประการดังต่อไปนี้

1. ข้อมูลต้องมีการจัดเก็บอย่างปลอดภัย เนื่องจาก

1.1. ข้อมูลมีลักษณะเป็นความลับโดยตัวเอง (Confidential) ซึ่งนำไปสู่ความเสี่ยงที่สำคัญ 2 ประการ ได้แก่

1.1.1. ความเสี่ยงที่ข้อมูลจะรั่วไหล (Risk of Data Leakage) หมายถึง ความเสี่ยงที่ข้อมูลอาจเกิดการรั่วไหล “จากภายใน” ไม่ว่าจะเป็นไปด้วยความประมาทของบุคลากร หรือด้วยช่องโหว่ของการดำเนินงาน เป็นต้น

1.1.2. ความเสี่ยงที่ข้อมูลจะถูกเจาะ (Risk of Data Breach) หมายถึง ความเสี่ยงที่ข้อมูลอาจถูกเข้าถึงจากบุคคลภายนอก (3rd party) โดยการเจาะเข้าสู่ระบบของ OR ได้สำเร็จ

1.2. ข้อมูลมีการถูกกำกับควบคุมโดยกฎหมาย (Legally Regulated) ซึ่งนำไปสู่ความเสี่ยงที่สำคัญ 2 ประการ ได้แก่

1.2.1. ความเสี่ยงที่จะถูกฟ้องร้อง (Risk of Legal Litigation) หมายถึง ความเสี่ยงที่ OR จะถูกฟ้องร้องโดยบุคคลภายนอกอันเนื่องมาจากการบริหารจัดการข้อมูลที่ผิดพลาด ทั้งโดยปัจเจกบุคคลและโดยนิติบุคคลที่เกี่ยวข้อง

1.2.2. ความเสี่ยงที่จะถูกสอบสวน (Risk of Prosecution) หมายถึง ความเสี่ยงที่ OR จะถูกดำเนินการสอบสวนโดยหน่วยงานที่ทำหน้าที่กำกับดูแล

2. ข้อมูลต้องพร้อมต่อการนำมาสร้างประโยชน์ ประกอบด้วย

2.1. ข้อมูลต้องอยู่ในสภาพที่พร้อมให้นำมาใช้งาน (Availability) ซึ่งนำไปสู่ความเสี่ยง 1 ประการ ได้แก่

2.1.1. ความเสี่ยงข้อมูลด้อยคุณภาพ (Risk of Data Quality) หมายถึง ความเสี่ยงที่ข้อมูลของ OR อาจไม่อยู่ในสภาพที่สามารถนำมาใช้งานได้ หรือไม่อาจใช้งานได้โดยสะดวก ซึ่งจะก่อให้เกิดผลเสียต่อธุรกิจ

2.1.2. ความเสี่ยงในการไม่สามารถเข้าถึงข้อมูล (Risk of Inaccessibility) หมายถึง ความเสี่ยงที่ผู้ใช้งานข้อมูลอาจไม่สามารถเข้าถึงข้อมูลได้จนส่งผลกระทบต่อการดำเนินงานด้านข้อมูล อันเนื่องจากสาเหตุด้านระบบ, กระบวนการเข้าถึงข้อมูล เป็นต้น

3. ข้อมูลต้องไม่สร้างภาระทางการเงินเกินคุณค่าของข้อมูล ประกอบด้วย

3.1. ระยะเวลาการจัดเก็บข้อมูลที่เหมาะสม (Proper Retention) ซึ่งนำมาสู่ความเสี่ยงที่สำคัญได้แก่

