นโยบายการบริหารความเสี่ยง

(Risk Management Policy)

บริษัท กิจเจริญ เอ็นจิเนียริ่ง อีเลคทริค จำกัด (มหาชน)

ผู้จัดทำ

(พงศกร ประเวศวัฒนกุล)

เลขานุการบริษัท

ผู้อนุมัติ

(วรุตม์ เตมีย์)

ประธานกรรมการบริหารความเสี่ยง

ประวัติการปรับปรุงแก้ไขเอกสาร

ครั้งที่	วันที่	รายละเอียดการแก้ไข	ผู้อนุมัติ
00	30 มีนาคม 2565	จัดทำครั้งแรก	คณะกรรมการบริหารความเสี่ยง
01	6 มิถุนายน 2565	เพิ่มเติมข้อมูลการประเมินความเสี่ยง	คณะกรรมการบริหารความเสี่ยง
02	20 กุมภาพันธ์ 2568	1) ปรับแก้รูปแบบ 2) จัดกลุ่มหัวข้อใหม่ให้สอดคล้องกับเนื้อหา 3) ย้ายหัวข้อการทบทวนนโยบายมาเป็นข้อที่ 1.5	คณะกรรมการบริหารความเสี่ยง
03	20 กุมภาพันธ์ 2569	ทบทวนประจำปี	คณะกรรมการบริหารความเสี่ยง

คำนำ

บริษัท กิจเจริญ เอ็นจิเนียริ่ง อีเลคทริค จำกัด (มหาชน) (“**บริษัท**”) ตระหนักถึงความสำคัญในเรื่องการบริหารความเสี่ยง (Risk management) ในระบบการบริหารงานและการปฏิบัติงาน โดยมุ่งหมายให้การบริหารความเสี่ยงเป็นวัฒนธรรมของผู้ปฏิบัติงานทุกคน ซึ่งนอกจากจะช่วยให้องค์กรสามารถบรรลุวัตถุประสงค์หลัก และเป้าหมายที่ตั้งไว้แล้วยังเป็นการสนับสนุนให้บริษัทมีการดำเนินงานที่สร้างมูลค่าเพิ่มให้องค์กรอย่างเป็นรูปธรรม ดังนั้นเพื่อให้หน่วยงานต่างๆ ในบริษัทมีแนวทางในการบริหารความเสี่ยงเป็นไปในทิศทางเดียวกัน คณะกรรมการบริหารความเสี่ยงจึงจัดทำนโยบายการบริหารความเสี่ยงของบริษัท กิจเจริญ เอ็นจิเนียริ่ง อีเลคทริค จำกัด ฉบับนี้ขึ้นเพื่อให้เป็นนโยบายบริหารความเสี่ยงในการปฏิบัติงานสำหรับพนักงานทุกคน อันจะก่อให้เกิดการบรรลุวัตถุประสงค์การบริหารความเสี่ยงทั่วทั้งองค์กร และเกิดประโยชน์สูงสุดแก่บริษัทฯ ต่อไป

คณะกรรมการบริหารความเสี่ยง

สารบัญ

นโยบายการบริหารความเสี่ยง

Risk Management Policy

1. แนวทางและประโยชน์ของการบริหารความเสี่ยง

1.1. คำนิยาม

"**การบริหารความเสี่ยง**" หมายถึง กระบวนการดำเนินการเกี่ยวกับความเสี่ยง ในการดำเนินงานของบริษัทตามเป้าหมายที่ได้วางไว้ โดยจัดให้มีระบบและแบบแผนในการปฏิบัติงานด้านความเสี่ยง เพื่อการจัดการความเสี่ยงที่ส่งผลกระทบต่อบริษัทให้ระดับ และขนาดของผลกระทบที่จะเกิดขึ้นอยู่ในระดับที่สามารถยอมรับได้ รวมทั้งมีการประเมินควบคุมและการตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมายของบริษัทเป็นสำคัญ

"**ความเสี่ยง**" หมายถึง เหตุการณ์การกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบ หรือสร้างความเสียหาย หรือความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จของเป้าหมายและวัตถุประสงค์ของบริษัทที่กำหนดไว้ ซึ่งผลกระทบอาจเป็นตัวเงินหรือผลกระทบที่มีต่อภาพลักษณ์และชื่อเสียง ทั้งในระดับองค์กร ระดับหน่วยงาน และระดับบุคคลได้

"**คณะผู้ปฏิบัติงาน**" หมายถึง ผู้จัดการฝ่าย ผู้จัดการแผนกและพนักงานในองค์กรทุกคน

1.2. วัตถุประสงค์ของการบริหารความเสี่ยง

1.2.1. เพื่อจัดการปัญหาอุปสรรคในการทำงาน

1.2.2. เพื่อป้องกัน หรือลดโอกาสที่จะเกิดเหตุการณ์ไม่พึงประสงค์และผลกระทบที่อาจเกิดขึ้น ซึ่งจะทำให้การดำเนินงานไม่บรรลุวัตถุประสงค์และเป้าหมายขององค์กร

1.2.3. เพื่อเป็นการส่งเสริมให้มีการกำกับดูแลกิจการที่ดี และให้เกิดความมั่นใจว่าบริษัทมีการกำหนดหน้าที่ความรับผิดชอบในการควบคุมความเสี่ยงที่ได้ระบุไว้อย่างเหมาะสม

1.3. ขอบเขตการบริหารความเสี่ยง

เพื่อให้การดำเนินงานมีความต่อเนื่องและบรรลุตามวัตถุประสงค์ของบริษัทฯ ดังนั้น ทุกหน่วยงานต้องมีการบริหารความเสี่ยง โดยให้การบริหารความเสี่ยงเป็นกระบวนการหนึ่งในการปฏิบัติงานประจำวันของพนักงานทุกคน โดยมีจุดมุ่งหมายให้การบริหารความเสี่ยงถูกปลูกฝังเป็นส่วนหนึ่งของวัฒนธรรมองค์กร

1.4. นโยบายการบริหารความเสี่ยง

ทุกหน่วยงานต้องจัดให้มีการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่องภายใต้กระบวนการบริหารความเสี่ยงที่เป็นมาตรฐานเดียวกัน โดยการนำเทคโนโลยีสารสนเทศมาใช้ เพื่อให้เกิดความรวดเร็วในการสื่อสารและประมวลผลตลอดจนต้องมีการติดตามและประเมินผลพร้อมปรับแผนการบริหารความเสี่ยงเป็นระยะ ๆ อย่างสม่ำเสมอเพื่อให้การดำเนินการบรรลุวัตถุประสงค์

1.5. การทบทวนนโยบาย

นโยบายบริหารความเสี่ยงจะต้องได้รับการทบทวนปีละหนึ่งครั้ง และนำเสนอให้คณะกรรมการบริษัทพิจารณาอนุมัติต่อไป

1.6. ประโยชน์ของการบริหารความเสี่ยง

เมื่อบริษัทมีการบริหารความเสี่ยงที่ดีและเหมาะสมแล้ว บริษัทจะได้ประโยชน์โดยตรงจากการบริหารความเสี่ยง ดังนี้

1.6.1. ทำให้ผลการดำเนินงานของบริษัทเป็นไปตามเป้าหมายและวัตถุประสงค์ของบริษัทที่ได้ตั้งไว้ อีกทั้งยังเป็นการส่งเสริมให้เกิดการเจริญเติบโตทางธุรกิจอย่างต่อเนื่องและยั่งยืนเพื่อสร้างมูลค่าเพิ่มให้กับบริษัทและผู้มีส่วนได้ส่วนเสีย รวมถึงส่งเสริมให้เกิดการกำกับดูแลกิจการที่ดี

1.6.2. ส่งเสริมให้พนักงานเกิดความรู้ความเข้าใจและตระหนักถึงความสำคัญของการบริหารความเสี่ยงซึ่งจะส่งผลต่อเนื่อง ให้เกิดความระมัดระวังในการทำงานและลดโอกาสที่จะทำให้เกิดการสูญเสียจากการดำเนินงาน

1.6.3. ในการจัดทำแผนงานโครงการต่าง ๆ บริษัทสามารถนำผลของการวิเคราะห์ความเสี่ยงที่เกิดขึ้นใช้เป็นส่วนหนึ่งเพื่อประกอบการตัดสินใจในการดำเนินโครงการใดหรือไม่ที่จะส่งผลกระทบต่อบริษัท

1.6.4. ช่วยให้การกำหนดวัตถุประสงค์และกลยุทธ์ของบริษัทมีความสมบูรณ์และความเป็นไปได้มากขึ้นและสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้

1.6.5. ส่งเสริมให้เกิดการเตรียมความพร้อมและแนวทางแก้ไขปัญหาที่อาจจะเกิดขึ้นและส่งผลกระทบกับผลการดำเนินงานของบริษัท

