นโยบายการบริหารความเสี่ยง

บริษัท ไมโครไฟเบอร์อุตสาหกรรม จำกัด

ประวัติการแก้ไข

ฉบับที่	รายละเอียด	วันที่แก้ไข	วันที่มีผลบังคับใช้
001	**นโยบายการบริหารความเสี่ยง**	แก้ไขครั้งที่ 1 วันที่ 20 ธันวาคม 2565	วันที่ 24 มกราคม 2566
	1. **การจัดประเภทความเสี่ยง เพิ่มเติม**: **ความเสี่ยงด้านการเงิน** (Financial Risk : F) หมายถึง ความเสี่ยงเกี่ยวกับสภาพคล่องทางการเงิน การบริหารทางการเงินและงบการเงิน เช่น ความเสี่ยงจากการจัดสรรงบประมาณไม่เหมาะสม ตั้งงบประมาณผิดพลาด และใช้งบประมาณเกิน รวมทั้งความเสี่ยงจากความผันผวนของปัจจัยทางการตลาด (Market Risk) และ ความเสี่ยงจากการที่คู่สัญญาไม่ปฏิบัติตามภาระผูกพัน (Credit Risk) **ความเสี่ยงที่จะเกิดใหม่** (Emerging Risk: E) ความเสี่ยงที่จะเกิดใหม่เป็นความสูญเสียที่เกิดขึ้นจากความเสี่ยงที่ยังไม่ได้ปรากฏขึ้นในปัจจุบันแต่อาจจะเกิดขึ้นได้ในอนาคตเนื่องจากสภาวะแวดล้อมที่เปลี่ยนไป ความเสี่ยงประเภทนี้เป็นความเสี่ยงที่เกิดขึ้นอย่างช้า ๆ ยากที่จะระบุได้ มีความถี่ของการเกิดต่ำ เมื่อเกิดขึ้นแล้วจะส่งผลกระทบอย่างรุนแรง ความเสี่ยงที่จะเกิดใหม่นี้มักจะถูกระบุขึ้นมาจากการคาดการณ์บนพื้นฐานของการศึกษาจากหลักฐานที่มีปรากฏอยู่ ความเสี่ยงที่จะเกิดใหม่นี้มักจะเป็นผลมาจากการเปลี่ยนแปลงทางการเมือง กฎหมาย สังคม เทคโนโลยี สภาพแวดล้อมทางกายภาพ หรือการเปลี่ยนแปลงตามธรรมชาติ **ความเสี่ยงที่จะเกิดการทุจริต**(Fraud Risk: Fr) เป็นความเสี่ยงที่เกิดจากจากการดำเนินงานที่อาจก่อให้เกิดการทุจริต การขัดกันระหว่างผลประโยชน์ส่วนตนกับผลประโยชน์ส่วนรวม หรือการรับสินบนบนความเสี่ยงประเภทนี้อาจกระทบต่อชื่อเสียงภาพลักษณ์ของกิจการและอื่นๆ เป็นต้น **ความเสี่ยงในการดำเนินงานอย่างยั่งยืน**(Environmental, Social and Governance : ESG) เป็นความเสี่ยงที่เกี่ยวข้องกับประเด็นด้านสิ่งแวดล้อม สังคมและบรรษัทภิบาลความเสี่ยงประเภทนี้อาจกระทบต่อชื่อเสียงภาพลักษณ์ของกิจการและอื่นๆเป็นต้น **ความเสี่ยงด้านข้อมูลส่วนบุคคล** (Privacy : P) เป็นความเสี่ยงที่มุ่งเรื่องการปฏิบัติการในการประมวลผลข้อมูล เริ่มตั้งแต่กระบวนการเก็บ การเก็บรักษา การใช้ การส่งต่อหรือเปิดเผยและการลบและทำลายที่อาจทำให้สูญหาย รั่วไหลหรือละเมิดข้อมูลส่วนบุคคลซึ่งกระทบต่อสิทธิและเสรีภาพของส่วนบุคคล		

ฉบับที่	รายละเอียด	วันที่แก้ไข	วันที่มีผลบังคับใช้
	2. **แก้ไข**: 3 ระดับ ดังนี้ ระดับ 1. H: High Risk ความเสี่ยงสูงระดับที่มีนัยสำคัญ โดยผู้บริหารจำเป็นต้องเร่งจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ทันที (ระดับคะแนน 15-25 คะแนน) ระดับ 2. M: Moderate Risk ความเสี่ยงระดับปานกลาง โดยต้องมีการจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป หรือการติดตามอย่างเหมาะสม เพื่อป้องกันไม่ให้ความเสี่ยงดังกล่าวเกิดขึ้น (ระดับ 5-12 คะแนน) ระดับ 3. L: Low Risk ความเสี่ยงระดับต่ำ โดยต้องมีการควบคุมเพื่อป้องกัน หรือการติดตามอย่างเหมาะสม เพื่อไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ (ระดับคะแนน 1-4 คะแนน)		
	3. **แก้ไข**: 4.1 วิเคราะห์หาวิธีการจัดการกับความเสี่ยงที่คาดว่าจะเกิดขึ้น โดยมีแนวทางในการจัดการ / บริหารความเสี่ยงได้ 4 วิธี ดังนี้ 4.1.1 การควบคุม/ลด (Reduce) คือ การควบคุมความเสี่ยงหรือหาวิธีการบริหารความเสี่ยง เช่น ใช้เทคนิควิชาการทางวิศวกรรมหรือการจัดทำแผนฉุกเฉิน หรือการปรับปรุงแก้ไขกระบวนการดำเนินงาน เป็นต้น 4.1.2 การโอนย้าย (Transfer) คือ การถ่ายโอนความเสี่ยงหรือโอนย้ายความเสี่ยงให้ผู้อื่นรับผิดชอบ เช่นการทำประกันภัยหรือจ้างบุคคลภายนอกเป็นผู้ดำเนินการแทน เป็นต้น 4.1.3 การหลีกเลี่ยง (Avoid) คือ การกำจัดความเสี่ยงหรือหลีกเลี่ยงไม่ยอมรับความเสี่ยงนั้นเลย เช่น การเปลี่ยนวัตถุประสงค์หรือหยุดทำกิจกรรม เป็นต้น 4.1.4 การยอมรับ (Accept) ความเสี่ยงที่เหลือในปัจจุบันอยู่ในระดับที่ยอมรับได้ โดยไม่ต้องดำเนินการใด ๆ เพื่อลดโอกาสหรือผลกระทบที่อาจเกิดขึ้นอีก มักใช้กับความเสี่ยงที่ต้นทุนของมาตรการจัดการสูงไม่คุ้มกับประโยชน์ที่ได้รับ		
	4. **เพิ่มเติม**: บริษัทกำหนดให้ทั่วทั้งองค์กรทั้งระดับองค์กรและฝ่ายร่วมมือในการจัดการประเมินความเสี่ยง พร้อมทั้งรายงานการประเมินความเสี่ยง และกำหนดกระบวนการติดตามและประเมินผลการ		

ฉบับที่	รายละเอียด	วันที่แก้ไข	วันที่มีผลบังคับใช้
	ดำเนินงานตาม แผนการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อรายงานต่อคณะกรรมการตรวจสอบ/คณะกรรมการบริษัท		
	5. **เพิ่มเติม**: บริษัทจะกำหนดให้มีการสอบทานและทบทวนนโยบายการบริหารความเสี่ยงเป็นประจำอย่างน้อยปีละ 1 ครั้งเพื่อให้สอดคล้องกับการปฏิบัติงานปัจจุบัน		

บริษัท ไมโครไฟเบอร์อุตสาหกรรม จำกัด

นโยบาย

ที่ PL - MI - 010

เรื่อง การบริหารความเสี่ยง

1. **วัตถุประสงค์**

บริษัท ไมโครไฟเบอร์อุตสาหกรรม จำกัด (“**บริษัท**”) ได้กำหนดนโยบายการบริหารความเสี่ยงทั่วทั้งองค์กร โดยจัดตั้งคณะทำงานบริหารความเสี่ยงภายใต้คณะกรรมการบริหาร เพื่อทำหน้าที่ในการจัดทำแผนการจัดการความเสี่ยง ซึ่งรวมถึงการประเมินความเสี่ยงต่าง ๆ ทั้งที่เกิดจากปัจจัยภายนอกและจากการบริหารงาน และการปฏิบัติงานภายในองค์กร รวมทั้งกำหนดแนวทางในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ มีการสื่อสาร จัดฝึกอบรมสัมมนาเชิงปฏิบัติการแก่พนักงาน ให้ตระหนักถึงความสำคัญของการบริหารความเสี่ยง