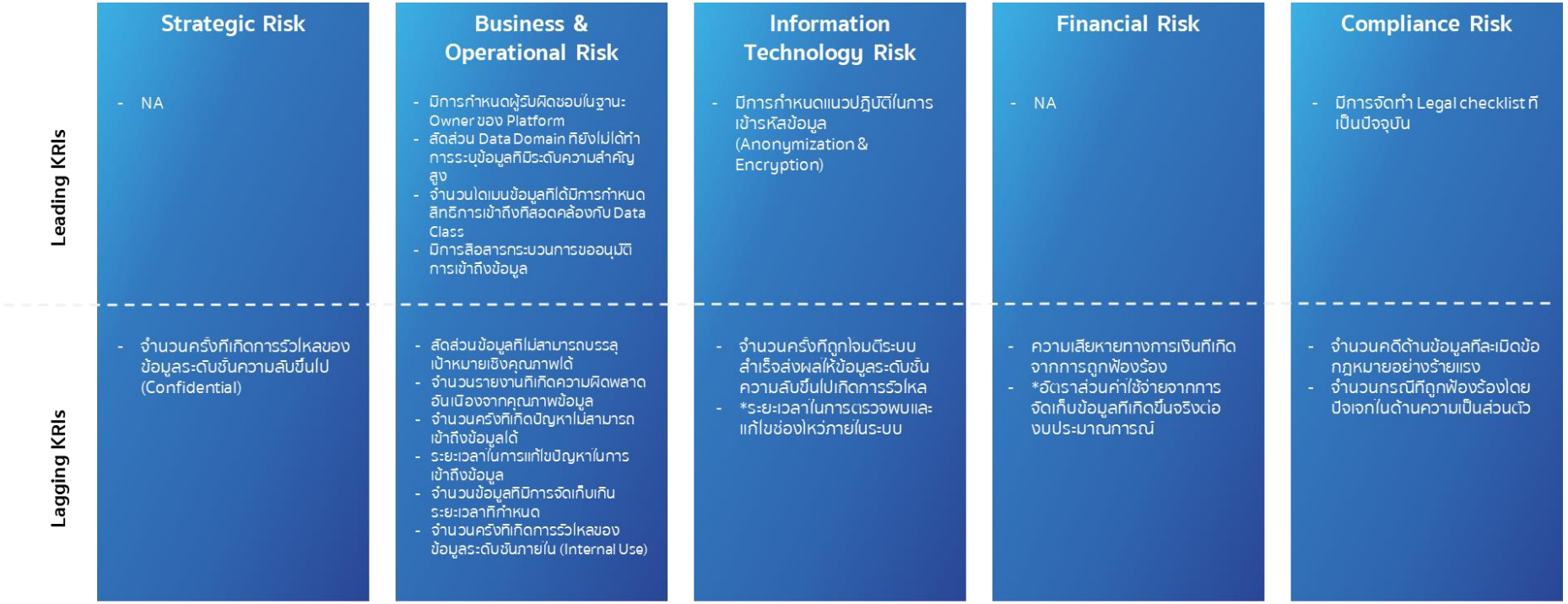
3.1.1. ความเสี่ยงในการจัดเก็บข้อมูลเกินระยะเวลา (Risk of Over Retention) หมายถึง ความเสี่ยงที่อาจจะเกิดการจัดเก็บข้อมูลเป็นระยะเวลาที่ยาวนานกว่าที่ควรจะจัดเก็บ ซึ่งอาจเกิดขึ้นจากช่องโหว่ในเชิงกระบวนการติดตาม, ตรวจสอบ, บริหารจัดการทำลายข้อมูล (Data disposal)

3.2. รูปแบบการจัดเก็บที่เหมาะสม (Retention Format) ซึ่งนำมาสู่ความเสี่ยงที่สำคัญได้แก่

3.2.1. ความเสี่ยงของรูปแบบการจัดเก็บข้อมูล (Risk of Inefficient Storage) หมายถึง ความเสี่ยงที่จะมีการจัดเก็บข้อมูลในรูปแบบที่ไม่คุ้มทุนที่สุด (Unoptimized) ซึ่งอาจเกิดขึ้นจากช่องโหว่ของกระบวนการติดตาม, ตรวจสอบ, บริหารจัดการทำลายข้อมูล (Data disposal)

รายละเอียดประกอบการดำเนินงานขั้นที่ 2 – กำหนดตัวชี้วัดความเสี่ยงด้านข้อมูลในมิติต่าง ๆ

โดยส่วนงานสามารถกำหนดตัวชี้วัดความเสี่ยงด้านข้อมูลทั้ง 8 มิติ โดยอาจพิจารณาเบื้องต้นจากตัวอย่างตัวชี้วัดนำ (Leading KRI) และตัวชี้วัดตาม (Lagging KRI) ได้จากรูปที่ 22



รูป 22 ตัวอย่างตัวชี้วัดความเสี่ยงด้านข้อมูลที่เป็นไปได้

นอกจากนี้ ส่วนงานสามารถพิจารณาแบ่งกลุ่มตัวชี้วัดที่ได้กำหนดไว้ ลงในกรอบมิติของความเสี่ยงทั้ง 5 ด้านตามที่ได้กำหนดในคู่มือฉบับนี้ โดยอาจพิจารณาจากตัวอย่างดังตารางต่อไปนี้

ตาราง 5 แสดงมิติผลกระทบสำหรับตัวชี้วัดความเสี่ยงข้อมูลประเภทตัวชี้วัดตาม (Lagging KRIs)