1.6.6. มีระบบเทคโนโลยีและสารสนเทศที่ช่วยในการจัดเก็บข้อมูล การคำนวณต่าง ๆ การรายงานและการสอบทานข้อมูลได้ อย่างถูกต้องครบถ้วนสมบูรณ์รวดเร็ว

1.6.7. ผู้บริหารมีข้อมูลเพื่อใช้ประกอบในการตัดสินใจได้อย่างถูกต้องและรวดเร็วยิ่งขึ้น

1.6.8. มีการจัดสรรทรัพยากรอย่างเหมาะสมโดยคำนึงถึงความคุ้มค่าในการลงทุน

1.6.9. เกิดการมีส่วนร่วมของพนักงานในบริษัท และการบูรณาการเข้ากับระบบงานส่วนอื่นขององค์กรที่จะร่วมกันผลักดันให้องค์กรเกิดผลสำเร็จตามวัตถุประสงค์ที่ตั้งไว้

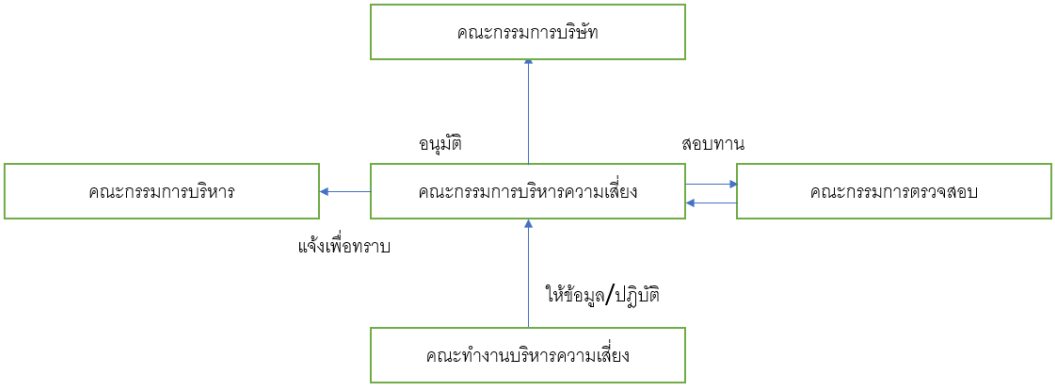
2. โครงสร้างการบริหารความเสี่ยงของบริษัท

โครงสร้างการบริหารความเสี่ยงประกอบด้วย คณะกรรมการบริหารความเสี่ยงและคณะทำงานบริหารความเสี่ยงในระดับฝ่าย คือ

2.1. ระดับองค์กร ได้แก่ คณะกรรมการบริหารความเสี่ยง โดยมีประธานกรรมการบริหารความเสี่ยงเป็นประธาน มีหน้าที่และความรับผิดชอบเป็นไปตามแนวทางปฏิบัติของบริษัท

2.2. ระดับฝ่าย หรือเรียกว่า “**คณะทำงาน**” ได้แก่ ผู้จัดการฝ่าย ผู้จัดการแผนก และพนักงานภายในองค์กรทุกคน ปฏิบัติงานด้านการบริหารความเสี่ยงภายใต้การกำกับดูแลของคณะกรรมการบริหารความเสี่ยง

รูปที่ 1 โครงสร้างการบริหารความเสี่ยง



3. หน้าที่และความรับผิดชอบของคณะกรรมการต่างๆ ในระบบการบริหารความเสี่ยง

3.1. หน้าที่ความรับผิดชอบของคณะกรรมการบริหารความเสี่ยง

คณะกรรมการบริหารความเสี่ยง หน้าที่และความรับผิดชอบดังนี้

3.1.1. กำหนดนโยบายและโครงสร้างการบริหารความเสี่ยงโดยรวมของบริษัท ซึ่งครอบคลุมถึงความเสี่ยงที่สำคัญ เช่น ความเสี่ยงด้านการเงิน ความเสี่ยงด้านการลงทุน และความเสี่ยงที่มีผลกระทบต่อ ชื่อเสียงของกิจการ เป็นต้น เพื่อนำเสนอคณะกรรมการบริษัทให้ความเห็นชอบ โดยให้สอดคล้องและเป็นไปตามแนวทางการบริหารความเสี่ยงของตลาดหลักทรัพย์แห่งประเทศไทย และสมาคมผู้ตรวจสอบภายในแห่งประเทศไทย

3.1.2. กำหนดยุทธศาสตร์และแนวทางในการบริหารความเสี่ยงของบริษัทให้สอดคล้องกับนโยบายการบริหารความเสี่ยง เพื่อให้สามารถประเมิน ติดตาม และควบคุมความเสี่ยงแต่ละประเภทให้อยู่ในระดับที่ยอมรับได้ โดยให้หน่วยงานต่าง ๆ มีส่วนร่วม ในการบริหารและควบคุมความเสี่ยง

3.1.3. ดูแลและติดตามการปฏิบัติตามนโยบายการบริหารความเสี่ยงภายใต้แนวทางและนโยบายที่ได้รับอนุมัติจากคณะกรรมการบริษัท

3.1.4. กำหนดเกณฑ์วัดความเสี่ยงและเพดานความเสี่ยงที่บริษัทจะยอมรับได้

3.1.5. กำหนดมาตรการที่จะใช้ในการจัดการความเสี่ยงให้เหมาะสมต่อสภาวการณ์

3.1.6. ประเมินความเสี่ยงในระดับองค์กร และกำหนดวิธีการบริหารความเสี่ยงนั้นให้อยู่ในระดับที่ยอมรับได้ รวมทั้งควบคุมดูแลให้มีการบริหารความเสี่ยงตามวิธีการที่กำหนดไว้

3.1.7. ทบทวนนโยบายการบริหารความเสี่ยงและปรับปรุงให้มีประสิทธิภาพและประสิทธิผลอย่างเพียงพอ ที่จะควบคุมความเสี่ยง

3.1.8. มีอำนาจในการเรียกบุคคลที่เกี่ยวข้องมาชี้แจง หรือแต่งตั้งและกำหนดบทบาทที่ให้ผู้ปฏิบัติงานทุกระดับมีหน้าที่บริหารความเสี่ยงตามความเหมาะสม และให้รายงานต่อคณะกรรมการบริหารความเสี่ยงเพื่อให้การบริหารความเสี่ยงบรรลุวัตถุประสงค์

3.1.9. รายงานผลเกี่ยวกับการบริหาร การดำเนินงาน และสถานะความเสี่ยงของบริษัท และการเปลี่ยนแปลงต่าง ๆ รวมถึงสิ่งที่ต้องดำเนินการปรับปรุงแก้ไขเพื่อให้สอดคล้องกับนโยบายและกลยุทธ์ที่กำหนดต่อคณะกรรมการตรวจสอบ เพื่อสอบทานและนำเสนอต่อคณะกรรมการบริษัทอย่างสม่ำเสมอ

3.1.10. จัดทำคู่มือการบริหารความเสี่ยงระดับองค์กรประจำปี

3.1.11. จัดวางระบบบริหารความเสี่ยงแบบบูรณาการโดยเชื่อมโยงระบบสารสนเทศ

3.2. หน้าที่ความรับผิดชอบของคณะผู้ปฏิบัติงาน

คณะผู้ปฏิบัติงานมีหน้าที่ความรับผิดชอบ ดังนี้

3.2.1. เป็นผู้รับแนวทางการบริหารความเสี่ยงไปจัดทำแผนรองรับความเสี่ยงที่เกี่ยวข้อง

3.2.2. ดำเนินการและรายงานผลการดำเนินการตามแนวทางที่คณะกรรมการบริหารความเสี่ยงระบุไว้ใน “คู่มือบริหารความเสี่ยงระดับองค์กรประจำปีของแต่ละปี”

3.2.3. ประเมินผลและจัดทำรายงานการบริหารความเสี่ยงของแต่ละฝ่าย หรือแต่ละแผนก ให้เลขานุการคณะกรรมการบริหารความเสี่ยง ตามกำหนดเวลา ภายใต้การกำกับดูแลของคณะกรรมการบริหารความเสี่ยง

3.2.4. ปฏิบัติงานอื่นๆ ตามที่คณะกรรมการบริหารความเสี่ยงมอบหมาย

3.3. หน้าที่ความรับผิดชอบของคณะกรรมการตรวจสอบ (Audit Committee)

3.3.1. สอบทานนโยบายการบริหารความเสี่ยง และคู่มือการบริหารความเสี่ยงระดับองค์กร เพื่อแน่ใจว่าบริษัทมีระบบบริหารความเสี่ยงที่เหมาะสมและมีประสิทธิผลในการกำกับดูแลกิจการที่ดี

