บริษัท อัคคีปราการ จำกัด (มหาชน)

AKKHIE PRAKARN PUBLIC COMPANY LIMITED

คู่มือบริหารความเสี่ยง

(Risk Management Manual)

สารบัญ

บทนำ

ปัจจุบันการดำเนินงานขององค์กรจะต้องเผชิญกับสภาวะความไม่แน่นอนทั้งจากปัจจัยภายใน และภายนอกองค์กร ซึ่งก่อให้เกิดเหตุการณ์ทั้งที่เป็นความเสี่ยงและโอกาส (Risk and Opportunities) ต่อองค์กร โดยความเสี่ยงจะส่งผลกระทบในเชิงลบ ในขณะที่โอกาสจะเป็นตัวสร้างมูลค่าต่อองค์กร ดังนั้น การบริหารความเสี่ยงจึงเป็นเครื่องมือที่สำคัญที่จะช่วยบริหารจัดการกับความไม่แน่นอน ความเสี่ยงและโอกาสที่เกี่ยวข้องได้อย่างมีประสิทธิผล เพิ่มมูลค่าสูงสุดให้กับผู้มีส่วนได้เสีย ป้องกัน รักษา และส่งเสริมให้องค์กรสามารถบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในระยะสั้นและระยะยาว

บริษัทฯ ให้ความสำคัญของการบริหารความเสี่ยง เพื่อเตรียมความพร้อมในการป้องกันและปรับตัวรับความเสี่ยงต่าง ๆ รวมถึงแสวงหาโอกาสในการดำเนินธุรกิจจากความเสี่ยงเหล่านั้นอย่างมีประสิทธิภาพ จึงมีการกำหนดกรอบการบริหารความเสี่ยงขององค์กร (Enterprise Risk Management Framework) โดยพิจารณาแนวทางการจัดการความเสี่ยงขององค์กร ตามกรอบการบริหารความเสี่ยง COSO-ERM 2017 เพื่อนำมาปรับใช้ในการบริหารจัดการความเสี่ยงขององค์กรให้อยู่ในระดับที่เหมาะสม หรือ ที่องค์กรยอมรับได้ รวมถึงเป็นสื่อกลางให้บุคลากรทุกระดับของบริษัทฯ เข้าใจถึงความสำคัญของกระบวนการบริหารความเสี่ยง สามารถนำไปปฏิบัติจนเป็นวัฒนธรรมองค์กร อันจะนำไปสู่ความมั่นคงเข้มแข็งขององค์กรต่อไป

การบริหารความเสี่ยง
(Risk Management)

นิยามความเสี่ยง และการบริหารความเสี่ยงองค์กร

ความเสี่ยง (Risk) หมายถึง ความไม่แน่นอนของเหตุการณ์ หรือการดำเนินการใด ๆ ที่เกิดขึ้นจากทั้งปัจจัยภายในและปัจจัยภายนอก ที่มีผลกระทบต่อองค์กร ส่งผลให้การดำเนินงานอาจไม่ประสบความสำเร็จตามวัตถุประสงค์ที่กำหนดไว้ และสามารถเกิดขึ้นได้ตลอดเวลา

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

ปัจจัยเสี่ยงพิจารณาได้จาก

1) **ปัจจัยภายนอก** เป็นองค์ประกอบต่างๆที่อยู่ภายนอกองค์กรซึ่งมีอิทธิพลต่อวัตถุประสงค์ เป้าหมายขององค์กร เช่น
   - วัฒนธรรม การเมือง กฎหมาย ข้อบังคับ การเงิน เทคโนโลยี เศรษฐกิจ สภาพแวดล้อมในการแข่งขันทั้งภายในประเทศและต่างประเทศ
   - ตัวขับเคลื่อนหลักและแนวโน้มที่ส่งผลกระทบต่อวัตถุประสงค์ขององค์กร
   - การยอมรับและคุณค่าของผู้มีส่วนได้เสียภายนอกองค์กร
2) **ปัจจัยภายใน** เป็นสิ่งต่างๆ ที่อยู่ภายในองค์กรและมีอิทธิพลต่อเป้าหมายขององค์กร เช่น
   - ขีดความสามารถขององค์กรในแง่ของทรัพยากรและความรู้ เช่น เงินทุน เวลา บุคลากร
   - กระบวนการ ระบบและเทคโนโลยี
   - ระบบสารสนเทศ Flow ข้อมูล และกระบวนการตัดสินใจทั้งที่เป็นทางการและไม่เป็นทางการ
   - ผู้มีส่วนได้เสียภายในองค์กร
   - นโยบาย วัตถุประสงค์และกลยุทธ์องค์กร รวมถึง การรับรู้ คุณค่าและวัฒนธรรมองค์กร
   - โครงสร้าง เช่น ระบบการจัดการ บทบาทหน้าที่และความรับผิดชอบ

กรอบการบริหารความเสี่ยงองค์กร (Enterprise Risk Framework)

เพื่อเพิ่มโอกาสในการบรรลุวัตถุประสงค์ทางธุรกิจ ส่งเสริมการบริหารเชิงรุก และตระหนักถึงความจำเป็นในการชี้บ่งและแก้ไขความเสี่ยงทั่วทั้งองค์กร บริษัทได้นำ COSO-ERM 2017 (Enterprise Risk Management-Integrating with Strategy and Performance) มาเป็นกรอบในการบริหารความเสี่ยงของบริษัท ประกอบด้วยองค์ประกอบ 5 ประการ ได้แก่

1. การกำกับดูแลกิจการ และวัฒนธรรมองค์กร (Governance & Culture)
2. กำหนดกลยุทธ์และวัตถุประสงค์องค์กร (Strategy & Objective-Setting)
3. ผลการปฏิบัติงาน (Performance)
4. การสอบทานและปรับปรุง (Review & Revision)
5. สารสนเทศ การสื่อสาร และการรายงาน (Information , Communication & Reporting)