ประเภทความเสี่ยง	ความเสี่ยง	มิติที่ควรประเมินด้านผลกระทบ						
		ผลกระทบทางการเงิน	ผลกระทบด้านที่ไม่ใช่การเงิน (Non-Financial Impact)					
			กระบวนการและขั้นตอนการดำเนินงาน	เทคโนโลยี	กฎหมายและระเบียบข้อบังคับ	ความพึงพอใจและชื่อเสียง	ความปลอดภัย	สิ่งแวดล้อม
Risk of Prosecution	จำนวนคดีด้านข้อมูลที่ละเมิดข้อกฎหมายอย่างร้ายแรง				✓	✓		
Risk of Legal Litigation	จำนวนครั้งที่ถูกฟ้องร้องโดยปัจเจกในด้านความเป็นส่วนตัว				✓	✓		
	ความเสียหายทางการเงินที่เกิดจากการถูกฟ้องร้อง	✓						
Risk of Data Leakage	จำนวนครั้งที่เกิดการรั่วไหลของข้อมูลระดับชั้นความลับ (Confidential Class) ขึ้นไป					✓		
	จำนวนครั้งที่เกิดการรั่วไหลของข้อมูลระดับชั้นภายใน (Internal Use Only Class)					✓		
	ระยะเวลาในการตรวจพบและแก้ไขปัญหาข้อมูลรั่วไหล					✓		
Risk of Data Breaching	จำนวนครั้งที่ถูกโจมตีระบบสำเร็จและส่งผลให้ข้อมูลระดับชั้นความลับ (Confidential Class) ขึ้นไปรั่วไหล			✓		✓		
	จำนวนครั้งที่ถูกโจมตีระบบสำเร็จและส่งผลให้ข้อมูลระดับชั้นภายใน (Internal Use Only Class) รั่วไหล			✓		✓		
	ระยะเวลาในการตรวจพบและแก้ไขช่องโหว่ภายในระบบ			✓		✓		

ประเภทความเสี่ยง	ความเสี่ยง	มิติที่ควรประเมินด้านผลกระทบ						
		ผลกระทบทางการเงิน	ผลกระทบด้านที่ไม่ใช่การเงิน (Non-Financial Impact)					
			กระบวนการและขั้นตอนการดำเนินงาน	เทคโนโลยี	กฎหมายและระเบียบข้อบังคับ	ความเสี่ยงและชื่อเสียง	ความปลอดภัย	สิ่งแวดล้อม
Risk of Data Quality	สัดส่วนข้อมูลที่สามารถบรรลุเป้าหมายเชิงคุณภาพได้		✓					
	จำนวนรายงานที่เกิดความผิดพลาดอันเนื่องจากคุณภาพของข้อมูล		✓					
Risk of Inaccessibility	จำนวนครั้งที่เกิดปัญหาไม่สามารถเข้าถึงข้อมูลของผู้ใช้งานข้อมูลได้		✓					
	ระยะเวลาในการแก้ไขปัญหาการเข้าถึงข้อมูล		✓					
Risk of Over Retention	จำนวนข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนด	✓						
Risk of Inefficient Storage	จำนวนข้อมูลที่มีการจัดเก็บผิดรูปแบบ	✓						
	อัตราส่วนค่าใช้จ่ายที่เกิดจากการเก็บข้อมูลที่เกิดขึ้นจริงเปรียบเทียบกับงบประมาณการ	✓						

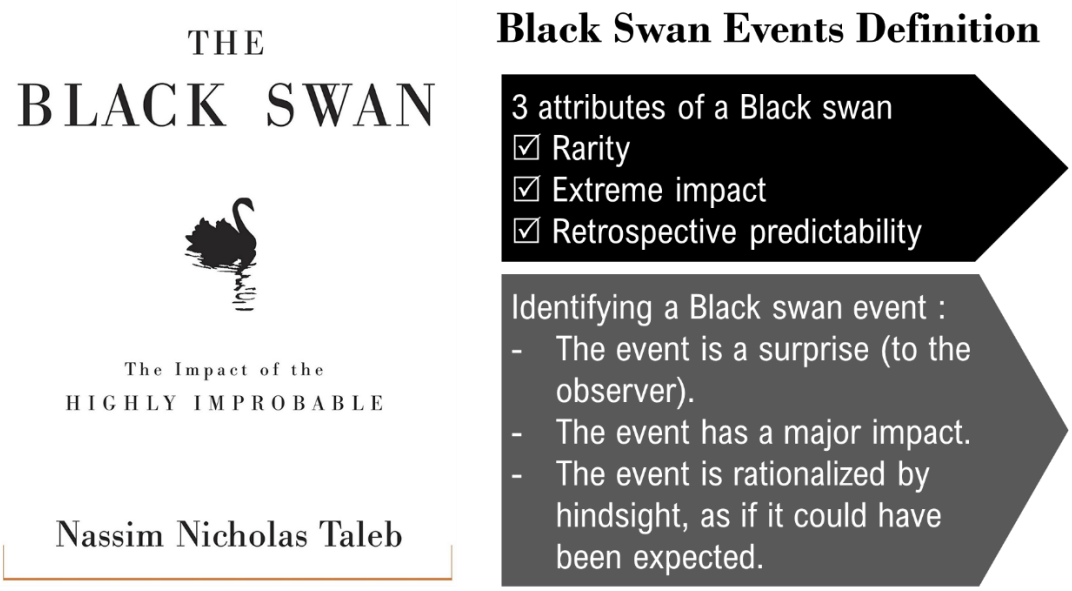
ตาราง 6 แสดงมิติผลกระทบสำหรับตัวชี้วัดความเสี่ยงข้อมูลประเภทตัวชี้วัดนำ (Leading KRIs)