3.3.2. ติดตามการบริหารความเสี่ยงอย่างเป็นอิสระ

3.3.3. สื่อสารกับคณะกรรมการบริหารความเสี่ยง เพื่อให้เข้าใจความเสี่ยงที่สำคัญและเชื่อมโยงกับการควบคุมภายใน

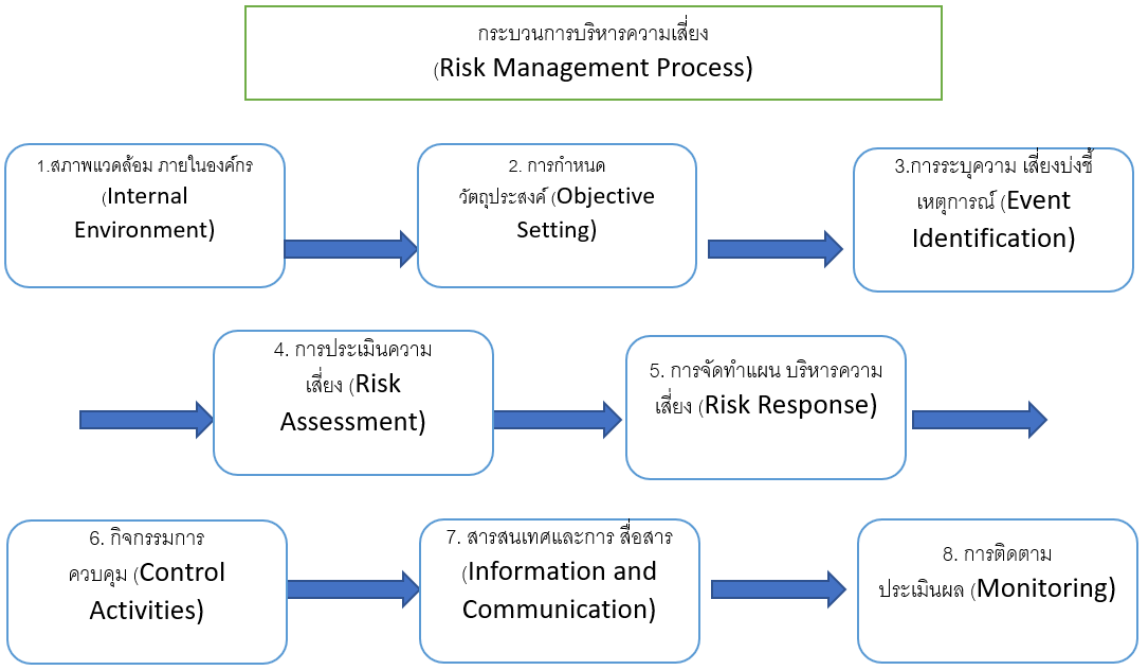
3.4. หน้าที่ความรับผิดชอบของฝ่ายตรวจสอบภายใน

ฝ่ายตรวจสอบภายในมีหน้าที่รับผิดชอบในการสอบทานและประเมินประสิทธิผลของกระบวนการบริหารความเสี่ยงว่าบริษัทมีระบบบริหารความเสี่ยงที่เหมาะสม และมีประสิทธิผลในการกำกับดูแลกิจการที่ดี

4. กระบวนการของการบริหารความเสี่ยงตามแนวทางของ COSO

บริษัทได้รับระบบการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management Integrated Framework) ตาม แนวทางของ The Committee of Sponsoring Organizations of the Treadway Commission (COSO) มาใช้เป็นแนวทาง ในการบริหารความเสี่ยง ซึ่งมีกระบวนการในการบริหารความเสี่ยงที่ทุกหน่วยงานต้องดำเนินการอย่างต่อเนื่อง 8 ขั้นตอน ดังรายละเอียดต่อไปนี้

รูปที่ 2 กระบวนการของการบริหารความเสี่ยง



4.1. ขั้นตอนที่ 1 การวิเคราะห์สภาพแวดล้อมภายในองค์กร (Internal Environment)

สภาพแวดล้อมขององค์กรเป็นองค์ประกอบที่สำคัญ ในการกำหนดกรอบการบริหารความเสี่ยง ซึ่งประกอบด้วยปัจจัยหลายประการ เช่น วัฒนธรรมองค์กร นโยบายของผู้บริหาร แนวทางการปฏิบัติงาน บุคลากร กระบวนการทำงาน ระบบสารสนเทศ เป็นต้น

สภาพแวดล้อมภายในองค์กรประกอบเป็นพื้นฐานสำคัญในการกำหนดทิศทางของกรอบการบริหารความเสี่ยงขององค์กร ในขั้นตอนนี้เป็นการระบุสภาพแวดล้อมภายในองค์กร ซึ่งระบบจะรับข้อมูลจากการที่ผู้ใช้งานตอบ แบบสอบถาม แล้วนำมาวิเคราะห์เพื่อแสดงออกเป็นรายงาน

บริษัทควรจัดให้มีสภาพแวดล้อมและบรรยากาศที่เอื้ออำนวย ซึ่งเป็นพื้นฐานสำหรับขั้นตอนอื่นๆ ในการบริหารความเสี่ยงในองค์กร หากไม่มีสภาพแวดล้อมภายในองค์กรที่ดี จะมีผลต่อการกำหนดกลยุทธ์และเป้าหมายของบริษัท ดังนั้น จึงควรมีการกำหนดกิจกรรมการบ่งชี้การประเมินและการจัดการกับความเสี่ยง ทั้งนี้ องค์ประกอบที่สำคัญต่อสภาพแวดล้อม ประกอบด้วย

(1) ปรัชญา ความเชื่อ วัฒนธรรมในการบริหารความเสี่ยง เพื่อสร้างมูลค่าให้กับบริษัทในระยะยาว

(2) บทบาทของคณะกรรมการตรวจสอบเป็นปัจจัยสำคัญในการกำกับดูแลการบริหารความเสี่ยง

(3) การคัดเลือกบุคลากรที่มีความรู้ความสามารถ ความซื่อสัตย์ และพัฒนาให้เหมาะสมกับงานที่รับผิดชอบ

(4) จัดให้มีโครงสร้างองค์กรที่เหมาะสม

การกำหนดอำนาจหน้าที่ที่เหมาะสม ให้พนักงานสามารถปฏิบัติหน้าที่ให้บรรลุวัตถุประสงค์ของบริษัท

4.2. ขั้นตอนที่ 2 การกำหนดวัตถุประสงค์ (Objective Setting)

ขั้นตอนนี้ ผู้ใช้งานจะต้องบันทึกแผนงาน หรือโครงการของหน่วยงาน และระบุวัตถุประสงค์ของแผนงาน หรือ โครงการ ตัวชี้วัดระดับองค์กรที่สอดคล้องกับแผนงานหรือโครงการ ระบุประเด็นยุทธศาสตร์ที่แผนงานหรือโครงการนั้นๆ สนับสนุน กิจกรรมต่างๆ (เฉพาะกิจกรรมหลัก) ที่มีอยู่ภายใต้แต่ละแผนงานหรือโครงการ และวัตถุประสงค์ของการควบคุมของแต่ละกิจกรรมหลักนั้น ๆ เพื่อให้ทราบขอบเขตการดำเนินงานในแต่ระดับ และสามารถวิเคราะห์ความเสี่ยงที่คาดว่าจะเกิดขึ้นได้อย่างครบถ้วน ดังนั้น การกำหนดวัตถุประสงค์ในการบริหารความเสี่ยงที่ดีของระดับหน่วยงานเพื่อให้วัตถุประสงค์ในภาพรวมบรรลุเป้าหมายได้ ควรมีลักษณะดังนี้

4.2.1. ต้องมีความชัดเจน สามารถวัดได้ สามารถปฏิบัติได้ มีเหตุผล และมีกรอบระยะเวลาที่จะดำเนินการได้แล้ว เสร็จ ซึ่งเป็นไปตามหลักการ “SMART” หมายถึง

Specific: เฉพาะเจาะจง / ชัดเจน

Measurable: สามารถวัดได้

Achievable : สามารถบรรลุผลได้ / ปฏิบัติได้

Reasonable : เป็นจริงได้ / สมเหตุสมผล

Time Constrained: มีกำหนดเวลา / กรอบเวลา

4.2.2. จะต้องเชื่อมโยงกับเป้าหมายและสอดคล้องกับวัตถุประสงค์ของบริษัทฯ หรือตัวชี้วัดของหน่วยงานและสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และระดับของความเบี่ยงเบนจากระดับความ เสี่ยงที่ยอมรับได้ (Risk Tolerance)

Risk Appetite หมายถึง ประเภทปัจจัยความเสี่ยงและระดับของความเสี่ยงที่บริษัทฯ ยอมรับได้เพื่อช่วย ให้บริษัทฯ บรรลุวิสัยทัศน์และภารกิจของบริษัท