2. **ความหมายของการบริหารความเสี่ยง**

ความเสี่ยง คือ เหตุการณ์การกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย หรือความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จของเป้าหมาย และวัตถุประสงค์ของบริษัททั้งในระดับองค์กรระดับหน่วยงาน และระดับบุคคลได้

การบริหารความเสี่ยง คือ กระบวนการดำเนินการเกี่ยวกับความเสี่ยง ในการดำเนินงานของบริษัทตามเป้าหมายที่ได้วางไว้ โดยจัดให้มีระบบ และแบบแผนในการปฏิบัติงานด้านความเสี่ยงเพื่อการจัดการความเสี่ยงที่ส่งผลกระทบต่อบริษัทให้ระดับ และขนาดของผลกระทบที่จะเกิดขึ้นอยู่ในระดับที่สามารถยอมรับได้ รวมทั้งมีการประเมินควบคุมและการตรวจสอบได้อย่างมีระบบโดยคำนึงถึงการบรรลุเป้าหมายของบริษัทเป็นสำคัญ

3. **โครงสร้างการบริหารความเสี่ยงของบริษัท**

โครงสร้างการบริหารความเสี่ยง ประกอบด้วย คณะกรรมการบริหาร และคณะทำงานบริหารความเสี่ยงในทุกระดับ

ระดับองค์กร ได้แก่ คณะกรรมการบริหาร ภายใต้นโยบายและการกำกับดูแลของคณะกรรมการบริษัทมีประธานคณะกรรมการบริหารเป็นประธาน มีหน้าที่และความรับผิดชอบเป็นไปตามแนวทางปฏิบัติของบริษัท รวมทั้งมีการสอบทานระบบควบคุมภายในโดยคณะกรรมการตรวจสอบ

ระดับฝ่าย ได้แก่ ผู้จัดการฝ่าย และพนักงานภายในบริษัททุกคน (เรียกว่า คณะทำงานบริหารความเสี่ยง) ภายใต้การกำกับดูแลของคณะกรรมการบริหาร

4. **บทบาท หน้าที่และความรับผิดชอบในการบริหารความเสี่ยง**

การบริหารความเสี่ยง ถือเป็นหน้าที่ของบุคลากรบริษัททุกระดับทุกคน รวมทั้งผู้ทำหน้าที่ที่ปรึกษา ผู้กระทำการแทน หรือ ผู้ได้รับมอบหมายให้กระทำหน้าที่ในนามบริษัท โดยมีบทบาทหน้าที่ความรับผิดชอบ ดังนี้

4.1 คณะกรรมการบริหาร

4.1.1 พิจารณาให้ความเห็นต่อนโยบายการบริหารความเสี่ยง กลยุทธ์การบริหารความเสี่ยง และกรอบการบริหาร ความเสี่ยงองค์กร ที่สอดคล้องกับวัตถุประสงค์ เป้าหมายหลัก แผนธุรกิจของบริษัท และความเสี่ยงที่ยอมรับได้ของกิจการ ในเรื่องของการบริหารความเสี่ยงโดยรวม และครอบคลุมถึงความเสี่ยงหลัก เช่น ความเสี่ยงด้านธุรกิจ ความเสี่ยงด้านการตลาด ความเสี่ยงด้านสภาพคล่อง ความเสี่ยงด้านปฏิบัติการ และความเสี่ยงที่มีผลกระทบต่อชื่อเสียงของกิจการ เป็นต้น ก่อนนำเสนอต่อคณะกรรมการบริษัทเพื่อพิจารณาอนุมัติ

4.1.2 วางกลยุทธ์ให้สอดคล้องกับนโยบายการบริหารความเสี่ยง โดยสามารถประเมิน ติดตาม และดูแลระดับความเสี่ยงขององค์กรให้อยู่ในระดับที่เหมาะสม สอดคล้องกับกลยุทธ์และเป้าหมายทางธุรกิจ รวมถึงสถานการณ์ที่เปลี่ยนแปลงไป รวมถึงการพิจารณากำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ของบริษัท (Risk Tolerance) ก่อนนำเสนอต่อคณะกรรมการบริษัทเพื่อพิจารณาอนุมัติ

4.1.3 ประเมินกระทบและโอกาสที่เกิดขึ้นของความเสี่ยงที่ได้ระบุไว้เพื่อจัดลำดับความเสี่ยง และมีวิธีจัดการความเสี่ยงที่เหมาะสม ก่อนนำเสนอต่อคณะกรรมการบริษัทเพื่อพิจารณาอนุมัติ

4.1.4 ดูแลและสนับสนุนให้มีการสอบทาน ทบทวนนโยบายและกรอบการบริหารความเสี่ยง ของบริษัท เป็นประจำอย่างน้อยปีละ 1 ครั้งเพื่อให้แน่ใจว่านโยบายและกรอบการบริหารความเสี่ยงดังกล่าวยังคงสอดคล้อง และเหมาะสมกับสภาพการดำเนินธุรกิจในภาพรวม และกิจกรรมการบริหารความเสี่ยงของบริษัท

4.1.5 มีอำนาจในการเรียกบุคคลที่เกี่ยวข้องมาชี้แจง หรือแต่งตั้งและกำหนดบทบาทที่ให้ผู้ปฏิบัติงานทุกระดับมีหน้าที่บริหารความเสี่ยงตามความเหมาะสม และให้รายงานต่อคณะกรรมการบริหารเพื่อให้การบริหารความเสี่ยงบรรลุวัตถุประสงค์

4.1.6 รายงานความเสี่ยงที่สำคัญของบริษัท รวมถึงสถานะของความเสี่ยง แนวทางในการจัดการความเสี่ยง ความคืบหน้า และผลของการบริหารความเสี่ยงให้แก่คณะกรรมการบริษัทเพื่อรับทราบเป็นประจำ และในกรณีที่มีปัจจัยหรือเหตุการณ์สำคัญ ซึ่งอาจมีผลกระทบต่อบริษัทอย่างมีนัยสำคัญต้องรายงานต่อคณะกรรมการบริษัท เพื่อทราบและพิจารณาโดยเร็วที่สุด

4.1.7 มีอำนาจในการแต่งตั้งคณะทำงานบริหารความเสี่ยงตามความจำเป็น โดยสนับสนุนคณะทำงานบริหารความเสี่ยงในด้านบุคลากร งบประมาณ และทรัพยากรอื่นที่จำเป็น ให้สอดคล้องกับขอบเขตความรับผิดชอบ

4.1.8 ให้คำแนะนำ และการสนับสนุนแก่คณะกรรมการบริษัท และคณะทำงานบริหารความเสี่ยง ในเรื่องการบริหารความเสี่ยงระดับองค์กร รวมถึงส่งเสริมและสนับสนุนให้มีการปรับปรุง และพัฒนาระบบการบริหารความเสี่ยงภายในบริษัทอย่างต่อเนื่องและสม่ำเสมอ

4.1.9 ขอความเห็นทางวิชาชีพจากบุคคลหรือองค์กรภายนอก เพื่อให้คำปรึกษาหรือคำแนะนำที่เป็นอิสระเกี่ยวกับการบริหารจัดการความเสี่ยงให้แก่คณะกรรมการบริหารและผู้เกี่ยวข้อง รวมทั้งการว่าจ้างบุคคลภายนอกเฉพาะคราว เพื่อช่วยให้การปฏิบัติงานของคณะทำงานบริหารความเสี่ยงเพื่อให้สามารถปฏิบัติหน้าที่ให้บรรลุวัตถุประสงค์ภายในระยะเวลาที่กำหนด