ประเภทความเสี่ยง	ความเสี่ยง	มิติที่ควรประเมินด้านผลกระทบ						
		ผลกระทบทางการเงิน	ผลกระทบด้านที่ไม่ใช่การเงิน (Non-Financial Impact)					
			กระบวนการและขั้นตอนการดำเนินงาน	เทคโนโลยี	กฎหมายและระเบียบข้อบังคับ	ความพึงพอใจและชื่อเสียง	ความปลอดภัย	สิ่งแวดล้อม
Risk of Prosecution	มีการจัดทำ Legal Check List ที่เป็นปัจจุบัน				✓	✓		
Risk of Legal Litigation	มีการจัดทำ Legal Check List ที่เป็นปัจจุบัน				✓	✓		
Risk of Data Leakage	จำนวนโดเมนข้อมูลที่ได้มีการกำหนดสิทธิการเข้าถึงที่สอดคล้องกับ Data Class และ Role Based Authority Classification				✓	✓		
	มีการสื่อสารกระบวนการขอเข้าถึงข้อมูล				✓	✓		
Risk of Data Breaching	มีการกำหนดแนวปฏิบัติในการเข้ารหัสเพื่อรักษาความปลอดภัยข้อมูล (Encryption & Anonymization)			✓				
Risk of Data Quality	สัดส่วนโดเมนข้อมูลที่ยังไม่ได้มีการกำหนดข้อมูลที่มีระดับความสำคัญสูง (Critical Data Element)			✓				
Risk of Inaccessibility	มีการกำหนดผู้รับผิดชอบในฐานะเจ้าของ Platform (Platform Owner)			✓				

Black Swan

1) นิยามและคำจำกัดความ (Definition)

Black Swan หมายถึง เหตุการณ์ที่ไม่คาดฝัน มีโอกาสเกิดขึ้นได้ยาก แต่หากเกิดขึ้นแล้วจะส่งผลกระทบอย่างรุนแรง และหลังเหตุการณ์นั้นจะมีเหตุผลมาอธิบายได้ว่าเกิดอะไรขึ้น



รูป 23 นิยามและคำจำกัดความ Black Swan

2) วัตถุประสงค์ (Objective)

OR Group มีการตระหนักถึงและให้ความสำคัญกับความเสี่ยงจากเหตุการณ์ Black Swan ที่หากเหตุการณ์ดังกล่าวเกิดขึ้นอาจส่งผลกระทบต่อองค์กรอย่างรุนแรง ดังนั้น OR Group จึงมีการกำหนดและทบทวนเหตุการณ์ Black Swan ที่เกี่ยวข้องกับองค์กร และจัดทำแผนการบริหารจัดการเหตุการณ์ Black Swan เพื่อให้องค์กรและธุรกิจสามารถดำเนินงานได้อย่างต่อเนื่อง และช่วยลดผลกระทบที่จะเกิดขึ้นต่อผู้มีส่วนได้ส่วนเสีย

3) เกณฑ์การประเมิน OR Group Black Swan (OR Group Black Swan Criteria)[1]

การกำหนดเกณฑ์สำหรับการประเมิน Black Swan เป็นองค์ประกอบที่สำคัญที่จะบ่งชี้ว่าเหตุการณ์ความเสี่ยงนั้นเข้าข่ายเหตุการณ์ Black Swan หรือไม่ โดยประกอบไปด้วย 2 องค์ประกอบ ได้แก่ ระดับโอกาสที่ความเสี่ยงอาจเกิดขึ้น (Likelihood) และระดับความรุนแรงของผลกระทบที่เกิดขึ้นจากความเสี่ยง (Impact)