ประเภทความเสี่ยงขององค์กร

1. ความเสี่ยงด้านกลยุทธ์ การให้บริการและภาพลักษณ์ (Strategic & Brand Risk) : ความเสี่ยงที่เกี่ยวข้องกับการกำหนดแผนกลยุทธ์ แผนการดำเนินงาน และการนำแผนดังกล่าวไปปฏิบัติอย่างไม่เหมาะสม นอกจากนี้ ความเสี่ยงด้านกลยุทธ์ยังรวมถึงการเปลี่ยนแปลงจากปัจจัยภายนอกและปัจจัยภายใน อันส่งผลกระทบต่อการกำหนดกลยุทธ์ หรือการดำเนินงานเพื่อให้บรรลุวัตถุประสงค์หลัก เป้าหมาย และแนวทางการดำเนินงานขององค์กร

2. ความเสี่ยงด้านปฏิบัติงาน และการบริหารจัดการห่วงโซ่อุปทาน (Operational & Supply Chain Risk) : ความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติงานของแต่ละกระบวนการ หรือกิจกรรมภายในองค์กร รวมทั้งความเสี่ยงที่เกี่ยวข้องกับการบริหารจัดการห่วงโซ่อุปทาน และข้อมูลความรู้ต่างๆ เพื่อให้การปฏิบัติงานบรรลุเป้าหมายที่กำหนด ซึ่งความเสี่ยงด้านปฏิบัติการ จะส่งผลกระทบต่อประสิทธิภาพของกระบวนการทำงาน และการบรรลุวัตถุประสงค์หลักขององค์กรในภาพรวม

3. ความเสี่ยงด้านการเงิน (Financial Risk) : ความเสี่ยงที่เกี่ยวข้องกับการบริหารจัดการทางการเงิน โดยอาจเป็นความเสี่ยงที่เกิดจากปัจจัยภายใน เช่น การบริหารจัดการด้านสภาพคล่อง ด้านเครดิต ด้านเงินลงทุน หรือจากปัจจัยภายนอก เช่น การเปลี่ยนแปลงของอัตราดอกเบี้ย อัตราแลกเปลี่ยน หรือความเสี่ยงที่คู่สัญญาไม่สามารถปฏิบัติตามภาระผูกพันที่ตกลงไว้ อันส่งผลกระทบต่อการดำรงอยู่ รวมถึงส่งผลให้เกิดความเสียหายต่อองค์กร

4. ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ และพันธสัญญา (Compliance Risk) :ความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติตามกฎระเบียบ ข้อบังคับของหน่วยงานกำกับดูแล รวมทั้งความเสี่ยงที่เกี่ยวกับกฎหมายต่างๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัท ซึ่งเมื่อมีความเสี่ยงด้านนี้เกิดขึ้น จะส่งผลกระทบต่อชื่อเสียงและภาพลักษณ์ขององค์กรโดยรวม

5. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) : ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยี ซึ่งจะมีผลกระทบต่อระบบหรือการปฏิบัติงาน ของสถาบันการเงิน รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (cyber threat)

6. ความเสี่ยงด้านความยั่งยืน (ESG Risk) : เป็นความเสี่ยงที่เกี่ยวข้องกับประเด็นด้าน “ESG” หรือสิ่งแวดล้อม (Environmental) สังคม (Social) และบรรษัทภิบาล (Governance) หรือเรียกว่า “ Risk” ซึ่งเป็นความท้าทายที่องค์กรจะต้องหาวิธีการบริหารจัดการความเสี่ยง เพื่อสร้างโอกาส และลดความเสี่ยง ซึ่งมีผลต่อความสามารถในการสร้างผลกำไร การแข่งขัน ภาพลักษณ์ ชื่อเสียง และความอยู่รอดขององค์กร

7. ความเสี่ยงที่เกิดขึ้นใหม่ /การจัดการ หรือการตอบสนองต่อวิกฤต (Emerging Risk/Crisis Management & Response) : เป็นความสูญเสียที่อาจเกิดขึ้นจากความเสี่ยงที่ยังไม่เคยปรากฏขึ้นหรือไม่เคยมีประสบการณ์ ณ เวลาปัจจุบัน แต่เนื่องจากในอนาคตมักจะมีการเปลี่ยนแปลงเกิดขึ้นได้หลายกรณี อันอาจเป็นผลจากการเปลี่ยนแปลงทางการเมือง กฎหมาย สังคม เทคโนโลยี สภาพแวดล้อมทางกายภาพ หรือการเปลี่ยนแปลงตามธรรมชาติ ซึ่งในบางเหตุการณ์อาจจะไม่สามารถประเมินผลกระทบหรืออาจจะไม่สามารถระบุความเสี่ยงได้แน่นอน เช่น ความเสี่ยงจากนาโนเทคโนโลยี ความเสี่ยงจากภาวะเศรษฐกิจ หรือความเสี่ยงจากการ เปลี่ยนแปลงของสภาวะภูมิอากาศ เป็นต้น

กระบวนการบริหารความเสี่ยง

บริษัทฯ ให้ความสำคัญกับการบริหารจัดการความเสี่ยง เพื่อเตรียมความพร้อมในการป้องกัน และปรับตัวรับความเสี่ยงต่างๆ รวมถึงแสวงหาโอกาสในการดำเนินธุรกิจจากความเสี่ยงเหล่านั้นอย่างมีประสิทธิภาพ จึงได้กำหนดกระบวนการบริหารความเสี่ยง ซึ่งประกอบด้วย 7 ขั้นตอน ดังนี้