Risk Tolerance หมายถึง ระดับความเบี่ยงเบนจากประเภทปัจจัยความเสี่ยงและระดับของความเสี่ยงที่ ยอมรับได้

4.3. ขั้นตอนที่ 3 การระบุความเสี่ยง/บ่งชี้เหตุการณ์ (Event Identification)

ในขั้นตอนนี้ เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงาน ทั้งในส่วนของปัจจัยเสี่ยงที่เกิดจากภายในและภายนอกองค์กร เช่น นโยบายบริหารงาน บุคลากร การปฏิบัติงาน การเงิน ระบบสารสนเทศ ระเบียบ กฎหมาย ระบบบัญชี ภาษีอากร ทั้งนี้เพื่อทำความเข้าใจต่อเหตุการณ์และสถานการณ์นั้น เพื่อให้ผู้บริหารสามารถพิจารณากำหนดแนวทางและนโยบายในการจัดการกับความเสี่ยงที่อาจจะเกิดขึ้นได้เป็นอย่างดี ซึ่งการระบุความเสี่ยงมีขั้นตอน ดังนี้

4.3.1. พิจารณาจากกิจกรรม โครงการ กระบวนการทำงานที่เกี่ยวข้อง ตามแผนงานต่างๆ ของบริษัทฯ เช่น แผนปฏิบัติการประจำปี และแผนธุรกิจประจำปี และอื่นๆ เป็นต้น ที่จะทำให้ไม่สามารถบรรลุวัตถุประสงค์ และเป้าหมาย

4.3.2. ระบุความเสี่ยงหรือค้นหาความเสี่ยงและสาเหตุ โดยพิจารณาแหล่งที่มาของความเสี่ยงทั้งปัจจัยภายในและ ปัจจัยภายนอก ที่มีผลทำให้การดำเนินการของแต่ละกิจกรรม โครงการ กระบวนการทำงาน ไม่บรรลุ วัตถุประสงค์และเป้าหมาย

4.3.2.1. วิธีการระบุความเสี่ยงที่สำคัญ อาจทำได้ดังนี้

(1) วิเคราะห์ทางเดินของงานและเอกสาร หรือวิเคราะห์กระบวนการ

(2) การระดมสมอง

(3) จัดประชุมเชิงปฏิบัติการ

(4) การเก็บข้อมูลประวัติเหตุการณ์ความเสียหายที่เกิดขึ้น

(5) อื่นๆ

4.3.2.2. แหล่งที่มาของความเสี่ยงจากปัจจัยภายใน อาจมาจากปัจจัยต่างๆ ดังนี้

(1) วัตถุประสงค์ของบริษัทฯ

(2) นโยบายและกลยุทธ์การดำเนินงาน กระบวนการทำงาน

(3) โครงสร้างองค์กรและระบบการบริหารงาน

(4) ข้อมูลทางบัญชีและการเงิน

(5) อื่นๆ

4.3.2.3. แหล่งที่มาของความเสี่ยงจากปัจจัยภายนอก อาจมาจากปัจจัยต่างๆ ดังนี้

(1) นโยบายของรัฐบาล

(2) สภาวะเศรษฐกิจ

(3) การแข่งขัน (คู่แข่งขันทางการดำเนินธุรกิจ)

(4) กฎหมาย รวมถึงกฎเกณฑ์ หรือระเบียบต่าง ๆ

(5) เหตุการณ์ธรรมชาติ สงคราม หรือโรคระบาด

(6) อื่นๆ

4.3.3. การจัดประเภทความเสี่ยง สามารถแบ่งเป็น 7 ประเภท ดังนี้

4.3.3.1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) หมายถึง ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์และการปฏิบัติตามแผนกลยุทธ์อย่างไม่เหมาะสม รวมถึงความไม่สอดคล้องกันระหว่างนโยบาย เป้าหมายกลยุทธ์ โครงสร้างองค์กร ภาวะการณ์แข่งขัน

4.3.3.2. ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk) หมายถึง ความเสี่ยงที่เกิดจากการปฏิบัติงานทุกๆขั้นตอนโดยครอบคลุมถึงปัจจัยที่เกี่ยวข้องกับกระบวนการ อุปกรณ์ เทคโนโลยีและบุคลากรในการปฏิบัติงาน

4.3.3.3. ความเสี่ยงด้านกฎหมายกฎระเบียบ (Compliance Risk) หมายถึง ความเสี่ยงที่เกิดจากการไม่สามารถปฏิบัติตามกฎระเบียบ กฎหมายที่เกี่ยวข้องได้ หรือกฎระเบียบกฎหมายที่มีอยู่ไม่เหมาะสมหรือเป็นอุปสรรคในการปฏิบัติงาน

4.3.3.4. ความเสี่ยงด้านการทุจริตคอร์รัปชัน (Fraud Risk Governance) เพื่อแสดงท่าที (Tone at the Top)ของ คณะกรรมการบริษัท ในเรื่องการต่อต้านการทุจริตในองค์กร คณะกรรมการตรวจสอบ มีวิธีการ เชิงรุกในการติดตามผลการจัดการ ความเสี่ยงใน

เรื่องการทุจริต (Fraud Risk Management) หรือ FRM ผู้บริหารมีการออกแบบสร้าง Fraud Risk Management Program (FRMP) และ รายงานผล ให้คณะกรรมการ และคณะกรรมการตรวจสอบ ทราบเป็นระยะ พนักงานต้องเข้าใจ Red Flags และรายงานทันทีเมื่อพบสิ่งบอกเหตุว่าจะเกิดการทุจริต ผู้ตรวจสอบภายในจะต้องมี การประเมิน FRMP ว่ามีประสิทธิผล เพื่อความมั่นใจต่อคณะกรรมการ ฯว่าการบริหารความเสี่ยงของผู้บริหารในเรื่องทุจริตอยู่ในระดับที่คณะกรรมการฯยอมรับ

4.3.3.5. ความเสี่ยงด้านเทคโนโลยีสารสนเทศมีความเสี่ยงหลักๆ ดังนี้

(1) ความไม่พร้อมในการใช้งานระบบเทคโนโลยีสารสนเทศ (Available)

(2) การไม่สามารถเข้าถึงข้อมูลและระบบงานของบุคคลต่างๆ (Access)

(3) ความไม่ถูกต้องและความไม่ทันสมัยของข้อมูล (Accuracy)

(4) ความไม่คล่องตัวในการปรับแนวทางการดำเนินธุรกิจให้สอดคล้องกับการดำเนินธุรกิจและกลยุทธ์ (Agility)

4.3.3.6. ความเสี่ยงของระบบบัญชีและการเงิน (Financial Risk)

เป็นความเสี่ยงที่จะนำไปสู่ความผันผวนทางการเงิน ที่อาจจะแยกเป็นส่วนที่มีผลกระทบทางตรงต่อการประกอบการ และส่วนที่มีผลกระทบทางอ้อมต่อกิจการ เช่น

(1) ระบบการธนาคารและสถาบันการเงินมีความอ่อนแอ

(2) ตลาดสินทรัพย์ตกต่ำซบเซา

(3) โครงสร้างการกำกับดูแลระบบการเงินอ่อนแอ

(4) มาตรฐานการบัญชีมีผลต่อการเปิดเผยข้อมูลทางการเงินที่ครบถ้วนถูกต้อง

(5) ฐานะการเงินการคลังของภาครัฐ

(6) ความไหวตัวของภาคสถาบันการเงินต่อความเปลี่ยนแปลงผันผวนของระบบการเงิน

(7) การบังคับใช้เกณฑ์ตามมาตรฐาน Basel II มาตรฐานความมั่นคงตามเกณฑ์ของธนาคารโลก

4.3.3.7. ความเสี่ยงด้านเศรษฐกิจ สังคม และการเมือง แบ่งเป็นประเภทย่อย ๆ ได้ดังต่อไปนี้

(1) ความเสี่ยงทางเศรษฐกิจ (Economic Risk)

เป็นความเป็นไปได้ที่เศรษฐกิจของประเทศ จะเกิดความอ่อนแอจากระดับพื้นฐาน ซึ่งเป็นเหตุให้ผลการดำเนินงาน เสถียรภาพของรายได้ ปริมาณธุรกิจได้รับผลกระทบกระเทือนในทางลบ โดยทั่วไปแล้วประเด็นทาง เศรษฐกิจควรจะ

ประกอบด้วย การเติบโตหรือชะลอตัวทางเศรษฐกิจ สถานะการเงินและการคลังของภาครัฐ ธุรกรรมการติดต่อระหว่างประเทศ ด้านการค้าระหว่างประเทศและดุลการชำระเงินระหว่างประเทศ และแนวโน้มของการเติบโตและเสถียรภาพทางเศรษฐกิจ