4.1.10 ระบุความเสี่ยง โดยพิจารณาจากปัจจัยทั้งภายนอกและภายในบริษัทที่อาจส่งผลให้บริษัทไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ ก่อนนำเสนอต่อคณะกรรมการบริษัทเพื่อพิจารณาอนุมัติ

4.1.11 สื่อสารแลกเปลี่ยนข้อมูล และประสานงานเกี่ยวกับความเสี่ยง และการควบคุมภายในกับคณะกรรมการตรวจสอบ อย่างน้อยปีละ 1 ครั้ง

4.1.12 ประเมินผลกระทบ และโอกาสที่เกิดขึ้นของความเสี่ยงที่ได้ระบุไว้เพื่อจัดลำดับความเสี่ยง และมีวิธีจัดการความเสี่ยงที่เหมาะสมก่อนนำเสนอต่อคณะกรรมการบริษัทเพื่อพิจารณาอนุมัติ

4.1.13 ทบทวนความเพียงพอของนโยบาย และระบบการบริหารความเสี่ยง โดยรวมถึงความมีประสิทธิผลของระบบ และการปฏิบัติตามนโยบายที่กำหนด

4.1.14 พิจารณารายงานผลการประเมินโอกาสที่จะเกิดการทุจริตขึ้น รวมถึงผลกระทบโดยครอบคลุมการทุจริตแบบต่าง ๆ เช่น การจัดทำรายงานทางการเงินเท็จ การทำให้สูญเสียทรัพย์สิน การคอร์รัปชั่น การที่ผู้บริหารสามารถฝ่าฝืนระบบควบคุมภายใน (management override of internal controls) การเปลี่ยนแปลงข้อมูลในรายงานที่สำคัญ การได้มาหรือใช้ไปซึ่งทรัพย์สินโดยไม่ถูกต้อง เป็นต้น

4.1.15 ปฏิบัติหน้าที่อื่นใดตามที่คณะกรรมการบริษัทมอบหมาย

4.2 คณะทำงานบริหารความเสี่ยง

คณะทำงานบริหารความเสี่ยง ได้แก่ ผู้จัดการฝ่ายและพนักงานในบริษัททุกคนจะเป็นผู้รับแนวทางการจัดการความเสี่ยงไปจัดทำแผนรองรับความเสี่ยงที่เกี่ยวข้อง ดำเนินการและรายงานผลการดำเนินการตามแผนให้เลขานุการคณะกรรมการบริหารตามกำหนดเวลา ภายใต้การกำกับดูแลของคณะกรรมการบริหาร ซึ่งแต่ละฝ่ายจะต้องดำเนินการดังต่อไปนี้ระบุความเสี่ยงด้านต่าง ๆ พร้อมทั้งวิเคราะห์ และประเมินความเสี่ยงที่อาจเกิดขึ้น รวมทั้งแนวโน้มผลกระทบต่อบริษัท

4.2.1 จัดทำแผนการบริหารความเสี่ยงในสายงานที่รับผิดชอบ เพื่อให้มีการนำระบบการบริหารความเสี่ยงมาเป็นส่วนหนึ่งของกระบวนการทำงาน รวมทั้งสื่อสารและถ่ายทอดให้ผู้ปฏิบัติงานในสาย

งานรับทราบ และถือปฏิบัติโดยถูกต้องเพื่อให้มั่นใจว่าการปฏิบัติมีการประเมิน จัดการ และรายงานความเสี่ยงอย่างเพียงพอ

4.2.2 ศึกษา ทบทวน และประเมินความเสี่ยงที่อาจเกิดขึ้น รวมถึงแนวโน้มของผลกระทบที่อาจมีต่อองค์กร ทั้งความเสี่ยงจากภายนอกและภายในองค์กร

4.2.3 กำหนดนโยบายบริหารความเสี่ยง แนวทาง และกระบวนการบริหารความเสี่ยงเสนอต่อคณะกรรมการบริหาร เพื่อพิจารณาในเรื่องการบริหารความเสี่ยงโดยรวม

4.2.4 กำหนดกลยุทธ์ และทรัพยากรที่ใช้ในการบริหารความเสี่ยงของบริษัท ให้สอดคล้องกับนโยบายการบริหารความเสี่ยงตลอดจนกลยุทธ์และทิศทางธุรกิจของบริษัท

4.2.5 รายงานผลการดำเนินการในการบริหารความเสี่ยง และจัดการความเสี่ยง รวมถึงสถานะความเสี่ยงในแต่ละหัวข้อที่กำหนดไว้ต่อคณะกรรมการบริหาร เพื่อพิจารณาทุกไตรมาส

4.2.6 ปฏิบัติงานอื่น ๆ ตามที่คณะกรรมการบริหารมอบหมาย

4.3 คณะกรรมการตรวจสอบ (Audit Committee)

คณะกรรมการตรวจสอบ (Audit Committee) มีบทบาทหน้าที่ในการพิจารณาความเสี่ยงที่สำคัญของบริษัท พร้อมเสนอแนะวิธีป้องกันหรือแจ้งให้คณะกรรมการบริษัททราบ เพื่อหามาตรการป้องกันเพื่อลดความเสี่ยงนั้น รวมถึงสอบทานความเพียงพอและความมีประสิทธิภาพในการบริหารความเสี่ยงของบริษัท

4.4 ผู้ตรวจสอบภายใน

4.4.1 สอบทานและประเมินประสิทธิผลของกระบวนการบริหารความเสี่ยง

4.4.2 สื่อสารทำความเข้าใจกับผู้บริหารและผู้รับการตรวจสอบเกี่ยวกับความเสี่ยง เพื่อวางแผนการตรวจสอบที่เน้นตามความเสี่ยง (Risk Based Auditing)

4.4.3 ให้ความมั่นใจว่า บริษัทมีการควบคุมภายในที่เพียงพอและเหมาะสมต่อการจัดการความเสี่ยงและการควบคุมนั้นได้มีการปฏิบัติตามอย่างมีประสิทธิผล

5. วัตถุประสงค์และขอบเขตการบริหารความเสี่ยง

5.1 วัตถุประสงค์ของการบริหารความเสี่ยง

เพื่อจัดการปัญหาอุปสรรคในการทำงาน ป้องกัน หรือลดโอกาสที่จะเกิดเหตุการณ์ไม่พึงประสงค์ และผลกระทบที่อาจเกิดขึ้น ซึ่งจะทำให้การดำเนินงานไม่บรรลุวัตถุประสงค์และเป้าหมายขององค์กร นอกจากนี้ยังเป็นการส่งเสริมให้มีการกำกับดูแลกิจการที่ดี

5.2 ขอบเขตการบริหารความเสี่ยง

เพื่อให้การดำเนินงานมีความต่อเนื่อง และบรรลุตามวัตถุประสงค์ของบริษัท ดังนั้น ทุกหน่วยงานภายในบริษัทจะต้องมีการบริหารความเสี่ยงเป็นไปตามนโยบายและระเบียบของบริษัท โดยให้การบริหารความเสี่ยงเป็นกระบวนการหนึ่งในการปฏิบัติงานประจำวันของพนักงานทุกคน โดยมีจุดมุ่งหมายให้การบริหารความเสี่ยงถูกปลูกฝังเป็นส่วนหนึ่งของวัฒนธรรมองค์กร

5.3 ปัจจัยที่ผลักดันให้มีการบริหารความเสี่ยง

5.3.1 ข้อกำหนดของหน่วยงานที่กำกับดูแลบริษัท

5.3.2 สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย

5.3.3 ทัศนคติของผู้บริหาร

5.4 นโยบายการบริหารความเสี่ยง

ทุกหน่วยงานภายในบริษัท ต้องจัดให้มีการบริหารความเสี่ยงอย่างเป็นระบบ และต่อเนื่องภายใต้กระบวนการบริหารความเสี่ยงที่เป็นมาตรฐานเดียวกัน โดยการนำเทคโนโลยีสารสนเทศมาใช้เพื่อให้เกิดความรวดเร็วในการสื่อสาร และประมวลผลตลอดจนต้องมีการติดตามและประเมินผลพร้อมปรับแผนการบริหารความเสี่ยงเป็นระยะ ๆ อย่างสม่ำเสมอเพื่อให้การดำเนินการบรรลุวัตถุประสงค์