1. กำหนดโครงสร้างการกำกับดูแล

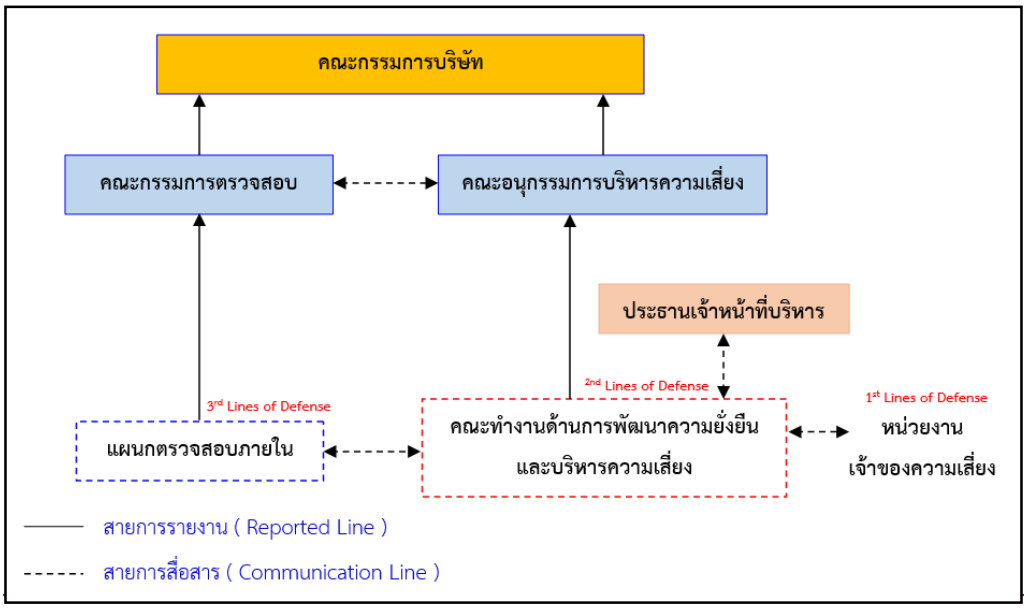
โครงสร้างการกำกับดูแลของบริษัทฯ กำหนดให้ครอบคลุมตั้งแต่ระดับคณะกรรมการบริษัท คณะกรรมการตรวจสอบ คณะอนุกรรมการบริหารความเสี่ยง ประธานกรรมการบริหาร คณะกรรมการระบบการจัดการและบริหารความเสี่ยง หน่วยงานตรวจสอบภายใน และเจ้าของความเสี่ยง โดยบุคคลเหล่านี้ มีบทบาทสำคัญ ในการกำ กับดูแล ควบคุม และติดตามการบริหารจัดการความเสี่ยงขององค์กร ให้เกิดประสิทธิภาพสูงสุด

บริษัทกำหนดให้มี คณะกรรมการระบบการจัดการมาตรฐานและบริหารความเสี่ยง ทำหน้าที่ ควบคุมดูแลกลยุทธ์ความเสี่ยง และกำกับดูแล เพื่อสนับสนุนผู้บริหารในการดำเนินการเพื่อบรรลุกลยุทธ์และวัตถุประสงค์ทางธุรกิจ และมีความเป็นอิสระที่จะส่งเสริมให้ คณะกรรมการบริษัท (BOD) มีความเที่ยงตรงในการประเมินผลการปฏิบัติงานโดยปราศจาก Conflict of interest โดยทำการตรวจสอบและถ่วงดุลผู้บริหาร เพื่อให้มั่นใจว่าองค์กรบริหารงานโดยยึดผลประโยชน์สูงสุดของผู้มีส่วนได้ส่วนเสียทุกฝ่าย

คณะกรรมการระบบการจัดการมาตรฐานและบริหารความเสี่ยง จะได้รับข้อมูลในประเด็นที่เกี่ยวข้องอยู่เสมอ เมื่อบริบททางธุรกิจเปลี่ยน ความเสี่ยงที่จะมีผลต่อกลยุทธ์และวัตถุประสงค์ก็เปลี่ยนแปลงไปด้วย

กำหนดโครงสร้างดำเนินงานในการบริหารความเสี่ยง และออกแบบสายการรายงานเพื่อดำเนินการตามกลยุทธ์และวัตถุประสงค์ขององค์กร ในการกำกับดูแล ควบคุม และติดตามการบริหารจัดการความเสี่ยงขององค์กร ให้เกิดประสิทธิภาพสูงสุด ดังนี้

โครงสร้างการบริหารจัดการความเสี่ยง



ระดับ	ความรับผิดชอบและอำนาจหน้าที่
<u>กำกับดูแลกิจการ</u>	
คณะกรรมการบริษัท (Board Of Director : BOD)	- พิจารณาอนุมัตินโยบายและสนับสนุนการบริหารจัดการความเสี่ยงที่เกิดขึ้นในบริษัทฯ ให้เป็นไปอย่างมีประสิทธิภาพ - พิจารณาอนุมัติรายงานระดับความเสี่ยงที่ยอมรับได้ขององค์กร (Risk Appetite - มอบอำนาจการบริหารความเสี่ยงให้กับ คณะอนุกรรมการบริหารความเสี่ยง
คณะอนุกรรมการบริหารความเสี่ยง (Risk Management sub-Committee : RMC)	- สอบทานและนำเสนอนโยบายการบริหารความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้ให้แก่ BOD เพื่อพิจารณาอนุมัติ - กำหนดกรอบการบริหารความเสี่ยง กำกับดูแลการพัฒนา และการปฏิบัติตามกรอบการบริหารความเสี่ยงทั่วทั้งองค์กร - สอบทานรายงานการบริหารความเสี่ยงเพื่อติดตามความเสี่ยงที่สำคัญ และดำเนินการให้มั่นใจได้ว่าองค์กรมีการจัดการความเสี่ยงอย่างเพียงพอและเหมาะสม - นำเสนอความเสี่ยงในภาพรวมของบริษัท รวมถึงความเพียงพอของระบบการควบคุมภายใน เพื่อการจัดการความเสี่ยงด้านต่าง ๆ ที่สำคัญให้กับ BOD - ให้คำแนะนำในด้านงานบริหารความเสี่ยง และการพิจารณาแก้ไขข้อมูลต่าง ๆ ที่เกี่ยวกับการพัฒนาระบบการบริหารความเสี่ยง - มีอำนาจแต่งตั้งคณะทำงานประเมินและติดตามความเสี่ยง - ดำเนินการประชุม 2 ครั้ง/ปี เพื่อติดตามประสิทธิผลของการบริหารจัดการความเสี่ยงและทบทวนสถานะของความเสี่ยง
<u>การจัดการ</u> (1st Line and 2nd Line Roles)	
คณะทำงานด้านการพัฒนาความยั่งยืนและบริหารความเสี่ยง (SD & Risk Management : SD & RM)	- กำหนดวัตถุประสงค์ เป้าหมาย นโยบาย และกลยุทธ์ในการดำเนินงานด้านความยั่งยืน โดยให้สอดคล้องกับนโยบายในการดำเนินธุรกิจของบริษัทฯ - กำหนดแผนงานที่เหมาะสม สอดคล้องกับแผนกลยุทธ์ทางธุรกิจและสามารถบรรลุเป้าหมายตัวชี้วัด ด้านความยั่งยืนที่กำหนดอย่างสอดคล้อง และสนับสนุนตัวชี้วัดผลงาน