(2) ความเสี่ยงด้านสังคม (Social Risk Management)

แนวโน้มของสถานการณ์ในระดับโลกมากมายได้นำไปสู่สถานการณ์ความเสี่ยงทางสังคม (Social Risk) ทั้งทางตรงและทางอ้อม โดยเฉพาะการเชื่อมโยงถึงกันของผู้คนในประเทศต่าง ๆ และการพึ่งพาอาศัยกันมากขึ้น ทั้งในด้านของความสัมพันธ์ทางการค้า และห่วงโซ่อุปทาน กระแสการไหลทางการเงินระหว่างประเทศ การอพยพ เคลื่อนย้ายของแรงงานการสื่อสารและเทคโนโลยีสารสนเทศทำให้กำแพงของการการสื่อสารทลายลง

นอกจากนี้ ภายในประเทศเองก็มีความเปลี่ยนแปลงไปในลักษณะเกี่ยวข้องสัมพันธ์กัน รัฐบาลอาจจะขอให้ภาคเอกชนช่วยผลิตบริการ หรือสินค้าสาธารณะให้ เช่น การศึกษา ระบบรักษาความปลอดภัย หรือภาคเอกชนอาจจะ ขอให้ NGOs ช่วยคุ้มครองทรัพย์สินทางปัญญา หรือ NGOs อาจจะขอให้ภาคเอกชนประกันการเคารพในสิทธิ มนุษยชน การพึ่งพาอาศัยเกี่ยวข้องกันดังกล่าวเป็นบ่อเกิดของความเสี่ยงทางสังคมที่เพิ่มขึ้นในสังคมและทำให้เกิดสภาพแวดล้อมรูปแบบใหม่ซึ่งไม่อาจใช้กลยุทธ์ทางธุรกิจแบบดั้งเดิมในการบริหารจัดการ

ทั้งนี้ การที่จะเกิด Social Risk กับกิจการก็จะประกอบด้วย 4 องค์ประกอบด้วยกัน ได้แก่

- ประเด็นทางสังคมและสภาพแวดล้อม ได้แก่ การเปลี่ยนแปลงของภูมิอากาศโลกที่มีแนวโน้มร้อนขึ้นหรือการแพร่ระบาดของโรคบางโรคหรือการอพยพของคนจากชนบทเข้าสู่ตัวเมือง
- ความคาดหวังและความเกี่ยวข้องของผู้มีส่วนได้ส่วนเสียเพิ่มเติม เป็นกลุ่มของผู้มีส่วนได้ส่วนเสีย กลุ่มใหม่ที่เพิ่มเติมขึ้นไปจากกลุ่มผู้มีส่วนได้ส่วนเสียดั้งเดิมที่มีอยู่แล้ว เช่น องค์กรคุ้มครอง สิ่งแวดล้อม กลุ่มคุ้มครองสิทธิเด็กและสตรี แม้แต่บุคคลธรรมดาที่มีบทบาทในการปกป้องสังคมเพิ่มขึ้น
- การรับรู้ในทางลบเกี่ยวกับกิจการ เป็นการเกิดข้อมูลทางลบเกี่ยวกับบริษัทที่ผ่านแหล่งข่าวของ ทางและการบอกต่อทางอินเทอร์เน็ตผ่านสื่อสังคมออนไลน์ บุคลากรภายในกิจการเองออกไปให้ ข่าวภายนอก การส่งข้อมูลเหล่านี้ทำให้

เกิดการสั่งสมและทัศนคติในทางลบ

- ช่องทางที่นำไปสู่ความเสียหาย การกระจายความเห็นผ่านเครือข่ายทั้งเล็กและใหญ่ เช่น การ ส่ง forward e-mail ไปจนถึงการให้ความเห็นในที่สาธารณะ การคว่ำบาตร (boycott) การออกมารณรงค์ ต่อต้าน

(3) ความเสี่ยงทางการเมือง (Political Risk)

เป็นความเป็นไปได้ที่รัฐบาลจะมีการบริหารประเทศอย่างไม่มีประสิทธิภาพ ซึ่งอาจพิจารณาจาก

- การเปลี่ยนแปลงตัวผู้บริหารในรัฐบาลย่อย ความไร้เสถียรภาพของรัฐ
- แรงกดดันและความแตกแยกในสังคม ความไม่สงบในสังคม การชุมนุมทางการเมือง หรือการก่อเหตุจลาจล
- ระบบการบังคับใช้กฎหมายไม่เพียงพอ
- มีปัญหาความไม่สงบในบางพื้นที่
- มีปัญหาความขัดแย้งทางการเมืองระหว่างประเทศ
- โครงสร้างพื้นฐานด้านความมั่นคงของประเทศ
- นโยบายของรัฐไม่เหมาะสม

4.4. ขั้นตอนที่ 4 การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงเป็นการจำแนกและพิจารณาจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่ โดยการประเมินจาก โอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) โดยสามารถประเมินความเสี่ยงได้ทั้งจากปัจจัยความเสี่ยงภายนอกและ ปัจจัยความเสี่ยงภายในองค์กร

การประเมินความเสี่ยง หมายถึง การวัดระดับความรุนแรงของความเสี่ยงว่ามีมากน้อยเพียงใด โดยนำความเสี่ยงที่ได้จากขั้นตอนที่ 3 (การระบุความเสี่ยง) มาประเมินความเสี่ยงโดยมีขั้นตอน ดังนี้

4.4.1. พิจารณาความเสี่ยงที่เกิดขึ้นจากการดำเนินการก่อนมีมาตรการการควบคุมความเสี่ยงที่ได้จากการระบุความเสี่ยงในขั้นตอนที่ 2 โดยพิจารณาระดับความรุนแรงของความเสี่ยง และโอกาสที่อาจจะเกิดขึ้นก่อนมี มาตรการควบคุม (Inherent Risk)

4.4.1.1. การพิจารณาระดับความรุนแรงของความเสี่ยง (Severity of impact) ดำเนินการพิจารณาระดับความรุนแรงของความเสี่ยงในมุมมองด้านต่าง ๆ ดังนี้

(1) มุมมองด้านความพึงพอใจของลูกค้า

ความรุนแรงของผลผลกระทบจากเหตุการณ์ความเสี่ยง	ความเสียหาย	คะแนน
สูงมาก	ส่งผลต่อการส่งมอบสูงมาก ทำให้ไม่สามารถส่งมอบสินค้าให้กับลูกค้าได้เลยเนื่องจากกระบวนการเกิดการหยุดชะงัก	5
สูง	ส่งผลต่อการส่งมอบสูง ทำให้ส่งมอบสินค้าล่าช้า ลูกค้าเกิดการร้องเรียนเป็นลายลักษณ์อักษร	4
ปานกลาง	ส่งผลต่อการส่งมอบปานกลาง ทำให้ส่งมอบสินค้าล่าช้า ลูกค้าร้องเรียนทางวาจา	3
น้อย	ไม่มีข้อร้องเรียนด้านการส่งมอบจากลูกค้า แต่ไม่สะดวกต่อกระบวนการส่งมอบ เช่น มีค่าขนส่งเพิ่มขึ้น ทำให้ไม่บรรลุวัตถุประสงค์ของบริษัท	2
น้อยมาก	ไม่มีผลกระทบต่อการส่งมอบดำเนินการได้ตามแผนที่กำหนด	1

(2) มุมมองด้านชื่อเสียงของบริษัท

ความรุนแรงของผลผลกระทบจากเหตุการณ์ความเสี่ยง	ความเสียหาย	คะแนน
สูงมาก	มีการเผยแพร่ข่าวของบริษัทในสื่อต่าง ๆ รวมถึงสื่อออนไลน์ (Online) หรือหนังสือพิมพ์มากกว่า 3 สื่อ	5
สูง	มีการเผยแพร่ข่าวของบริษัทในสื่อต่าง ๆ รวมถึงสื่อออนไลน์ (Online) หรือหนังสือพิมพ์ 3 สื่อ	4
ปานกลาง	มีการเผยแพร่ข่าวของบริษัทในสื่อต่าง ๆ รวมถึงสื่อออนไลน์ (Online) หรือหนังสือพิมพ์ 2 สื่อ	3
น้อย	มีการเผยแพร่ข่าวของบริษัทในสื่อต่าง ๆ รวมถึงออนไลน์ (Online) หรือหนังสือพิมพ์ 1 สื่อ	2
น้อยมาก	ไม่มีการเผยแพร่ข่าวของบริษัท	1