6. ประโยชน์ของการบริหารความเสี่ยง

เมื่อบริษัทมีการบริหารความเสี่ยงที่ดี และเหมาะสมแล้วบริษัทจะได้ประโยชน์โดยตรงจากการบริหารความเสี่ยงดังนี้

6.1 ผลการดำเนินงานของบริษัทสามารถเป็นไปตามเป้าหมาย และวัตถุประสงค์ของบริษัทที่ได้ตั้งไว้

6.2 ส่งเสริมให้เกิดความเจริญเติบโตทางธุรกิจอย่างต่อเนื่อง และยั่งยืนเพื่อสร้างมูลค่าเพิ่มให้กับบริษัท และผู้มีส่วนได้ส่วนเสีย

6.3 ส่งเสริมให้เกิดการกำกับดูแลกิจการที่ดี

6.4 ส่งเสริมให้กรรมการ ผู้บริหาร และพนักงานเกิดความรู้ความเข้าใจและตระหนักถึงความสำคัญของการบริหารความเสี่ยงซึ่งจะส่งผลต่อเนื่องให้เกิดความระมัดระวังในการทำงาน และลดโอกาสที่จะทำให้เกิดการสูญเสียจากการดำเนินงาน

6.5 ในการจัดทำแผนงานโครงการต่าง ๆ บริษัทสามารถนำผลของการวิเคราะห์ความเสี่ยงที่เกิดขึ้นมาใช้เป็นส่วนหนึ่งเพื่อประกอบการตัดสินใจที่จะทำ หรือไม่ทำโครงการใด ๆ ที่จะส่งผลกระทบต่อบริษัทได้

6.6 ช่วยให้การกำหนดวัตถุประสงค์และกลยุทธ์ต่าง ๆ ของบริษัทให้มีความสมบูรณ์ และความเป็นไปได้มากขึ้น และสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้

6.7 ส่งเสริมให้เกิดการเตรียมความพร้อม และแนวทางแก้ไขปัญหาต่าง ๆ ที่อาจจะเกิดขึ้น และส่งผลกระทบกับผลการดำเนินงานของบริษัท

6.8 มีระบบเทคโนโลยี และสารสนเทศที่ช่วยในการจัดเก็บข้อมูล การคำนวณต่าง ๆ การรายงาน และสอบทานข้อมูลได้อย่างถูกต้องครบถ้วนสมบูรณ์รวดเร็ว

6.9 ผู้บริหารมีข้อมูลเพื่อใช้ประกอบในการตัดสินใจได้อย่างถูกต้อง และรวดเร็วยิ่งขึ้น

6.10มีการจัดสรรทรัพยากรอย่างเหมาะสมโดยคำนึงถึงความคุ้มค่าในการลงทุน

6.11เกิดการมีส่วนร่วมของพนักงานในบริษัท และการบูรณาการเข้ากับระบบงานส่วนอื่น ๆ ขององค์กรที่จะร่วมกันผลักดันให้องค์กรเกิดผลสำเร็จตามวัตถุประสงค์ที่ตั้งไว้

7. องค์ประกอบการบริหารความเสี่ยง

บริษัทได้นำองค์ประกอบระบบการบริหารความเสี่ยงระดับองค์กร(Enterprise Risk Management Integrated Framework) ตามแนวทางกรอบการบริหารความเสี่ยงของ The Committee of Sponsoring Organizations of the Treadway Commission (COSO) ซึ่งเป็นแนวทางการบริหารความเสี่ยงที่มีมาตรฐานในระดับสากล มาใช้เป็นแนวทางในการบริหารความเสี่ยงของบริษัท โดยมีองค์ประกอบการบริหารความเสี่ยง ดังนี้

7.1 กำหนดวัตถุประสงค์ (Objective Setting)

7.2 การระบุความเสี่ยง (Risk Identification)

7.3 การประเมินความเสี่ยง (Risk Assessment)

7.4 การจัดทำแผนจัดการความเสี่ยง (Risk Response)

7.5 กิจกรรมการควบคุม (Control Activities)

7.6 ติดตาม และประเมินผล (Monitoring & Evaluation)

องค์ประกอบการบริหารความเสี่ยงข้างต้น เรียกว่า “กระบวนการการบริหารความเสี่ยง” นอกจากนี้ เพื่อเสริมให้กระบวนการการบริหารความเสี่ยง มีประสิทธิภาพ และเพิ่มโอกาสให้การบริหารความเสี่ยงบรรลุวัตถุประสงค์ บริษัทได้กำหนดองค์ประกอบเพิ่มเติมสำหรับการบริหารความเสี่ยง ได้แก่ สภาพแวดล้อมภายในองค์กร (Internal Environment) และสารสนเทศและการสื่อสาร (Information & Communication) โดยมีรายละเอียดดังนี้

(ก) สภาพแวดล้อมภายในองค์กร (Internal Environment)

บริษัทจัดให้มีสภาพแวดล้อม และบรรยากาศที่เอื้ออำนวย ซึ่งเป็นหลักการพื้นฐานสำหรับขั้นตอนอื่น ๆ ในการบริหารความเสี่ยงในองค์กร หากไม่มีสภาพแวดล้อมภายในองค์กรที่ดีจะมีผลต่อการกำหนดกลยุทธ์และเป้าหมายของบริษัท ในการกำหนดกิจกรรมการบ่งชี้ การประเมิน และการจัดการกับความเสี่ยง โดย

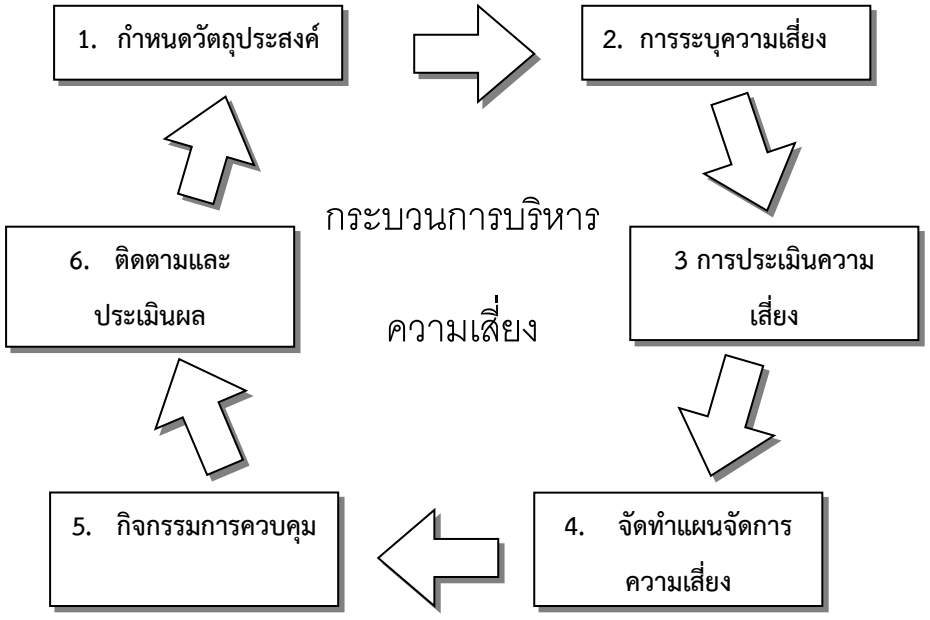
องค์ประกอบที่สำคัญที่มีผลต่อสภาพแวดล้อมภายในองค์กร มีดังนี้

1. ปรัชญา ความเชื่อ และวัฒนธรรมในการบริหารความเสี่ยงเพื่อสร้างมูลค่าให้กับบริษัทในระยะยาว
2. บทบาทของคณะกรรมการตรวจสอบ ซึ่งเป็นปัจจัยสำคัญในการกำกับดูแลการบริหารความเสี่ยง
3. คัดเลือกบุคลากรที่มีความรู้ความสามารถ และความซื่อสัตย์ รวมทั้งพัฒนาบุคลากรให้เหมาะสมกับงานที่รับผิดชอบ
4. จัดให้มีโครงสร้างองค์กรที่เหมาะสม
5. การกำหนดอำนาจหน้าที่ที่เหมาะสม ให้พนักงานสามารถปฏิบัติหน้าที่ ให้บรรลุวัตถุประสงค์ของบริษัท