ระดับ	ความรับผิดชอบและอำนาจหน้าที่
	- ติดตาม และประเมินผลงาน ตลอดจนการรายงานผลการดำเนินงานด้านความยั่งยืน ต่อผู้บริหาร พร้อมทั้งทบทวนแผนงานให้มีประสิทธิภาพอยู่เสมอ - ออกกฎเกณฑ์ ระเบียบ คำสั่ง และประกาศที่เกี่ยวกับการพัฒนาด้านความยั่งยืน ให้ทุกส่วนที่เกี่ยวข้องได้รับทราบ และนำไปปฏิบัติให้เป็นไปในทิศทางเดียวกัน - กำกับดูแลให้หน่วยงานเจ้าของความเสี่ยง (RO) มีการปฏิบัติตามกระบวนการบริหารจัดการความเสี่ยงขององค์กร - ควบคุม และติดตามการบริหารจัดการความเสี่ยงขององค์กรให้อยู่ในระดับความเสียงที่ยอมรับได้ (Risk Appetite) - สื่อสารความเสี่ยงที่อยู่ในระดับสูงและสูงมากทั้งหมด ที่อาจมีผลกระทบต่อแผนธุรกิจและกลยุทธ์ของบริษัทฯ และแนวทางการจัดการความเสี่ยงต่อคณะอนุกรรมการบริหารความเสี่ยง (RMC) ทันที - ให้คำแนะนำและข้อเสนอแนะแก่หน่วยงานเจ้าของความเสียง (RO) ที่เกี่ยวข้องกับความเสี่ยงที่สำคัญ และการบรรเทาผลกระทบทบ - ทวนการบริหารความเสียงอย่างสม่ำเสมอ เพื่อให้มันใจว่า ความเสียงของบริษัทฯ ได้รับการจัดการอย่างเหมาะสม เมื่อบริบททางธุรกิจเปลี่ยนแปลงไป - ส่งเสริม สนับสนุน ให้เกิดการแลกเปลี่ยน ความรู้ ความสำเร็จ และประสบการณ์ ด้านความยั่งยืน รวมถึงแนวทางการบริหารความเสี่ยงแก่ กรรมการ ผู้บริหาร และพนักงานอย่างต่อเนื่อง
หน่วยงานเจ้าของความเสี่ยง (Risk Owner : RO)	- ระบุเหตุการณ์ที่เป็นความเสี่ยงที่อาจจะเกิดขึ้น ที่จะส่งผลกระทบต่อการดำเนินการให้บรรลุวัตถุประสงค์และเป้าหมาย ตามกลยุทธ์ทางธุรกิจที่ได้กำหนดไว้ - ประเมินโอกาสของการเกิดเหตุการณ์ที่เป็นความเสี่ยง รวมทั้งผลกระทบที่ได้รับ หากเกิดเหตุการณ์ดังกล่าว - พิจารณากำหนดวิธีการจัดการความเสี่ยง และดำเนินการในการตอบสนองต่อความเสี่ยง - รายงานให้ SD&RM ทราบ
<u>ติดตามตรวจสอบ</u> ***(3rd Line Roles)***	
คณะกรรมการตรวจสอบ (Audit Committee : AC)	- สอบทานประสิทธิภาพ และประสิทธิผลของการบริหารความเสี่ยงขององค์กร (Enterprise Risk Management) ตามการตวจสอบกฎบัตรคณะกรรมการตรวจสอบ - สอบทานระบบควบคุมภายใน และประสิทธิผลของการควบคุม - ติดตามการบริหารความเสี่ยงอย่างเป็นอิสระ - รายงานต่อคณะกรรมการบริษัทเกี่ยวกับประสิทธิภาพและประสิทธิผลของการควบคุมภายใน และการบริหารความเสี่ยงขององค์กร - สื่อสารกับคณะอนุกรรมการบริหารความเสี่ยง เพื่อให้เข้าใจความเสี่ยงที่สำคัญและเชื่อมโยงให้สอดคล้องกับการควบคุมภายใน
แผนกตรวจสอบภายใน (Internal Audit : IA)	- ตรวจสอบและสอบทานอย่างเป็นอิสระ เพื่อให้แน่ใจว่าการปฏิบัติงานเพื่อจัดการความเสี่ยงเป็นไปอย่างถูกต้อง ตรงตามนโยบาย แนวปฏิบัติ และมีประสิทธิภาพ - ให้คำแนะนำเพื่อการพัฒนาอย่างต่อเนื่อง - รายงานผลการตรวจสอบและสอบทานต่อ AC

บริษัทกำหนดให้ **CHANGE** เป็นวัฒนธรรมในการทำงานระดับบุคคล

Customer to centric	ลูกค้าเป็นศูนย์กลางในการดำเนินธุรกิจ
Honesty & integrity	ซื่อสัตย์ สุจริต มีจริยธรรม
Accountability & responsibility	ตระหนักในหน้าที่ และความรับผิดชอบ
Networking & collaboration	ประสานงาน สร้างเครือข่าย การทำงานร่วมกัน
Growth & innovation	เรียนรู้ สร้างคุณค่า พัฒนาสิ่งใหม่ ๆ
Excellence with promise	เป็นเลิศด้วยสัญญาของความสำเร็จตามเป้าหมาย

และบริหารองค์กรโดยใช้ข้อมูลเชิงประจักษ์ และการมีส่วนร่วม เป็นวัฒนธรรมระดับองค์ เพื่อให้เกิดเป็นพฤติกรรมการดำเนินงานที่สอดคล้องตามคุณค่าหลักขององค์กร ซึ่งได้แก่ มุ่งสร้างสรรค์นวัตกรรมที่ล้ำหน้า พัฒนาศักยภาพ ยกระดับความพึงพอใจในการให้บริการ และทำงานเป็นทีม

กำหนดให้นำ Objective and Key Result (OKR) มาใช้ในการกำหนดวัตถุประสงค์และเป้าหมายรายหน่วยงาน โดยต้องมีการประเมินในส่วนของความเสี่ยงและกำหนดแผนการจัดการกับความเสี่ยงนั้น ๆ