1. ระดับโอกาสที่ความเสี่ยงอาจเกิดขึ้น (Likelihood) เป็นการพิจารณาความเป็นไปได้ที่จะเกิดเหตุการณ์ Black Swan โดยจะต้องเป็น Incident ที่มีโอกาสเกิด (Likelihood) น้อยกว่า 1%

2. ระดับความรุนแรงของผลกระทบที่เกิดขึ้นจากความเสี่ยง (Impact) เป็นการพิจารณาผลกระทบจากเหตุการณ์ Black Swan ในมุมมอง 5 ด้าน คือ ด้านการเงิน (Finance) ด้านธุรกิจและกระบวนการปฏิบัติงาน (Business and Process Operation) ด้านภาพลักษณ์และชื่อเสียง(Image and Reputation) ด้านลูกค้า/คู่ค้า (Consumer/Customer/Supplier/Dealer) ด้านประชาชน/พนักงาน (People) โดยเหตุการณ์ Incident จะต้องมีผลกระทบรุนแรง (Extreme Impact) อย่างน้อยข้อใดข้อหนึ่งดังต่อไปนี้ ถึงจะเข้าข่าย Black Swan

ตาราง 7 Black Swan Level

Impact Type		Black Swan Level
1) Finance	การเงิน	ความเสียหายที่เกิดขึ้นทั้งหมด >20% ของกำไรสุทธิต่อปีของบริษัท
2) Business Process and Operation	Operation	กำลังการผลิต หรือ ความสามารถในการส่งมอบผลิตภัณฑ์หรือบริการลดลง > 50% เกินกว่าช่วงระยะเวลาที่ยอมรับได้
3) Image and Reputation	ผู้ถือหุ้น	การถูกถอดถอนออกจากตลาดหลักทรัพย์
	ชื่อเสียงองค์กร	ความเชื่อมั่นต่อองค์กรลดลงอย่างรุนแรง และเป็นประเด็นในระดับประเทศที่กระทรวงที่เกี่ยวข้องมีการติดตาม ตรวจสอบ และร่วมดำเนินการแก้ไข
	ชุมชน	ชุมชนรอบโรงงานได้รับผลกระทบในการประกอบอาชีพ หรือสุขภาพ จนต้องอพยพออกจากพื้นที่เป็นเวลา >1 ปี

[1] OR Group Black Swan Criteria ได้รับการอนุมัติโดย OR ERMC ครั้งที่ 1/2565 วันที่ 10 ก.พ. 65 และเกณฑ์ดังกล่าวครอบคลุมถึงบริษัทในกลุ่ม OR ที่มี Critical Infrastructure และ Business Function ของกลุ่ม OR

	สิ่งแวดล้อม	สิ่งแวดล้อมได้รับผลกระทบอย่างเฉียบพลันเป็นวงกว้าง ใช้เวลาฟื้นฟู >1 ปี
4) Consumer/ Customers/Suppliers/Dealer	ลูกค้า/คู่ค้า	- ผู้บริโภค/ลูกค้าต่อต้าน (Boycott) ไม่ซื้อสินค้าและบริการของบริษัทฯ คิดเป็นมูลค่า > 50% ของยอดขายของบริษัท/ปี - คู่ค้าต่อต้าน (Boycott) ยกเลิกธุรกรรมการขายสินค้าและบริการ คิดเป็นมูลค่า > 50% ของยอดขายของบริษัท/ปี
5) People	ประชาชน / พนักงาน	ได้รับบาดเจ็บ ทุพพลภาพ หรือเสียชีวิต จำนวนมาก [2]

4) ขั้นตอน / กระบวนการดำเนินงาน (Procedure / Workflow Process)

1. จัดทำ/ทบทวนเกณฑ์การประเมิน OR Group Black Swan (OR Group Black Swan Criteria) และแบบฟอร์มการจัดทำ Black Swan

2. จัดสื่อความการจัดทำ Black Swan ให้กับหน่วยงานกลยุทธ์สายงานและหน่วยงานที่เกี่ยวข้อง

3. จัดส่งเกณฑ์การประเมินความเสี่ยง Black Swan และแบบฟอร์มการจัดทำ Black Swan ให้กับหน่วยงานกลยุทธ์สายงานและหน่วยงานที่เกี่ยวข้อง เพื่อจัดทำข้อมูล Incident และการประเมินผลกระทบความเสี่ยง