(ข) สารสนเทศและการสื่อสาร (Information & Communication)

1. ต้องมีการสื่อสารที่ชัดเจนจากคณะกรรมการบริษัท และผู้บริหารระดับสูงเกี่ยวกับนโยบายการบริหารความเสี่ยง และให้พนักงานทุกคนได้เข้าใจบทบาทหน้าที่ของตนในการบริหารความเสี่ยงเพื่อปรับเปลี่ยนพฤติกรรม และ/หรือ กิจกรรมที่ต้องดำเนินการ โดยคาดหวังให้ความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้
2. ต้องมีการระบุแหล่งที่มาและรวบรวมสารสนเทศทั้งจากภายในและภายนอกองค์กร รวมถึงมีการจัดเก็บ และสื่อสารกันภายในองค์กร โดยการจัดเก็บสารสนเทศจะต้องเป็นไปตามรูปแบบ และภายในระยะเวลาตามที่กฎหมายกำหนดเพื่อให้ผู้บริหาร และบุคลากรในบริษัททราบถึงสารสนเทศและทันต่อเหตุการณ์ รวมทั้งปฏิบัติหน้าที่และติดต่อสื่อสารในเรื่องที่เกี่ยวกับการบริหารความเสี่ยงได้อย่างสม่ำเสมอและมีประสิทธิภาพ

8. **กระบวนการบริหารความเสี่ยงของบริษัท ตามแนวทางของ COSO ประกอบด้วย 6 ขั้นตอน ดังนี้**



<u>ขั้นตอนที่ 1</u> **การกำหนดวัตถุประสงค์** (Objective Setting)

ในการดำเนินงานของทุกหน่วยงาน พึงกำหนดวัตถุประสงค์ทางธุรกิจ หรือวัตถุประสงค์ของงานที่ทำให้ชัดเจน สอดคล้องกับนโยบาย เป้าหมาย กลยุทธ์ และความเสี่ยงที่ยอมรับได้ เพื่อให้สามารถวิเคราะห์ความเสี่ยงที่คาดว่าจะเกิดขึ้นได้อย่างครบถ้วน ซึ่งจะทำให้เกิดการบริหารความเสี่ยงที่ดีของระดับหน่วยงาน โดยองค์ประกอบที่จะใช้พิจารณากำหนดวัตถุประสงค์ มีดังนี้

1.1 จะต้องมีความชัดเจน กำหนดขอบเขตได้ รวมทั้งสามารถนำไปปฏิบัติได้ให้เป็นจริงได้และมีกรอบระยะเวลาในการดำเนินการ ซึ่งเป็นไปตามหลักการ “SMART” ซึ่งย่อมาจาก

- Specific : เฉพาะเจาะจง / ชัดเจน
- Measurable : สามารถวัดได้
- Achievable : สามารถบรรลุผลได้ / ปฏิบัติได้
- Reasonable : เป็นจริงได้ / สมเหตุสมผล
- Time constrained : มีกำหนดเวลา / กรอบเวลา

1.2 จะต้องมีการเชื่อมโยงกับเป้าหมาย และสอดคล้องกับวัตถุประสงค์ของบริษัท หรือตัวชี้วัดของหน่วยงานและสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และระดับของความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance)

Risk Appetite หมายถึง ประเภทปัจจัยความเสี่ยงและระดับของความเสี่ยงที่บริษัทยอมรับได้เพื่อช่วยให้บริษัทบรรลุวิสัยทัศน์และภารกิจของบริษัท

Risk Tolerance หมายถึง ระดับความเบี่ยงเบนจากประเภทปัจจัยความเสี่ยงและระดับของความเสี่ยงที่ยอมรับได้

<u>ขั้นตอนที่ 2</u> การระบุความเสี่ยง (Risk Identification)

การระบุความเสี่ยง เป็นการค้นหาว่ามีความเสี่ยงใดที่มีโอกาสจะเกิดขึ้น และทำให้หน่วยงานและองค์กรไม่บรรลุวัตถุประสงค์ ซึ่งการระบุความเสี่ยงมีขั้นตอนดังนี้

2.1 ระบุความเสี่ยง โดยพิจารณาจากกิจกรรม โครงการ และกระบวนการทำงานที่เกี่ยวข้องตามแผนงานต่าง ๆ ของบริษัท เช่น แผนปฏิบัติการประจำปี และแผนธุรกิจประจำปี และอื่น ๆ เป็นต้น ที่ทำให้บริษัทไม่สามารถบรรลุวัตถุประสงค์และเป้าหมาย

2.2 ระบุความเสี่ยงหรือค้นหาความเสี่ยงและสาเหตุ โดยพิจารณาแหล่งที่มาของความเสี่ยงทั้งปัจจัยภายในและปัจจัยภายนอกที่มีผลทำให้การดำเนินงานของแต่ละกิจกรรม โครงการ และกระบวนการทำงาน ไม่บรรลุวัตถุประสงค์และเป้าหมาย

<u>วิธีการระบุความเสี่ยงที่สำคัญ</u> มีดังนี้

- วิเคราะห์การจัดลำดับการดำเนินงาน (Workflow) และการจัดลำดับเอกสาร (Document flow) หรือวิเคราะห์กระบวนการที่เกี่ยวข้องดังกล่าว
- การระดมสมอง หรือการระดมความคิด (Brainstorm)
- จัดประชุมเชิงปฏิบัติการ
- การเก็บข้อมูลประวัติเหตุการณ์ความเสียหายที่เกิดขึ้น

<u>แหล่งที่มาของความเสี่ยงจากปัจจัยภายใน</u> อาจมาจากปัจจัยต่าง ๆ ดังนี้

- วัตถุประสงค์ของบริษัท
- นโยบายและกลยุทธ์
- การดำเนินงานและกระบวนการทำงาน
- โครงสร้างองค์กรและระบบการบริหารงาน
- การบริหารทางการเงิน

<u>แหล่งที่มาของความเสี่ยงจากปัจจัยภายนอก</u> อาจมาจากปัจจัยต่าง ๆ ดังนี้

- นโยบายของรัฐบาล
- สภาวะเศรษฐกิจ
- การแข่งขัน (คู่แข่งขันทางการดำเนินธุรกิจ)
- กฎระเบียบ
- เหตุการณ์ธรรมชาติ
- อื่น ๆ

2.3 การจัดประเภทความเสี่ยงสามารถแบ่งเป็น 9 ประเภท ดังนี้

2.3.1 ความเสี่ยงด้านกลยุทธ์ (Strategic Risk: S) หมายถึง ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ และการปฏิบัติตามแผนกลยุทธ์อย่างไม่เหมาะสม รวมถึงความไม่สอดคล้องกันระหว่างนโยบาย เป้าหมาย กลยุทธ์ โครงสร้างองค์กร และภาวะการณ์แข่งขัน

2.3.2 ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk: O) หมายถึง ความเสี่ยงที่เกิดจากการปฏิบัติงานทุก ๆ ขั้นตอนโดยครอบคลุมถึงปัจจัยที่เกี่ยวข้องกับกระบวนการ อุปกรณ์เทคโนโลยี และบุคลากรในการปฏิบัติงาน

2.3.3 ความเสี่ยงด้านการรายงาน (Report Risk: R) หมายถึง ความเสี่ยงเกี่ยวกับการรายงานข้อมูลต่าง ๆ ให้มีความถูกต้องชัดเจนสร้างความน่าเชื่อถือ โดยตัวอย่างความเสี่ยงด้านการรายงาน เช่น การรายงานผลประกอบการของบริษัท เป็นต้น

2.3.4 ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบต่าง ๆ (Compliance Risk: C) หมายถึง ความเสี่ยงที่เกิดจากการไม่สามารถปฏิบัติตามกฎระเบียบ และกฎหมายที่เกี่ยวข้องได้ หรือกฎระเบียบ และกฎหมายที่มีอยู่ไม่เหมาะสม หรือเป็นอุปสรรคในการปฏิบัติงาน