ผลของการบรรลุตามวัตถุประสงค์และเป้าหมายของ OKR มาประเมินผลสำเร็จของการปฏิบัติงานของหน่วยงานนั้น ๆ ตามเกณฑ์พิจารณาประเมินผลงานของบริษัท

2. กลยุทธ์ในการดำเนินธุรกิจ และการจัดการกับความเสี่ยง

SD&RM และหน่วยงานที่เกี่ยวข้องในกระบวนการบริหารความเสี่ยง ทำงานร่วมกันอย่างใกล้ชิด เพื่อติดตาม และสื่อสารแนวโน้มที่สำคัญที่อาจจะเกิดขึ้นในอนาคต และประเด็นความเสี่ยงขององค์กรทั้งภายใน ภายนอก ที่อาจส่งผลต่อการดำเนินธุรกิจหรือส่งผลต่อกลยุทธ์ขององค์กรทั้งในระยะสั้น ระยะกลาง และระยะยาว โดยการวิเคราะห์บริบทในการดำเนินธุรกิจ ด้วยการใช้เครื่องมือต่าง ๆ เข้ามาช่วยในการพิจารณาสภาพแวดล้อมในการดำเนินธุรกิจและผู้มีส่วนได้ส่วนเสีย ดังนี้

- ใช้เครื่องมือ SWOT วิเคราะห์ปัจจัยภายใน โดยพิจารณาจาก ทุน คน กระบวนการ และเทคโนโลยี
- ใช้เครื่องมือ PESTEL วิเคราะห์ปัจจัยภายนอก

กำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) เพื่อให้บรรลุตามวิสัยทัศน์ และพันธกิจ และกำหนดช่วงเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) เพื่อระบุระดับความเบี่ยงเบนจากการบรรลุวัตถุประสงค์ ซึ่งสามารถยอมรับได้

Risk Matrix

ผลกระทบ \ โอกาส	เกิดขึ้นยาก (1)	เกิดขึ้นน้อย (2)	เกิดขึ้นบ้าง (3)	เกิดขึ้นสูง (4)	เกิดขึ้นสูงมาก (5)
สูงมาก (5)	5	10	15	20	25
สูง (4)	4	8	12	16	20
ปานกลาง (3)	3	6	9	12	15
น้อย (2)	2	4	6	8	10
น้อยมาก (1)	1	2	3	4	5

ระดับการยอมรับ

ระดับความเสี่ยงที่ไม่สามารถยอมรับได้
ต้องมีมาตรการควบคุมความเสี่ยง
ยอมรับได้

	(1) ระดับความเสี่ยง	17-25	คะแนน (สูงมาก)	ต้องกำกับดูแลอย่างใกล้ชิด
	(2) ระดับความเสี่ยง	10-16	คะแนน (สูง)	ต้องเฝ้าระวัง
	(3) ระดับความเสี่ยง	6 - 9	คะแนน (ปานกลาง)	พอจะยอมรับได้ใช้วิธีควบคุมปกติ
	(4) ระดับความเสี่ยง	1 - 5	คะแนน (ต่ำ)	ไม่ต้องมีการควบคุม

กลยุทธ์ในการจัดการความเสี่ยง

การยอมรับความเสี่ยง (Accept)	ยอมรับความเสี่ยงที่เกิดจากการปฏิบัติงาน และมีระดับความเสี่ยงอยู่ในระดับที่ยอมรับได้
การลดความเสี่ยง (Reduce)	ดำเนินการเพิ่มเติมเพื่อลดโอกาสที่จะเกิด หรือลดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้
การแบ่งความเสี่ยง (Share)	การร่วมจัดการโดยแบ่งความเสี่ยงบางส่วนกับบุคคลหรือองค์กรอื่น
การหลีกเลี่ยงความเสี่ยง (Avoid)	การดาเนินการเพื่อยกเลิกหรือหลีกเลี่ยงกิจกรรมที่ก่อให้เกิดความเสี่ยง

3. ระบุประเด็นความเสี่ยง

ผู้บริหารและพนักงานทุกคนเป็นเจ้าของความเสี่ยง ระบุและประเมินความเสี่ยงของหน่วยงานที่รับผิดชอบ ที่จะส่งผลกระทบต่อการดำเนินการให้บรรลุกลยุทธ์และเป้าหมายทางธุรกิจที่ได้กำหนดไว้ อีกทั้งต้องพิจารณาถึงความเสี่ยงที่เกิดขึ้นใหม่ รวมถึงการเปลี่ยนแปลงในอนาคตอันเนื่องมาจากเทคโนโลยีใหม่ แนวโน้มการเปลี่ยนแปลงทางสังคม พฤติกรรมของผู้ใช้บริการ และการเปลี่ยนแปลงทางการเมืองประกอบด้วย เพื่อทำความเข้าใจความเสี่ยงที่มีอยู่เดิม ความเสี่ยงที่จะเกิดขึ้นใหม่ (Emerging Risk) รวมถึงกำหนดความหมายและขอบเขตของความเสี่ยงให้ชัดเจน ตามขั้นตอนการระบุประเด็นความเสี่ยงดังนี้

(1) SD&RM ร่วมกันระบุประเด็นความเสี่ยง รวมทั้งความความจำเป็นและความคาดหวังของผู้มีส่วนได้ส่วนเสีย ที่มีผลกระทบต่อความสามารถขององค์กรในการบรรลุตามวัตถุประสงค์ เป้าหมาย และกลยุทธ์ โดยพิจารณาจาก ประเด็นภายในประเด็นภายนอก กฎหมายและข้อกำหนดที่เกี่ยวข้อง

(2) แต่ละหน่วยงานพิจารณากำหนดประเด็นความเสี่ยงที่มีผลต่อความสามารถของหน่วยงานในการบรรลุตามเป้าหมายขององค์กร โดยพิจารณาจาก ประเด็นภายในและภายนอกที่เกี่ยวข้อง ปัญหาที่ส่งผลกระทบด้านสิ่งแวดล้อมที่สำคัญของกิจกรรมที่รับผิดชอบ และสาเหตุของการเกิดอันตราย(ความเสี่ยงอันตราย)ในการทำงานของพนักงาน