(3) มุมมองด้านความต่อเนื่องในการดำเนินกิจการของบริษัท

ความรุนแรงของผลผลกระทบจากเหตุการณ์ความเสี่ยง	ความเสียหาย	คะแนน
สูงมาก	การหยุดดำเนินการของบริษัท หรือกระบวนการภายในเป็นเวลามากกว่า 1 เดือน	5
สูง	มีผลกระทบต่อกระบวนการและการดำเนินงานของบริษัทอย่างรุนแรง ประมาณ 2 – 4 สัปดาห์	4
ปานกลาง	มีการชะงักงันอย่างมีนัยสำคัญของกระบวนการและการดำเนินงานของบริษัทประมาณ 1 – 2 สัปดาห์	3
น้อย	มีผลกระทบเล็กน้อยต่อกระบวนการ และการดำเนินของบริษัทประมาณ 3 – 7 วัน	2
น้อยมาก	ไม่มีการชะงักของกระบวนการและการดำเนินงานของบริษัท	1

(4) มุมมองด้านระบบเทคโนโลยีและสารสนเทศ

ความรุนแรงของผลผลกระทบจากเหตุการณ์ความเสี่ยง	ความเสียหาย	คะแนน
สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลลูกค้า / ข้อมูลธุรกิจ	5
สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน	4
ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก	3
น้อย	เกิดเหตุเล็กน้อยที่แก้ไขได้	2
น้อยมาก	เกิดเหตุที่ไม่มีความสำคัญ	1

(5) มุมมองด้านคุณภาพของสินค้าหรือบริการ

ความรุนแรงของผลผลกระทบจากเหตุการณ์ความเสี่ยง	ความเสียหาย	คะแนน
สูงมาก	- คุณภาพของผลิตภัณฑ์หรือบริการไม่เป็นไปตามข้อกำหนดร้ายแรง หรือไม่สอดคล้องตามกฎหมาย - ทำให้บริษัทเกิดความเสียหายต่อชื่อเสียง ถูกปรับค่าเสียหาย ถูกร้องเรียนฟ้องร้อง หรือถูกสั่งปิดกิจการ	5
สูง	- คุณภาพของผลิตภัณฑ์หรือบริการไม่เป็นไปตามข้อกำหนดอย่างมาก ส่งผลทำให้ลูกค้าไม่พึงพอใจ - ทำให้เกิดข้อร้องเรียนฟ้องร้องความเสียหาย หรือถูกปรับ โดยลูกค้า	4
ปานกลาง	- คุณภาพของผลิตภัณฑ์หรือบริการไม่เป็นไปตามข้อกำหนดปานกลาง ส่งผลทำให้ลูกค้าไม่พึงพอใจ แต่สามารถยอมรับผลิตภัณฑ์และบริการบางส่วนที่ได้คุณภาพตามข้อกำหนด - กระทบกับส่วนงานถัดไปที่เกี่ยวข้องไม่พอใจ - กระบวนการถัดไปเกิดการเบี่ยงเบน เกิดความล่าช้า เกิดต้นทุนเพิ่ม (กระทบกับหน่วยงานที่เกี่ยวข้อง)	3
น้อย	- คุณภาพของผลิตภัณฑ์หรือบริการไม่เป็นไปตามข้อกำหนดเล็กน้อย ลูกค้าสามารถยอมรับได้ - กระทบกับแผนกทำให้ต้องดำเนินการแก้ไขระหว่างกระบวนการ	2
น้อยมาก	- ไม่มีผลกระทบด้านคุณภาพของผลิตภัณฑ์หรือบริการ - ไม่มีความเสียหายต่อบริษัทและผู้ที่เกี่ยวข้อง	1

4.4.1.2. การพิจารณาระดับโอกาสของความเสี่ยงที่อาจจะเกิดขึ้น

ดำเนินการพิจารณาระดับโอกาสของความเสี่ยงที่อาจจะเกิดขึ้น ในมุมมองด้านภาพลักษณ์ด้านชื่อเสียงของบริษัท(L1) และภาพลักษณ์ของกระบวนการดำเนินงานในบริษัท (L2) ตามตารางด้านล่างนี้

โอกาสของความเสี่ยงที่อาจจะเกิดขึ้น (Likelihood)			
โอกาส	**คำจำกัดความ**	**ความถี่โดยเฉลี่ย**	**คะแนน**
สูงมาก	บ่อยมาก	1 เดือนต่อครั้ง หรือมากกว่า	5
สูง	บ่อย	1-6 เดือนต่อครั้ง แต่ไม่เกิน 5 ครั้งต่อปี	4
ปานกลาง	ไม่บ่อย	1 ปีต่อครั้ง	3
ต่ำ	นานๆ ครั้ง	2-3 ปีต่อครั้ง	2
ต่ำมาก	มีโอกาสเกิด	5 ปีต่อครั้ง	1

4.4.2. ประเมินความเสี่ยงโดยวิเคราะห์หาโอกาสที่จะเกิดความเสี่ยง (Likelihood) และระดับความรุนแรงของ ผลกระทบ (Impact) ตามเกณฑ์ในการพิจารณาหาระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) และระดับ ความรุนแรงของผลกระทบ (Impact) ซึ่งสามารถพิจารณาได้ทั้งเชิงคุณภาพและเชิงปริมาณ โดยบริษัทฯกำหนดเกณฑ์ในการประเมินไว้ 5 ระดับ โดย “ระดับความเสี่ยง” เท่ากับ “ผลคูณของ ค่าเฉลี่ยโอกาสที่จะเกิดความเสี่ยง (Likelihood) กับค่าเฉลี่ยระดับความรุนแรงของผลกระทบ (Impact)” ความรุนแรงของผลกระทบ (Impact)

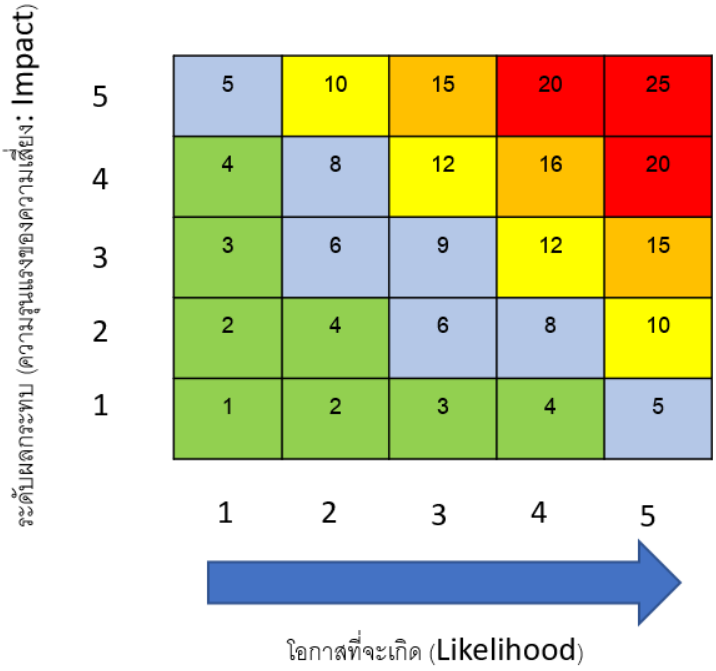
4.4.3. นำ “**ระดับความเสี่ยง**” ที่ได้ประเมินแล้วตามข้อ 4.2 มาจัดลำดับโดยระดับความสำคัญของความเสี่ยงมีทั้งหมด 5 ระดับ ดังนี้

ระดับความเสี่ยง	ระดับคะแนนความเสี่ยง	รายละเอียด	เหตุการณ์ที่ส่งผลกระทบ	ระยะเวลาในการจัดการ
ระดับ 5 Extremely Risk (E)	20-25 สูงมาก	ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที	- ความปลอดภัยของพนักงานหรือบุคคล -การกระทำที่ผิดกฎหมาย -มีผลเสียหายสำคัญต่อทรัพย์สิน -การกระทำที่กระทบต่อชื่อเสียงองค์กร -ไม่มีการควบคุมภายใน	จัดการทันทีและดำเนินการให้อยู่ในระยะเวลาที่ควบคุมได้ภายใน 1 เดือน
ระดับ 4. High Risk (H)	15-19 สูง	ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้	-การปฏิบัติงานไม่เป็นไปตามวัตถุประสงค์ -ขาดการควบคุมภายในที่ดี -มีผลเสียหายต่อทรัพย์สิน	ภายใน 1 เดือน
ระดับ 3 Moderate Risk (M)	10-14 ปานกลาง	ระดับที่พอยอมรับได้ ต้องใช้ความพยายามที่จะลดความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้	-ขาดการควบคุมภายในที่ดี หรือไม่มีประสิทธิภาพ -การจัดทำงบการเงินและรายงานทางการเงิน รายงานข้อมูลของการขาย ไม่ถูกต้องไม่เหมาะสม	ภายใน 4 เดือน
ระดับ 2 Low Risk (LR)	5-9 น้อย	ระดับที่ยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้	เหตุการณ์ที่กระทบงบการเงิน หรือการ ควบคุมภายในและมีผลกระทบต่อการปฏิบัติงานปานกลาง	ภายใน 6 เดือน
ระดับ 1 Least (L)	1-4 น้อยที่สุด	ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่ม	เหตุการณ์ที่กระทบงบการเงิน หรือการ ควบคุมภายในและมีผลกระทบต่อการ ปฏิบัติงานไม่มากนักหรือไม่เป็นสาระสำคัญ	ใช้ระบบการควบคุมภายในที่มีอยู่หรือภายใน 12 เดือน