2.3.5 ความเสี่ยงด้านการเงิน (Financial Risk: F) หมายถึง ความเสี่ยงเกี่ยวกับสภาพคล่องทางการเงิน การบริหารทางการเงินและงบการเงิน เช่น ความเสี่ยงจากการจัดสรรงบประมาณไม่เหมาะสม ตั้งงบประมาณผิดพลาด และใช้งบประมาณเกิน รวมทั้งความเสี่ยงจากความผันผวนของปัจจัยทางการตลาด (Market Risk) และ ความเสี่ยงจากการที่คู่สัญญาไม่ปฏิบัติตามภาระผูกพัน (Credit Risk)

2.3.6 ความเสี่ยงที่จะเกิดใหม่ (Emerging Risk: E) ความเสี่ยงที่จะเกิดใหม่เป็นความสูญเสียที่เกิดขึ้นจากความเสี่ยงที่ยังไม่ได้ปรากฏขึ้นในปัจจุบันแต่อาจจะเกิดขึ้นได้ในอนาคตเนื่องจากสภาวะแวดล้อมที่เปลี่ยนไป ความเสี่ยงประเภทนี้เป็นความเสี่ยงที่เกิดขึ้นอย่างช้า ๆ ยากที่จะระบุได้ มีความถี่ของการเกิดต่ำ เมื่อเกิดขึ้นแล้วจะส่งผลกระทบอย่างรุนแรง ความเสี่ยงที่จะเกิดใหม่นี้มักจะถูกระบุขึ้นมาจากการคาดการณ์บนพื้นฐานของการศึกษาจากหลักฐานที่มีปรากฏอยู่ ความเสี่ยงที่จะเกิดใหม่นี้มักจะเป็นผลมาจากการเปลี่ยนแปลงทางการเมือง กฎหมาย สังคม เทคโนโลยี สภาพแวดล้อมทางกายภาพ หรือการเปลี่ยนแปลงตามธรรมชาติ

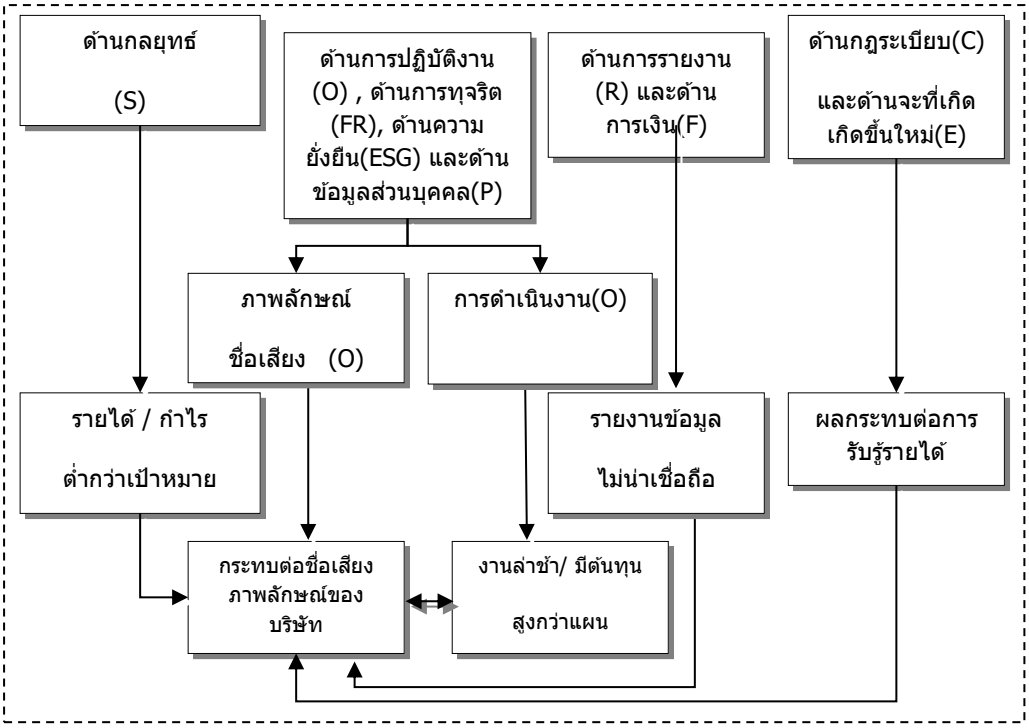
2.3.7 ความเสี่ยงที่จะเกิดการทุจริต (Fraud Risk: Fr) เป็นความเสี่ยงที่เกิดจากจากการดำเนินงานที่อาจก่อให้เกิดการทุจริต การขัดกันระหว่างผลประโยชน์ส่วนตนกับผลประโยชน์ส่วนรวมหรือการรับสินบน ความเสี่ยงประเภทนี้อาจกระทบต่อชื่อเสียงภาพลักษณ์ของกิจการและอื่นๆ เป็นต้น

2.3.8 ความเสี่ยงในการดำเนินงานอย่างยั่งยืน (Environmental, Social and Governance: ESG) เป็นความเสี่ยงที่เกี่ยวข้องกับประเด็นด้านสิ่งแวดล้อม สังคมและบรรษัทภิบาล ความเสี่ยงประเภทนี้อาจกระทบต่อชื่อเสียงภาพลักษณ์ของกิจการและอื่นๆเป็นต้น

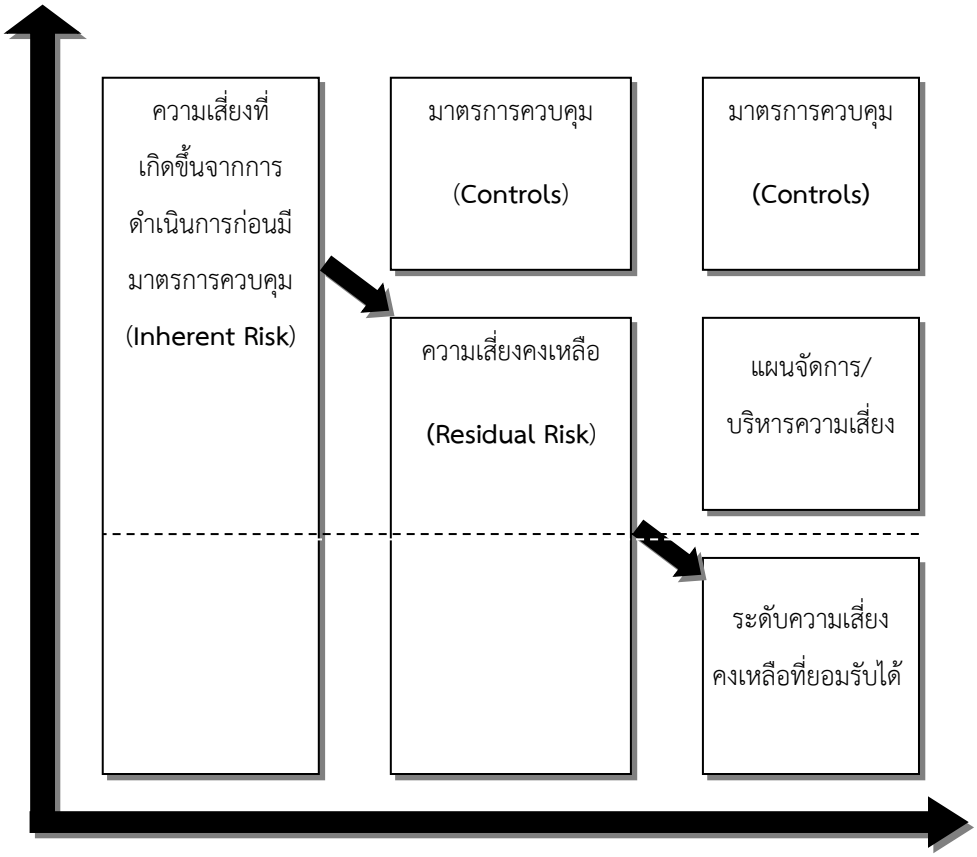
2.3.9 ความเสี่ยงด้านข้อมูลส่วนบุคคล (Privacy: P) เป็นความเสี่ยงที่มุ่งเรื่องการปฏิบัติการในการประมวลผลข้อมูล เริ่มตั้งแต่กระบวนการเก็บ การเก็บรักษา การใช้ การส่งต่อหรือเปิดเผยและการลบและทำลายที่อาจทำให้สูญหาย รั่วไหลหรือละเมิดข้อมูลส่วนบุคคลซึ่งกระทบต่อสิทธิและเสรีภาพของส่วนบุคคล