หมายเหตุ : อ้างอิงวิธีการปฏิบัติตามระเบียบปฏิบัติงาน P-002 , P-004 และ P-005

4. ประเมินและจัดลำดับความสำคัญความเสี่ยง

เมื่อกำหนดประเด็นความเสี่ยงได้จากขั้นตอนที่ 3 แล้ว ต้องทำความเข้าใจว่าประเด็นความเสี่ยงนั้น ๆ ส่งผลกระทบต่อความสามารถของบริษัทในการดำเนินธุรกิจให้บรรลุเป้าหมายอย่างไร รวมถึงกำหนดตัวแปรและสมมติฐานที่เกี่ยวข้อง เพื่อพิจารณาโอกาสที่จะเกิด (Likelihood) และ ความรุนแรงของผลกระทบ (Impact) ของเหตุการณ์ความเสี่ยงนั้น ๆ ดังนี้

<u>เกณฑ์การประเมินความเสี่ยง</u>

(1) ระดับโอกาสที่จะเกิดความเสี่ยง

โอกาสที่จะเกิด	ความหมาย	ระดับ
สูงมาก	มากกว่า 1 ครั้ง/เดือน	5
สูง	1-6 เดือนต่อครั้ง แต่ไม่เกิน 5 ครั้ง	4
ปานกลาง	1 ปีต่อครั้ง	3
น้อย	2-4 ปีต่อครั้ง	2
น้อยมาก	5 ปีต่อครั้ง	1

(2) ระดับความรุนแรงของผลกระทบ

ผลกระทบ	ความหมาย	ระดับ
สูงมาก	ส่งผลรุนแรงต่อบริษัท (กระทบชื่อเสียง/ภาพพจน์/ความสามารถในการแข่งขันอย่างรุนแรง)	5
สูง	ส่งผลกระทบอย่างมีนัยสำคัญ (กระทบชื่อเสียง/ภาพพจน์/ความสามารถในการแข่งขันอย่างมีนัยสำคัญ)	4
ปานกลาง	ส่งผลกระทบในระดับปานกลาง (กระทบชื่อเสียง/ภาพพจน์/ความสามารถในการแข่งขันในระดับปานกลาง)	3
น้อย	ส่งผลกระทบในระดับน้อยมาก/ควบคุมได้ (กระทบชื่อเสียง/เป็นข่าวที่เป็นที่สนใจของบุคคลทั่วไปน้อย รวมถึงกระทบความสามารถในการแข่งขันในระดับน้อยมาก)	2
น้อยมาก	ไม่ส่งผลกระทบต่อบริษัท (ไม่ส่งผลกระทบต่อชื่อเสียง/ภาพพจน์/ความสามารถในการแข่งขัน)	1

☐ **ผลกระทบด้านนโยบาย/เชิงปริมาณ**

ผลกระทบ	ความหมาย	ระดับ
สูงมาก	มากกว่า 10 ล้านบาท	5
สูง	มากกว่า 5 ล้านบาท – 9 ล้านบาท	4
ปานกลาง	1 ล้านบาท – 4 ล้านบาท	3
น้อย	1 แสนบาท – 9 แสนบาท	2
น้อยมาก	ไม่เกิน 1 แสนบาท	1

☐ **ผลกระทบต่อชื่อเสียง/ภาพลักษณ์องค์กร**

ผลกระทบ	ความหมาย	ระดับ
สูงมาก	มีการพาดหัวข่าวในทางเสื่อมเสียจนไม่สามารถแก้ข่าวได้	5
สูง	มีการเผยแพร่ข่าวในวงกว้างซึ่งต้องใช้เวลามากในการเผยแพร่ชี้แจง	4
ปานกลาง	มีการเผยแพร่ข่าวแต่สามารถแก้ไขข่าวได้ภายใน 1 – 3 วัน	3
น้อย	มีการเผยแพร่ข่าวในวงจำกัดสามารถแก้ไขข่าวได้ทันที	2
น้อยมาก	ไม่มีการเผยแพร่ข่าว	1

☐ **ผลกระทบต่อการดำเนินกิจการ**

ผลกระทบ	ความหมาย	ระดับ
สูงมาก	มีผลกระทบต่อกระบวนการและการดำเนินงานรุนแรงมาก เช่น หยุดดำเนินการมากกว่า 1 เดือน	5
สูง	มีผลกระทบต่อกระบวนการและการดำเนินงานรุนแรง เช่น หยุดดำเนินการ 1 เดือน	4
ปานกลาง	มีการชะงักงันอย่างมีนัยสำคัญของกระบวนการและการดำเนินงาน	3
น้อย	มีผลกระทบเล็กน้อยต่อกระบวนการและการดำเนินงาน	2
น้อยมาก	ไม่มีการชะงักงันของกระบวนการและการดำเนินงาน	1

☐ **ผลกระทบต่อบุคลากร**

ผลกระทบ	ความหมาย	ระดับ
สูงมาก	อันตรายต่อร่างกายถึงขั้นเสียชีวิต	5
สูง	อันตรายต่อร่างกายถึงขั้นบาดเจ็บสาหัส	4
ปานกลาง	อันตรายต่อร่างกายขั้นบาดเจ็บรักษาในโรงพยาบาล และหยุดงานมากกว่า 5 วัน	3
น้อย	อันตรายต่อร่างกายขั้นบาดเจ็บรักษาในโรงพยาบาล และหยุดงาน 1-5 วัน	2
น้อยมาก	อันตรายต่อร่างกายขั้นปฐมพยาบาลเบื้องต้น	1

☐ **ผลกระทบต่อผู้ใช้บริการ/ลูกค้า**

ผลกระทบ	ความหมาย	ระดับ
สูงมาก	ผู้รับบริการ/ลูกค้า ไม่พึงพอใจในบริการและ/หรือมีการร้องเรียนการดำเนินงานของบริษัท	5
สูง	ผู้รับบริการ/ลูกค้า ไม่พึงพอใจและไม่กลับมาใช้บริการซ้ำหรือซื้อขาย	4
ปานกลาง	ผู้รับบริการ/ลูกค้า แสดงความคิดเห็นในเชิงลบต่อการบริการ/การขาย	3
น้อย	ผู้รับบริการ/ลูกค้า ไม่พึงพอใจในการให้บริการ/การขาย	2
น้อยมาก	ผู้รับบริการ/ลูกค้า ไม่ได้รับบริการ การอำนวยความสะดวกภายใน	1