4. จัดทำ Workshop ร่วมกับหน่วยงานกลยุทธ์สายงานและหน่วยงานที่เกี่ยวข้อง เพื่อ Brainstorm การวิเคราะห์เหตุการณ์ Black Swan และคัดเลือกเหตุการณ์ Black Swan ตามผลกระทบสูงสุดที่เกิดขึ้นเพื่อนำไปจัดทำแผนรองรับการบริหารจัดการเหตุการณ์ Black Swan

5. จัดทำ Workshop ร่วมกับหน่วยงานกลยุทธ์สายงานและหน่วยงานที่เกี่ยวข้อง เพื่อนำเหตุการณ์ Black Swan ที่ถูกคัดเลือกมาจัดทำแผนรองรับการบริหารจัดการเหตุการณ์ Black Swan

7. วิเคราะห์และสรุปภาพรวมข้อมูล Black Swan ขององค์กร

ทั้งนี้ ควรมีการจัดทำและทบทวนเหตุการณ์ Black Swan ตามกระบวนการดำเนินงานดังกล่าวข้างต้น เป็นประจำอย่างน้อยปีละ 1 ครั้ง

[2] การพิจารณาจำนวนคนที่ได้รับบาดเจ็บ ทุพพลภาพ หรือเสียชีวิต พิจารณาร่วมกับลักษณะของเหตุการณ์ที่เกิดขึ้น

ภาคผนวก

1) Risk Appetite Perspective

ตาราง 8 Risk Appetite Perspective

Risk Appetite Perspective		**Monitoring Period**
Strategic Risk		
1. Investment Return	1) การลงทุนต้องมี IRR ≥ WACC ยกเว้น Strategic Investment 2) CAPEX for Strategic Investment ต้องไม่เกิน Invested Capital ที่ทำให้ ROIC ใน 5 ปีข้างหน้าลดลงมาต่ำกว่า WACC 3) การลงทุนในโครงการประเภท Venture Capital/Prototype ต้องไม่เกินงบประมาณที่คณะกรรมการบริษัทอนุมัติไว้ตามแผนธุรกิจประจำปี	Yearly
2. Sustainable Business	E/S/G Assessment Scores in Thailand Sustainability Investment (THSI) ≥ 50% for each dimension	Yearly
Business and Operation Risk		
3. Brand Image and Reputation	Net Promoter Score ≥ 30 คะแนน (Great Level 30 - 70 คะแนน)	Yearly
4. Operation Security	No Catastrophic Accident	Quarterly
Information Technology Risk		
5. No critical breach	No Data Breach Interrupting Business	Quarterly
Financial Risk		
6. Financial Ratio	Within policy guideline • Net Debt/Equity ≤ 1 • Net Debt/EBITDA ≤ 2	Quarterly

Risk Appetite Perspective		Monitoring Period
Compliance Risk		
7. Law & Governance Policy	• Zero Non-Compliance • Zero Fraud and / or Corruption	Quarterly

2) แบบฟอร์มการจัดทำ Black Swan

 # Black Swan Event Name

Potential root cause

Event detail & Assumptions:

Picture/Illustration (if necessary)

Impact Type		Black Swan Level
1) Finance	การเงิน	
2) Business Process and Operation	Operation	
3) Image and Reputation	ผู้ถือหุ้น	
	ชื่อเสียงองค์กร	
	ชุมชน	
	สิ่งแวดล้อม	
4) Consumer/ Customers/ Suppliers/Dealer	ลูกค้า/คู่ค้า	
5) People	ประชาชน / พนักงาน	

 # Black Swan Event Name

ช่วงระยะเวลาที่ .... : .....

..... Plan:

1. หน่วยงาน .... ดำเนินการ.... อ้างอิงตาม S_....
2. หน่วยงาน .... ดำเนินการ.... อ้างอิงตาม P_....