การจัดประเภทความเสี่ยงให้เป็นหมวดหมู่ (S, O, R, C, F, E, Fr, ESG and P) จะแสดงให้เห็นความสัมพันธ์ของความเสี่ยงแต่ละประเภทแต่ละเรื่องได้อย่างชัดเจนเพื่อให้สามารถบริหารจัดการความเสี่ยงที่เป็นต้นเหตุของความเสียหายอย่างแท้จริง โดยสามารถแสดงให้เห็นได้จากการจัดทำแผนที่ความเสี่ยง (Risk Map)

การจัดทำแผนที่ความเสี่ยง (Risk Map) ตามประเภทของความเสี่ยง



<u>ขั้นตอนที่ 3</u> **การประเมินความเสี่ยง (Risk Assessment)**



การประเมินความเสี่ยง หมายถึง การวัดระดับความรุนแรงของความเสี่ยงว่ามีมากน้อยเพียงใด โดยนำความเสี่ยงที่ได้จากขั้นตอนที่ 2 (การระบุความเสี่ยง) มาประเมินความเสี่ยง โดยมีขั้นตอนดังนี้

3.1 พิจารณาความเสี่ยงที่เกิดขึ้นจากการดำเนินการก่อนมีมาตรการการควบคุมความเสี่ยงที่ได้จากการระบุความเสี่ยงในขั้นตอนที่ 2 โดยพิจารณาระดับความรุนแรงของความเสี่ยง และโอกาสที่อาจจะเกิดขึ้นก่อนมีมาตรการควบคุม (Inherent Risk)

3.2 ระบุมาตรการควบคุมที่มีอยู่ (Controls) เพื่อควบคุม / ลดความเสี่ยงของแต่ละสาเหตุความเสี่ยง

3.3 ประเมินความเสี่ยงที่เหลืออยู่หลังจากมีมาตรการควบคุม (Residual Risk) โดยวิเคราะห์หาโอกาสที่จะเกิดความเสี่ยง (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) ตามเกณฑ์ในการพิจารณาหาระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) ซึ่งสามารถพิจารณาได้ทั้งเชิงคุณภาพและเชิงปริมาณ โดยบริษัทกำหนดเกณฑ์ในการประเมินไว้ 5 ระดับ โดย “ระดับความเสี่ยง” จะเท่ากับ ผลคูณของโอกาสที่จะเกิดความเสี่ยง (Likelihood) กับระดับความรุนแรงของผลกระทบ (Impact)

3.4 นำ “ระดับความเสี่ยง” ที่ได้ประเมินแล้วตามข้อ 3.3 มาจัดลำดับโดยระดับความสำคัญของความเสี่ยงมีทั้งหมด 3 ระดับ ดังนี้

ระดับ 1. **H: High Risk** ความเสี่ยงสูงระดับที่มีนัยสำคัญ โดยผู้บริหารจำเป็นต้องเร่งจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ทันที (ระดับคะแนน 15-25 คะแนน)

ระดับ 2. **M: Moderate Risk** ความเสี่ยงระดับปานกลาง โดยต้องมีการจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป หรือการติดตามอย่างเหมาะสม เพื่อป้องกันไม่ให้ความเสี่ยงดังกล่าวเกิดขึ้น (ระดับ 5-12 คะแนน)

ระดับ 3. **L: Low Risk** ความเสี่ยงระดับต่ำ โดยต้องมีการควบคุมเพื่อป้องกัน หรือการติดตามอย่างเหมาะสม เพื่อไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ (ระดับคะแนน 1-4 คะแนน)

การประเมินความเสี่ยงต้องดำเนินการทั้งก่อนการจัดทำแผนจัดการ / บริหารความเสี่ยง และหลังจากที่ได้ดำเนินการตามแผนจัดการ / บริหารความเสี่ยงแล้ว ซึ่งจะทำให้ทราบว่าแผนจัดการ / บริหารความเสี่ยงมีประสิทธิภาพ และประสิทธิผลเพียงใดควรทบทวน หรือปรับปรุงแผนจัดการ / บริหารความเสี่ยงหรือไม่

ตารางจัดลำดับความเสี่ยง (Risk Matrix) และระดับความเสี่ยงที่ยอมรับได้

คณะกรรมการบริหาร ได้กำหนดระดับความเสี่ยงที่ยอมรับได้ไว้ที่ระดับความเสี่ยงไม่เกินระดับ 5 โดยได้จัดทำเป็นตารางจัดลำดับความเสี่ยงและผลกระทบไว้ดังนี้

ระดับ		**ไม่มีนัยสำคัญ**	**น้อย**	**ปานกลาง**	**มาก**	**ร้ายแรงมาก**
ความน่าจะเกิด		Insignificant	Minor	Moderate	Major	Catastrophic
		1	2	3	4	5
บ่อยครั้ง	5					
บ่อย	4					
ปานกลาง	3					
ไม่บ่อย	2					
นาน ๆ ครั้ง	1					

<u>ขั้นตอนที่ 4</u> **การจัดทำแผนการจัดการความเสี่ยง** (Risk Response)

การจัดทำแผนการจัดการความเสี่ยง หมายถึง การกำหนดแนวทางการดำเนินงานเพื่อลดโอกาสที่จะเกิดความสูญเสียโดยนำผลจากการประเมินความเสี่ยงที่ได้จากขั้นตอนที่ 3 มาจัดทำแผนจัดการ / บริหารความเสี่ยงตามลำดับความสำคัญของความเสี่ยง โดยหน่วยงานเจ้าของความเสี่ยง ซึ่งเข้าใจความเสี่ยงที่เกี่ยวข้องกับหน่วยงานตนเองมากที่สุดเป็นผู้จัดทำแผนจัดการ / บริหารความเสี่ยงโดยวิเคราะห์หาวิธีการจัดการกับความเสี่ยงที่คาดว่าจะเกิดขึ้น วิธีการใดวิธีการหนึ่งหรือหลายวิธีรวมกันเพื่อลดโอกาสที่ความเสี่ยงจะเกิดขึ้น และ/หรือ ลดความรุนแรงของผลกระทบของความเสี่ยงให้อยู่ในระดับที่หน่วยงานยอมรับได้ และจัดทำเป็นแผนจัดการ / บริหารความเสี่ยงของหน่วยงานตนเอง โดยมีวิธีการจัดการความเสี่ยงไว้ดังนี้

4.1 วิเคราะห์หาวิธีการจัดการกับความเสี่ยงที่คาดว่าจะเกิดขึ้น โดยมีแนวทางในการจัดการ / บริหารความเสี่ยงได้ 4 วิธี ดังนี้

4.1.1 การควบคุม / ลด (Reduce) คือ การควบคุมความเสี่ยงหรือหาวิธีการบริหารความเสี่ยง เช่น ใช้เทคนิควิชาการทางวิศวกรรมหรือการจัดทำแผนฉุกเฉิน หรือการปรับปรุงแก้ไขกระบวนการดำเนินงาน เป็นต้น

4.1.2 การโอนย้าย (Transfer) คือ การถ่ายโอนความเสี่ยงหรือโอนย้ายความเสี่ยงให้ผู้อื่นรับผิดชอบ เช่น การทำประกันภัยหรือจ้างบุคคลภายนอกเป็นผู้ดำเนินการแทน เป็นต้น

4.1.3 การหลีกเลี่ยง (Avoid) คือ การกำจัดความเสี่ยงหรือหลีกเลี่ยงไม่ยอมรับความเสี่ยงนั้นเลย เช่น การเปลี่ยนวัตถุประสงค์หรือหยุดทำกิจกรรม เป็นต้น