☐ **ผลกระทบต่อระบบเทคโนโลยีสารสนเทศ**

ผลกระทบ	ความหมาย	ระดับ
สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลที่สำคัญขององค์กร	5
สูง	เกิดปัญหากับระบบ IT ที่สำคัญและระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน	4
ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก	3
น้อย	เกิดเหตุที่แก้ไขได้และไม่มีความสูญเสีย	2
น้อยมาก	เกิดเหตุที่ไม่มีความสำคัญ	1

☐ **ผลกระทบต่อสิทธิมนุษยชน/คอร์รัปชั่น**

ผลกระทบ	ความหมาย	ระดับ
สูงมาก	มีผลกระทบ ไม่สามารถควบคุมได้ และทำให้องค์กรต้องปิดกิจการ	5
สูง	มีผลกระทบ ไม่สามารถควบคุมได้ และทำให้เสื่อมเสียชื่อเสียงขององค์กร	4
ปานกลาง	มีผลกระทบ ไม่สามารถควบคุมได้ และยังสามารถดำเนินกิจการได้	3
น้อย	มีผลกระทบ แต่สามารถควบคุมได้	2
น้อยมาก	ไม่มีผลกระทบโดยตรง	1

นำผลของการประเมินระดับโอกาสของการเกิดเกิด และระดับของผลกระทบของประเด็นความเสี่ยงนั้น ๆ มาจัดลำดับความสำคัญในตารางความสัมพันธ์ระหว่าง ระดับโอกาสของการเกิด และ ระดับของผลกระทบ (Risk Matrix) เพื่อพิจารณากำหนดวิธีการจัดการกับความเสี่ยงตามกลยุทธ์ในการจัดการความเสี่ยงแต่ละระดับดังนี้

ระดับความเสี่ยง	ระดับคะแนน	การยอมรับความเสี่ยง
สูงมาก	17-25	ยอมรับไม่ได้ ต้องมีการจัดการทันที เพื่อให้อยู่ในระดับที่ยอมรับได้
สูง	10-16	ยอมรับไม่ได้ โดยต้องมีการจัดการเพื่อให้อยู่ในระดับที่ยอมรับได้
ปานกลาง	6 - 9	ยอมรับได้ โดยต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
ต่ำ	1 – 5	ยอมรับได้ โดยไม่ต้องมีการควบคุม

5. ตอบสนองต่อความเสี่ยง

SD&RM / หน่วยงานเจ้าของความเสี่ยง เลือกวิธีตอบสนองต่อความเสี่ยง โดยพิจารณาจาก

1. บริบทในการดำเนินธุรกิจ
2. ต้นทุนและประโยชน์
3. ความสอดคล้องกับมาตรฐานที่เกี่ยวข้องในอุตสาหกรรมความคาดหวังของผู้มีส่วนได้เสียรวมถึงพันธกิจ วิสัยทัศน์ และ ค่านิยมองค์กร
4. จากระดับความเสี่ยงที่ยอมรับได้(Risk Appetite) และค่าความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance) ขององค์กร
   - **ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) หมายถึง** คือค่าความเสี่ยงโดยรวมที่องค์กรยินดีจะยอมรับเพื่อให้องค์กรบรรลุเป้าหมาย ซึ่งการกำหนด Risk Appetite นี้ ผู้รับผิดชอบต้องคำนึงถึงผลที่สอดคล้องกับระเบียบ ข้อบังคับ หรือเป้าหมายที่ต้องการทำให้บรรลุผลในระยะยาว
   - **ค่าความเบี่ยงเบนที่ยอมรับได้(Risk Tolerance) หมายถึง** ระดับความเบี่ยงเบนจากเกณฑ์ที่ทำให้องค์กรมั่นใจว่าองค์กรได้ดำเนินการบริหารความเสี่ยงอยู่ภายในเกณฑ์ที่ยอมรับได้ โดยการเบี่ยงเบนที่รับได้นั้นอยู่ในระดับที่สามารถทำให้บรรลุเป้าหมาย สอดคล้องกับ Risk Appetite ที่ตั้งขึ้น
5. กำหนดแผนงานจัดการความเสี่ยงตามกลยุทธ์ในการจัดการความเสี่ยง ได้แก่ การยอมรับความเสี่ยง การลดความรุนแรงของความเสี่ยง การแบ่งปันความเสี่ยง และการหลีกเลี่ยงความเสี่ยง

แผนงานในการจัดการความเสี่ยงจะมีการนำเสนอต่อที่ประชุม Management Review เพื่อพิจารณา และขออนุมัติการจัดสรรทรัพยากรที่จำเป็นต้องใช้ดำเนินการ (ถ้ามี) โดยในการคัดเลือกแนวทางในการจัดการความเสี่ยงที่เหมาะสมที่สุด จะคำนึงถึงความเสี่ยงที่มีค่าความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance) กับต้นทุนที่เกิดขึ้นเปรียบเทียบกับประโยชน์ที่จะได้รับ รวมถึงข้อกฎหมายและข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง รวมทั้งความรับผิดชอบที่มีต่อสังคม

6. กำหนดกิจกรรมควบคุม

เมื่อกำหนดวิธีตอบสนองความเสี่ยงแล้ว เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยงให้อยู่ในระดับที่สามารถยอมรับได้ และป้องกันไม่ให้เกิดผลกระทบต่อเป้าหมายขององค์กร จึงได้กำหนดกิจกรรมการควบคุมแบ่งได้เป็น 4 ประเภท คือ

1. การควบคุมเพื่อการป้องกัน (Preventive Control)
2. การควบคุมเพื่อให้ตรวจพบ (Detective Control)
3. การควบคุมโดยการชี้แนะ (Directive Control)
4. การควบคุมเพื่อการแก้ไข (Corrective Control)

โดยกิจกรรมการควบคุมมีองค์ประกอบดังนี้

- กำหนดวิธีการดำเนินงาน (ขั้นตอน, กระบวนการ)
- กำหนดบุคลากรภายในองค์กรเพื่อรับผิดชอบการควบคุมนั้น ได้แก่ SD&RM