การประเมินความเสี่ยงต้องดำเนินการทั้งก่อนการจัดทำแผนจัดการ/บริหารความเสี่ยงและหลังจากที่ได้ดำเนินการตามแผนจัดการ/บริหารความเสี่ยงแล้ว ซึ่งจะทำให้ทราบว่าแผนจัดการ/บริหารความเสี่ยงมีประสิทธิภาพและประสิทธิผลเพียงใด ควรทบทวน หรือปรับปรุงแผนจัดการ/บริหารความเสี่ยงหรือไม่

ตารางจัดลำดับความเสี่ยง (Risk Matrix) และระดับความเสี่ยงที่ยอมรับได้ คณะกรรมการบริหารความเสี่ยงกำหนดระดับความเสี่ยงที่ยอมรับได้ไว้ที่ระดับความเสี่ยงไม่เกิน 5 ระดับ

รูปที่ 4 ตารางระดับความเสี่ยงและผลกระทบ



4.5. ขั้นตอนที่ 5 การจัดทำแผนการจัดการความเสี่ยง (Risk Response)

เป็นการดำเนินการหลังจากที่องค์กรสามารถบ่งชี้ความเสี่ยงขององค์กร และประเมินความสำคัญของความเสี่ยงแล้ว โดยจะต้องนำความเสี่ยงไปดำเนินการตอบสนองด้วยวิธีการที่เหมาะสม เพื่อลดความสูญเสียหรือโอกาสที่จะเกิดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้

การจัดทำแผนการจัดการความเสี่ยง หมายถึง การกำหนดแนวทางการดำเนินการเพื่อลดโอกาสที่จะเกิดความ สูญเสีย โดยนำผลจากการประเมินความเสี่ยงที่ได้จากขั้นตอนที่ 4 มาจัดทำแผนจัดการ / บริหารความเสี่ยงตามลำดับความสำคัญของความเสี่ยง โดยหน่วยงานเจ้าของความเสี่ยง ซึ่งเข้าใจความเสี่ยงที่เกี่ยวข้องกับหน่วยงานตนเองมากที่สุด เป็นผู้จัดทำแผนจัดการ/บริหารความเสี่ยงโดยวิเคราะห์หาแนวทางการจัดการกับความเสี่ยงที่คาดว่าจะเกิดขึ้น วิธีการใดวิธีการหนึ่งหรือหลายวิธีรวมกัน เพื่อลดโอกาสที่

จะเกิดขึ้น และ/หรือลดความรุนแรงของผลกระทบให้อยู่ในระดับที่หน่วยงานยอมรับได้ และจัดทำเป็นแผนจัดการ/บริหารความเสี่ยงของหน่วยงานตนเอง

4.5.1. ให้ผู้รับผิดชอบวิเคราะห์หาวิธีการจัดการกับความเสี่ยงที่คาดว่าจะเกิดขึ้น โดยมีแนวทางในการจัดการ/บริหารความเสี่ยงได้ วิธี (AT) ดังนี้

(1) Take การยอมรับความเสี่ยง (Risk Acceptance) การยอมรับให้มีความเสี่ยงเนื่องจากค่าใช้จ่ายในการจัดการหรือ สร้างระบบควบคุมอาจมีมูลค่าสูงกว่าผลลัพธ์ที่ได้แต่ควรมีมาตรการติดตามและดูแล เช่น การกำหนดระดับของผลกระทบที่ยอมรับได้ เตรียมแผนการตั้งรับจัดการความเสี่ยง

(2) Treat การลด/การควบคุมความเสี่ยง (Risk Reduction/Control) การออกแบบระบบควบคุม การแก้ไขปรับปรุงการ ทำงานเพื่อป้องกันหรือ จำกัดผลกระทบ และโอกาสเกิดความเสียหาย เช่น ติดตั้งอุปกรณ์ความปลอดภัย ฝึกอบรมเพื่อพัฒนาทักษะวางมาตรการเชิงรุก เป็นต้น

(3) Terminate การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) การหยุดหรือเปลี่ยนแปลงกิจกรรมที่เป็นความเสี่ยง เช่น งดทำขั้นตอนที่ไม่จำเป็นและจะนำมาซึ่งความเสี่ยง ปรับเปลี่ยนรูปแบบการทำงาน ลดขอบเขตการดำเนินการ เป็นต้น

(4) Transfer การกระจาย/โอนความเสี่ยง (Risk sharing/spreading) การกระจายทรัพย์สินหรือกระบวนการต่าง ๆ เพื่อลดความเสี่ยงจากการสูญเสีย เช่นการประกันทรัพย์สินเพื่อโอนความเสี่ยงไปยังบริษัทประกัน การจ้างบริษัทภายนอกให้ทำงาน บางส่วนแทนการทำสำเนาเอกสารหลาย ๆ ชุด การกระจายที่เก็บทรัพย์สินมีค่า เป็นต้น

ทั้งนี้การเลือกวิธีการจัดการความเสี่ยง ต้องพิจารณาเปรียบเทียบต้นทุนในการจัดการ/บริหารความเสี่ยงและความ เสียหายที่เกิดขึ้นด้วย

4.5.2. ให้ผู้รับผิดชอบร่วมกันจัดทำแผนงานเพื่อจัดการความเสี่ยง กรณีที่ผลการประเมินความเสี่ยงแล้วอยู่ในระดับความเสี่ยง “สูง” ถึง “สูงมาก” โดยมีขั้นตอน ดังนี้

(1) ระบุวิธีการ มาตรการที่เป็นทางเลือกจากวิธีการจัดการความเสี่ยง (4T) เพื่อให้ความเสี่ยงคงเหลืออยู่ในระดับที่ยอมรับได้ และสอดคล้องกับวัตถุประสงค์ที่กำหนดไว้

(2) ศึกษาเปรียบเทียบความเป็นไปได้และค่าใช้จ่ายของแต่ละทางเลือกตาม ข้อ (1) โดยคำนึงถึงความคุ้มค่าในการลงทุนทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน โดยต้นทุนในการดำเนินการต้องไม่สูงกว่าความเสียหายที่คาดว่าจะเกิดขึ้น

(3) เลือกวิธีการที่ดีที่สุดโดยกำหนดผู้รับผิดชอบ/ระยะเวลา/งบประมาณ กำหนดแผนปฏิบัติการ

4.6. ขั้นตอนที่ 6 การจัดทำกิจกรรมการควบคุม (Control Activities)

กิจกรรมการควบคุม หมายถึง นโยบายและแนวทางการปฏิบัติงานในการควบคุมที่ฝ่ายบริหารกำหนดขึ้น เพื่อมั่นใจว่าแผนจัดการหรือแผนบริหารความเสี่ยงที่กำหนดขึ้นอย่างมีประสิทธิภาพมีการกำหนดผู้รับผิดชอบและระยะเวลาในการดำเนินงานไว้อย่างชัดเจน และกิจกรรมการควบคุมนั้นเป็นวิธีการหนึ่งในการจัดการหรือบริหารความเสี่ยง