4.1.4 การยอมรับ (Accept) ความเสี่ยงที่เหลือในปัจจุบันอยู่ในระดับที่ยอมรับได้ โดยไม่ต้องดำเนินการใดๆ เพื่อลดโอกาสหรือผลกระทบที่อาจเกิดขึ้นอีก มักใช้กับความเสี่ยงที่ต้นทุนของมาตราการจัดการสูงไม่คุ้มกับประโยชน์ที่ได้รับ

ทั้งนี้ การเลือกวิธีการจัดการความเสี่ยง ต้องพิจารณาเปรียบเทียบต้นทุนในการจัดการ / บริหารความเสี่ยงและความเสียหายที่เกิดขึ้นด้วย

4.2 จัดทำแผนจัดการ / บริหารความเสี่ยงเพิ่มเติมโดยมีขั้นตอน ดังนี้

4.2.1 ระบุวิธีการ มาตรการที่เป็นทางเลือกจากแนวทางในการจัดการ / บริหารความเสี่ยงเพื่อให้ความเสี่ยงคงเหลืออยู่ในระดับที่ยอมรับได้ และสอดคล้องกับวัตถุประสงค์ที่กำหนดไว้

4.2.2 ศึกษาเปรียบเทียบความเป็นไปได้และค่าใช้จ่ายของแต่ละทางเลือกตามข้อ 4.2.1

ข้างต้น โดยคำนึงถึงความคุ้มค่าในการลงทุนทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน โดยต้นทุนในการดำเนินการจะต้องไม่สูงกว่าความเสียหายที่คาดว่าจะเกิดขึ้น

4.2.3 เลือกวิธีการที่ดีที่สุด โดยกำหนดผู้รับผิดชอบ / ระยะเวลา / งบประมาณพร้อมกำหนดแผนปฏิบัติการ

<u>ขั้นตอนที่ 5</u> **กิจกรรมการควบคุม** (Control Activities)

กิจกรรมการควบคุม หมายถึง นโยบาย และแนวทางการปฏิบัติงานในการควบคุมที่ฝ่ายบริหารกำหนดขึ้นเพื่อให้มั่นใจว่าแผนจัดการ / บริหารความเสี่ยงที่กำหนดขึ้นอย่างมีประสิทธิภาพมีการกำหนดผู้รับผิดชอบและระยะเวลาในการดำเนินงานไว้อย่างชัดเจน และกิจกรรมการควบคุมนั้นก็เป็นวิธีการหนึ่งในการจัดการ / บริหารความเสี่ยง

<u>ตัวอย่าง</u> กิจกรรมการควบคุม เช่น

- การจัดทำนโยบายและวิธีปฏิบัติงาน
- การสอบทานและการกำกับดูแลการปฏิบัติงาน
- ระบบงานคอมพิวเตอร์และการควบคุมด้านคอมพิวเตอร์
- การควบคุมทางกายภาพ
- ดัชนีตัวชี้วัดผลการดำเนินงาน
- การแบ่งแยกหน้าที่ความรับผิดชอบงาน

กิจกรรมการควบคุมที่จะเกิดประโยชน์มากที่สุดควรจะแทรกอยู่ในกระบวนการสามารถป้องกัน และลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยต้นทุนในการดำเนินงานการจะต้องไม่สูงกว่าความเสียหายที่คาดว่าจะเกิดขึ้น

การกำหนดกิจกรรมการควบคุมอย่างชัดเจนจะทำให้แผนการจัดการบริหารความเสี่ยงเพิ่มเติมที่ได้จัดทำไว้บรรลุวัตถุประสงค์โดยจัดทำนโยบาย และวิธีปฏิบัติเพิ่มเติม กำหนดผู้รับผิดชอบ และระยะเวลาแล้วเสร็จอย่างชัดเจน ในบางกรณีอาจจัดทำกระบวนการควบคุมภายในเพิ่มเติมกำหนดผู้รับผิดชอบและระยะเวลาแล้วเสร็จอย่างชัดเจน ในบางกรณีอาจจัดทำกระบวนการควบคุมภายในเพิ่มเติม เช่น การสอบทาน การกำกับดูแล การแบ่งแยกหน้าที่งานเพิ่ม เป็นต้น

กิจกรรมการควบคุม ถือเป็นองค์ประกอบหนึ่งของระบบการควบคุมภายในในลักษณะของการเสนอแนะ (Suggestive Control) เพื่อปรับปรุงและพัฒนาระบบการดำเนินงานและระบบการควบคุมภายในให้เหมาะสมกับสถานการณ์ ซึ่งหน่วยงานจะต้องจัดทำขึ้นเพื่อลดความเสี่ยง และทำให้เกิดความคุ้มค่า ตลอดจนทำให้ฝ่ายบริหารเกิดความมั่นใจในประสิทธิผลของระบบการควบคุมภายในที่มีอยู่

ขั้นตอนที่ 6 **การติดตามและประเมินผล** (Monitoring & Evaluation)

การติดตามและประเมินผล หมายถึง กระบวนการควบคุมคุณภาพการปฏิบัติงานและประเมินผล แผนการจัดการ / บริหารความเสี่ยงเพิ่มเติม หรือกิจกรรมการควบคุมที่วางไว้อย่างต่อเนื่องและสม่ำเสมอ โดยการติดตามในระหว่างการปฏิบัติงานและประเมินผลเป็นครั้งคราวตามระยะเวลา เพื่อให้มั่นใจว่าการจัดการ / การบริหารความเสี่ยงมีประสิทธิภาพและประสิทธิผล จึงต้องมีรายงานความก้าวหน้า ปัญหา และอุปสรรคของการจัดการ / บริหารความเสี่ยง เพื่อใช้เป็นแนวทางในการทบทวนหรือปรับปรุงแผนการจัดการ / บริหารความเสี่ยงต่อไป โดยมีขั้นตอนของการติดตามและประเมินผล ดังนี้

- จัดทำแผนการบริหารความเสี่ยง ซึ่งประกอบด้วย

    1) รายงานปัจจัยความเสี่ยง และระดับความเสี่ยง

    2) การควบคุมที่มีอยู่การจัดการความเสี่ยงที่เหลือ

    3) หน่วยงาน / ผู้รับผิดชอบความเสี่ยงหลังการควบคุม

- รายงานต่อผู้บริหารระดับสูงหรือคณะกรรมการบริษัท ซึ่งรายงานดังกล่าวมีเนื้อหาดังนี้

    4) ความเสี่ยงที่คลาดเคลื่อนเกินกว่าที่ยอมรับได้

    5) ความเสี่ยงสูงสุด 5 ระดับ

    6) เหตุการณ์ที่แม้จะมีโอกาสต่ำ แต่จะมีผลต่อความปลอดภัยต่อพนักงานหรือบุคคลอื่น

    7) การกระทำผิดกฎหมาย

    8) ผลเสียหายสำคัญต่อทรัพย์สิน การด้อยค่าของทรัพย์สิน

9) ชื่อเสียงของหน่วยงานการจัดทำงบและรายงานทางการเงินไม่เหมาะสม

9. บริษัทกำหนดให้ทั่วทั้งองค์กรทั้งระดับองค์กรและฝ่ายร่วมมือในการจัดการประเมินความเสี่ยง พร้อมทั้งรายงานการประเมินความเสี่ยง และกำหนดกระบวนการติดตามและประเมินผลการดำเนินงานตามแผนการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อรายงานต่อคณะกรรมการตรวจสอบ/คณะกรรมการบริษัท

10. บริษัทได้กำหนดให้มีการสอบทานและทบทวนนโยบายบริหารความเสี่ยงอย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับการปฏิบัติงานและสถานการณ์ที่เปลี่ยนแปลงไป

นโยบายการบริหารความเสี่ยงฉบับนี้ ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัทครั้งที่ 001 เมื่อวันที่ 23 เดือนมกราคม พ.ศ. 2566 และมีผลบังคับใช้ ตั้งแต่ วันที่ 24 เดือนมกราคม พ.ศ. 2566 เป็นต้นไป จนกว่าจะมีการเปลี่ยนแปลง

ลงชื่อ.....

(นายศมณ สุวรรณรัตน์)

ประธานกรรมการบริษัท