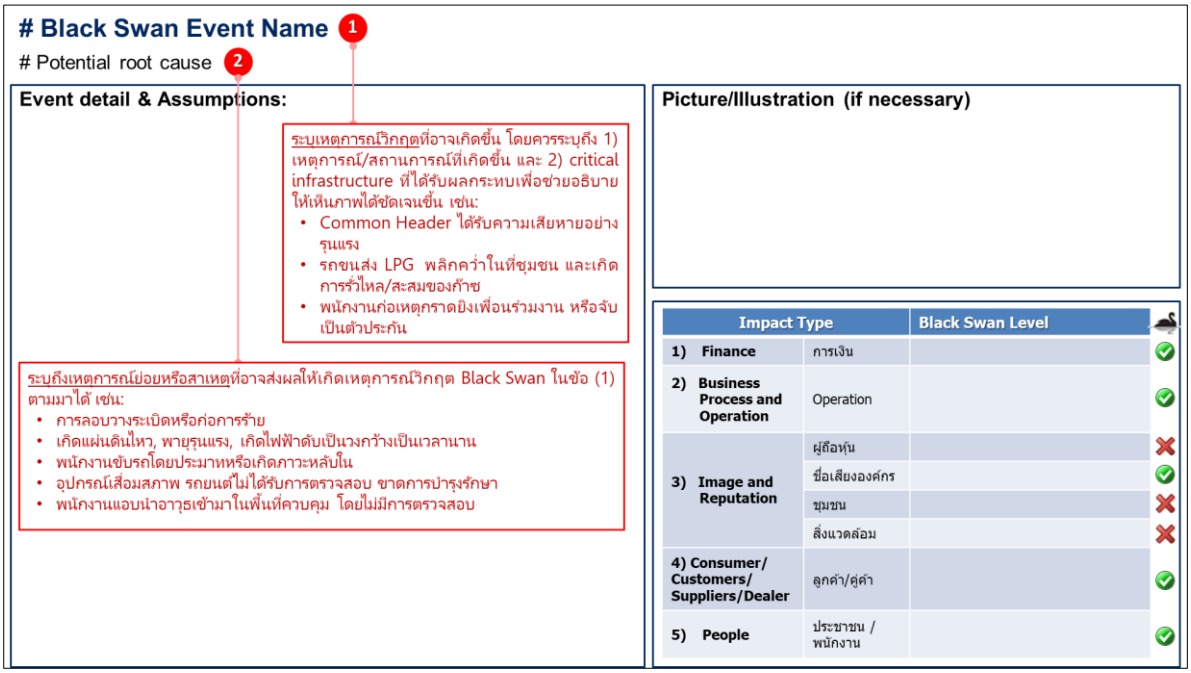
หมายเหตุ :
1. โปรดระบุเอกสาร แผน/มาตรการที่เกี่ยวข้องกับแต่ละขั้นตอนใน Response Plan เช่น Procedure, Work Instruction , Support Document
2. หากยังไม่มีการจัดทำระเบียบ/แผน/มาตรการ จะต้องดำเนินการจัดทำเพิ่มเติม

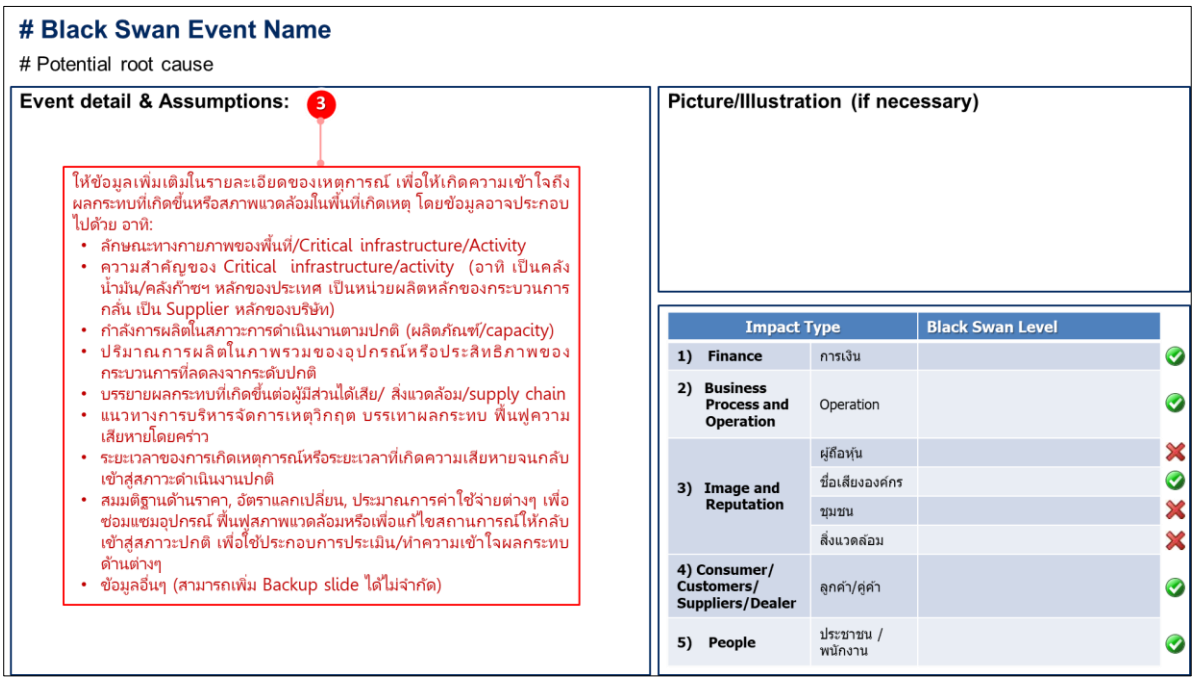
Resource:

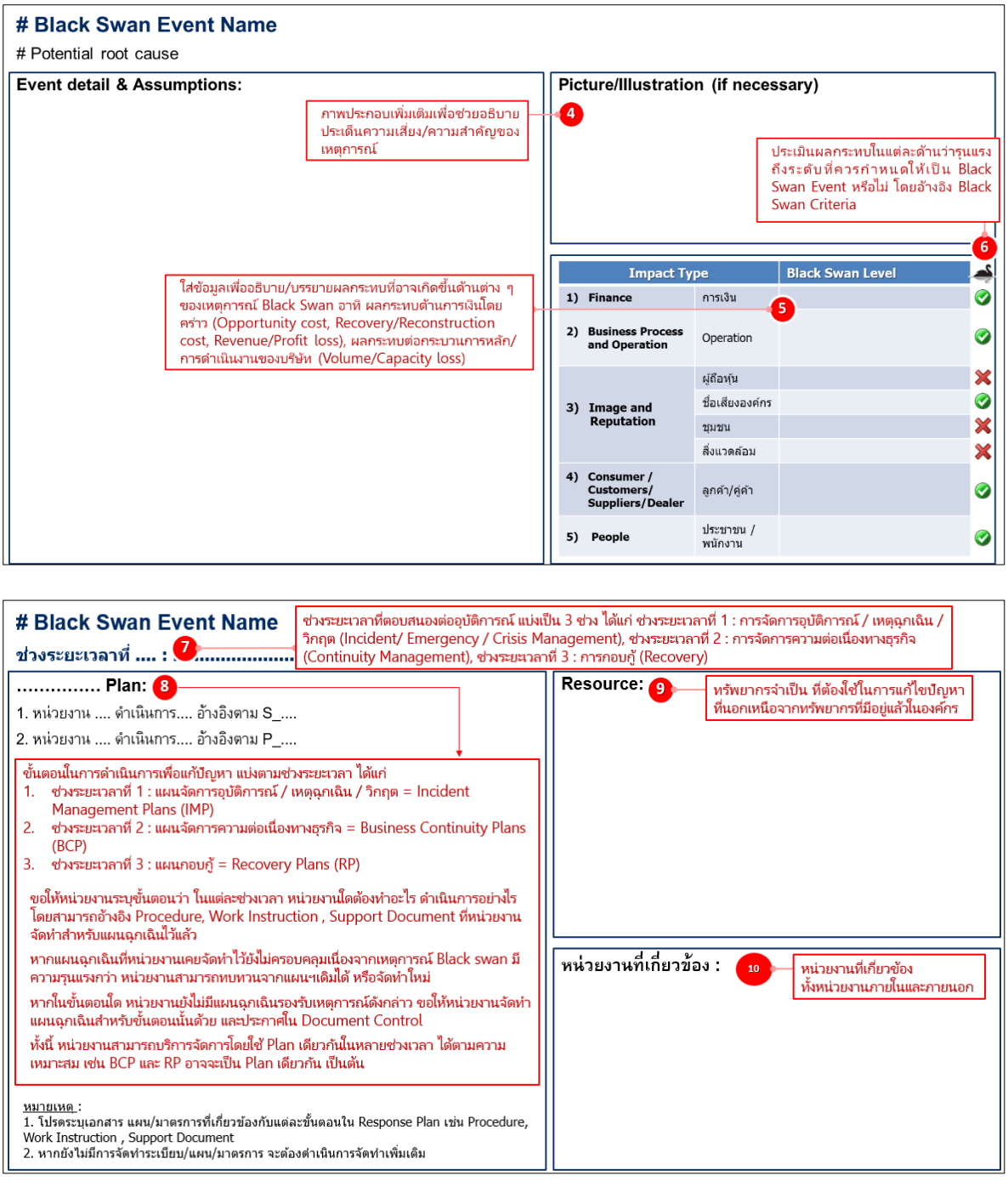
หน่วยงานที่เกี่ยวข้อง :

รูป 24 แบบฟอร์มการจัดทำ Black Swan

3) ขั้นตอนการกรอกแบบฟอร์มการจัดทำ Black Swan







รูป 25 ขั้นตอนการกรอกแบบฟอร์มการจัดทำ Black Swan