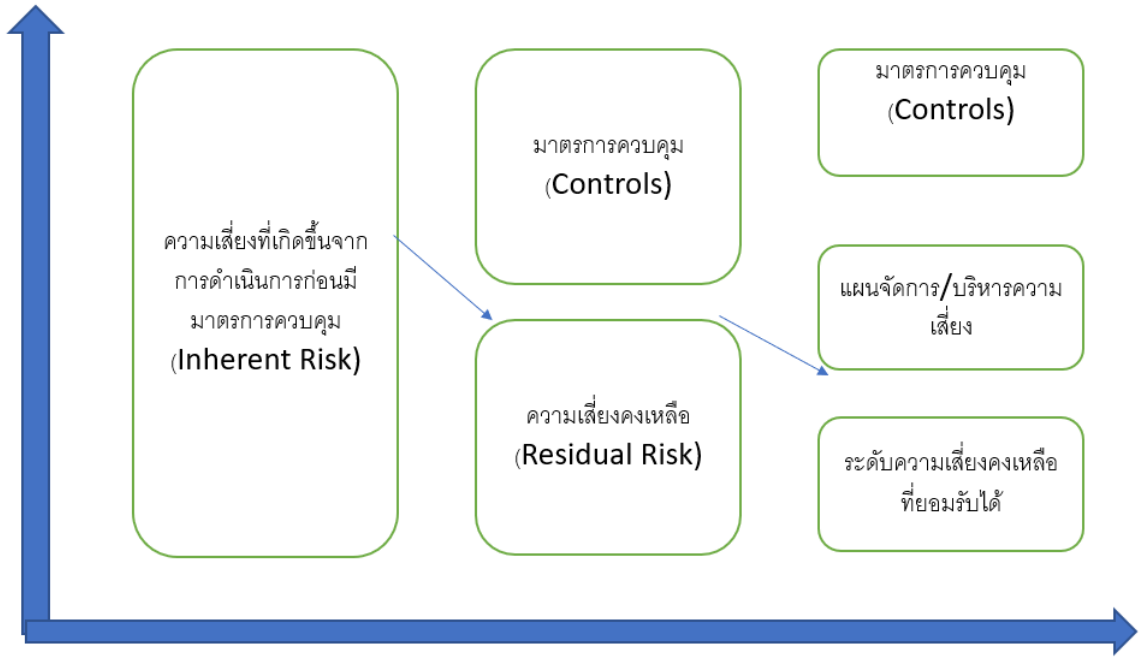
ดังนั้น การทำกิจกรรมการควบคุม (Control Activities) คือ การกำหนดกิจกรรมและการปฏิบัติต่างๆ ที่กระทำเพื่อลด ความเสี่ยง และทำให้การดำเนินงานบรรลุตามวัตถุประสงค์และเป้าหมายขององค์กร เช่น การกำหนดกระบวนการปฏิบัติงานที่เกี่ยวข้องกับการจัดการความเสี่ยงให้กับบุคลากรภายในองค์กร เพื่อเป็นการสร้างความมั่นใจว่าจะสามารถจัดการกับความเสี่ยงนั้นได้อย่างถูกต้องและเป็นไปตามเป้าหมายที่กำหนด

กิจกรรมการควบคุมที่จะเกิดประโยชน์มากที่สุดควรจะแทรกอยู่ในกระบวนการสามารถป้องกันและลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยต้นทุนในการดำเนินงานการต้องไม่สูงกว่าความเสียหายที่คาดว่าจะเกิดขึ้น

การกำหนดกิจกรรมการควบคุมอย่างชัดเจนจะทำให้แผนการจัดการบริหารความเสี่ยงเพิ่มเติมที่ได้จัดทำไว้บรรลุ วัตถุประสงค์โดยจัดทำนโยบายและวิธีปฏิบัติเพิ่มเติม กำหนดผู้รับผิดชอบและระยะเวลาแล้วเสร็จอย่างชัดเจน ในบางกรณีอาจ จัดทำกระบวนการควบคุมภายในเพิ่มเติมกำหนดผู้รับผิดชอบและระยะเวลาแล้วเสร็จอย่างชัดเจน เช่น การสอบทาน การกำกับดูแล การแบ่งแยกหน้าที่งานเพิ่ม เป็นต้น

กิจกรรมการควบคุม เป็นองค์ประกอบหนึ่งของระบบการควบคุมภายใน ในลักษณะการเสนอแนะ (Suggestive Control) เพื่อปรับปรุงและพัฒนาระบบการดำเนินงานและระบบการควบคุมภายในให้เหมาะสมกับสถานการณ์ที่หน่วยงานต้องจัดทำให้มีขึ้นเพื่อลดความเสี่ยง และทำให้เกิดความคุ้มค่าตลอดจนให้ฝ่ายบริหารเกิดความมั่นใจในประสิทธิผลของระบบการควบคุมภายในที่มีอยู่

รูปที่ 5 การลดลงของความเสี่ยงจากผลของการควบคุม



4.7. ขั้นตอนที่ 7 การจัดทำสารสนเทศและการสื่อสาร (Information and Communication)

องค์กรจะต้องมีระบบสารสนเทศและการติดต่อสื่อสารที่มีประสิทธิภาพ เพราะเป็นพื้นฐานสำคัญที่จะนำไปพิจารณา ดำเนินการบริหารความเสี่ยงให้เป็นไปตามกรอบ และขั้นตอนการปฏิบัติที่องค์กรกำหนด ซึ่งเป็นการแสดงรายงานการบริหารจัดการความเสี่ยงของทั้งระดับหน่วยงาน และระดับองค์กร จากข้อมูลที่ระบบได้รับตั้งแต่ขั้นตอน ที่ 1 ถึง 6 ซึ่งรายงานจะแบ่งออกได้เป็น 2 ส่วนหลัก คือ รายงานการควบคุมภายใน และรายงานการจัดการความเสี่ยง สรุปความเสี่ยงและการจัดการในระดับของหน่วยงาน รายงานแผนบริหารความเสี่ยงของหน่วยงานย่อย)

นอกจากนี้ บริษัทควรจัดให้มีระบบสารสนเทศและการสื่อสารที่ดี เพื่อเป็นเครื่องมือในการบริหารความเสี่ยงให้บรรลุตามวัตถุประสงค์ที่ตั้งไว้โดย

(1) ต้องมีการสื่อสารที่ชัดเจนจากคณะกรรมการบริษัทฯ และผู้บริหารระดับสูงเกี่ยวกับนโยบายการบริหารความเสี่ยง และให้พนักงานทุกคนได้เข้าใจบทบาทหน้าที่ของตนในการบริหารความเสี่ยง เพื่อปรับเปลี่ยนพฤติกรรมและ/กิจกรรมที่ต้องดำเนินการโดยคาดหวังให้ความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้

(2) ต้องมีการระบุแหล่งที่มาและรวบรวมสารสนเทศทั้งจากภายในและภายนอกองค์กร จัดเก็บและสื่อสารในรูปแบบที่กำหนด และภายในระยะเวลาที่กำหนดเพื่อให้ผู้บริหารและพนักงานสามารถรับรู้ทันต่อเหตุการณ์ ปฏิบัติหน้าที่ติดต่อสื่อสารทางด้านการบริหารความเสี่ยงอย่างสม่ำเสมอและมีประสิทธิภาพ

4.8. ขั้นตอนที่ 8 การติดตามและประเมินผล (Monitoring & Evaluation)

องค์กรจะต้องมีการติดตามผล เพื่อให้ทราบถึงผลการดำเนินการว่ามีความเหมาะสมและสามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพหรือไม่

การติดตามและประเมินผล หมายถึง กระบวนการควบคุมคุณภาพการปฏิบัติงานและประเมินผลแผนการจัดการ/บริหารความเสี่ยงเพิ่มเติม หรือกิจกรรมการควบคุมที่วางไว้อย่างต่อเนื่องและสม่ำเสมอ โดยผู้รับผิดชอบดำเนินการติดตามในระหว่างการปฏิบัติงาน และประเมินผลเป็นครั้งคราวตามความเหมาะสม เพื่อให้มั่นใจว่าการจัดการ/ การบริหารความเสี่ยงมีประสิทธิภาพและประสิทธิผล

หลังการติดตามและประเมินผลแล้ว ต้องรายงานความก้าวหน้า ปัญหา อุปสรรคของการจัดการ/บริหารความเสี่ยงให้คณะกรรมการบริหารความเสี่ยงทราบ เพื่อใช้เป็นแนวทางในการทบทวน หรือปรับปรุงแผนการจัดการ/บริหารความเสี่ยงต่อไป

ทั้งนี้ รายงานที่คณะกรรมการบริหารความเสี่ยงต้องจัดทำ มีเนื้อหา ดังนี้

(1) การสรุปปัจจัยความเสี่ยง ระดับความเสี่ยง

(2) การควบคุมที่มีอยู่ และแนวทางการจัดการความเสี่ยงที่เหลือ

(3) หน่วยงาน/ผู้รับผิดชอบ ผลของระดับความเสี่ยงหลังการควบคุม

(4) ความเสี่ยงที่คลาดเคลื่อนเกินกว่าที่ยอมรับได้

(5) ความเสี่ยงสูงสุด 5 ระดับ

(6) เหตุการณ์ที่แม้จะมีโอกาสต่ำ แต่จะมีผลต่อ

- ความปลอดภัยต่อพนักงาน หรือบุคคลอื่นการกระทำผิดกฎหมาย
- ผลเสียหายสำคัญต่อทรัพย์สิน การด้อยค่าของทรัพย์สิน
- ชื่อเสียงของหน่วยงาน
- การจัดทำงบและรายงานทางการเงินไม่เหมาะสม

(7) รายงานต่อผู้บริหารระดับสูง หรือคณะกรรมการบริษัท