- กำหนดระยะเวลาแล้วเสร็จของงาน

7. ติดตาม ทบทวน ปรับปรุง และรายงาน

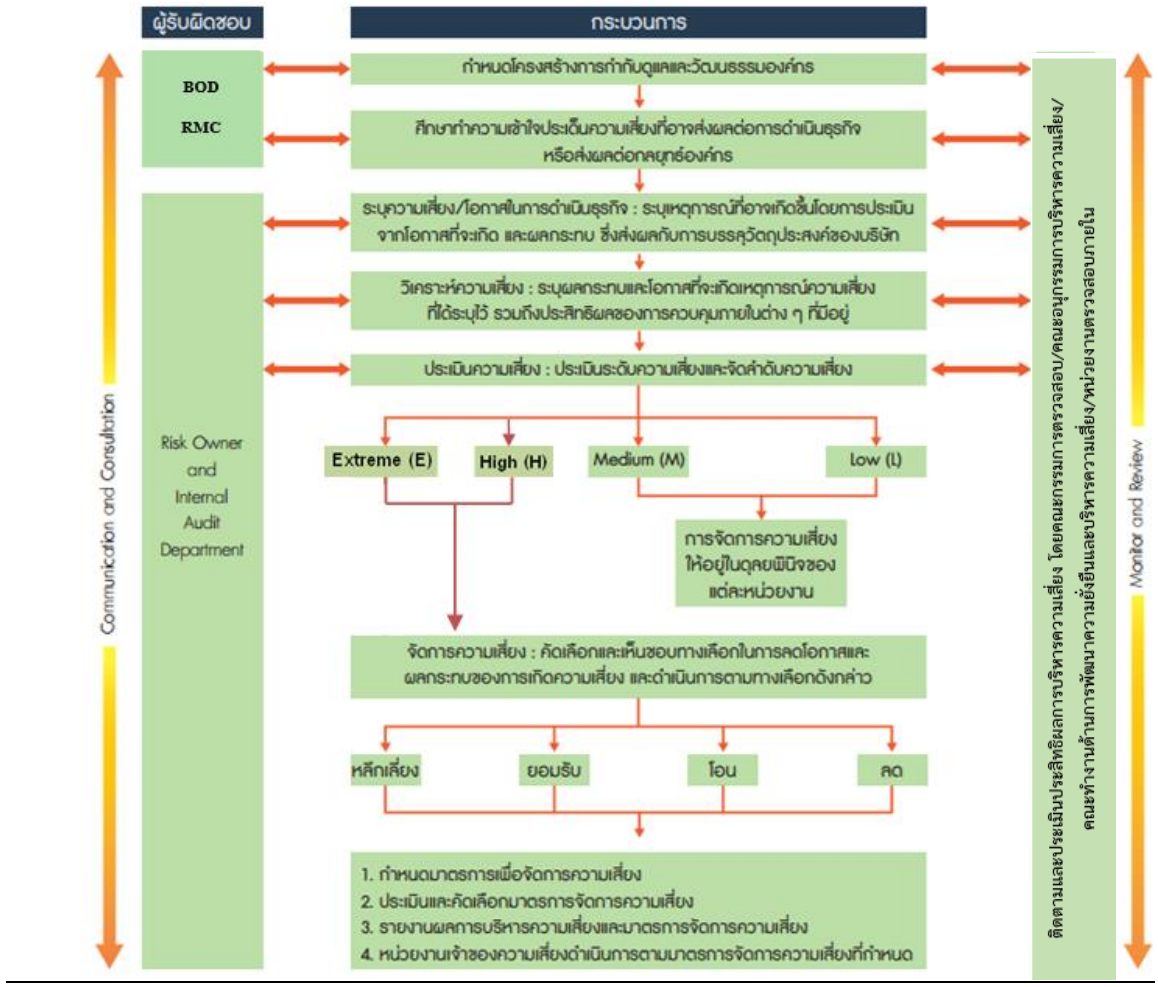
ดำเนินการติดตามประสิทธิผลการจัดการความเสี่ยงอย่างสม่ำเสมอ และทบทวน ปรับปรุง เพื่อสร้างความมั่นใจว่าการบริหารจัดการความเสี่ยงขององค์กรครอบคลุมประเด็นต่าง ๆ อย่างครบถ้วน และมีประสิทธิภาพ สอดคล้องกับการเปลี่ยนแปลงของธุรกิจรวมไปถึงเฝ้าระวัง และติดตามให้มีการดำเนินการตามกิจกรรมควบคุมที่ได้กำหนดไว้ อย่างเหมาะสม

- หน่วยงานเจ้าของความเสี่ยงรายงานผลการดำเนินงานตามแผนการจัดการความเสี่ยงทุก 3 เดือน ในการประชุม Management Review
- คณะกรรมการตรวจประเมินภายใน (Internal Auditor) รับผิดชอบในการตรวจติดตามอย่างน้อยปีละ 2 ครั้ง และรายงานผลการตรวจติดตามให้ SD&RM ทราบ เพื่อทบทวน และรายงานผลให้ RMC ทราบต่อไป
- แผนกตรวจสอบภายใน ทำการสอบทานประสิทธิภาพของการจัดการกับความเสี่ยงที่อยู่ในระดับที่ยอมรับไม่ได้ และรายงานต่อ AC
- RMC ทบทวนประสิทธิภาพในการจัดการความเสี่ยง ให้ที่ประชุม BOD เพื่อทราบ/พิจารณาต่อไป

8. สื่อสารและเปิดเผยประเด็นความเสี่ยง

จัดให้มีการสื่อสารความเสี่ยง แนวทางการจัดการ และผลการบริหารจัดการให้ผู้มีส่วนได้เสียทั้งภายใน และภายนอกรับทราบ ผ่านช่องทางการสื่อสารต่าง ๆ ขององค์กร เนื่องจากความเสี่ยงถือเป็นข้อมูลสำคัญสำหรับการทำกลยุทธ์ การปฏิบัติงาน และการตัดสินใจลงทุน รวมถึง เป็นการสร้างความตระหนักรู้ให้กับทุกคนในองค์กร ตลอดจนสร้างความเชื่อมั่น ในประสิทธิภาพของระบบการบริหารจัดการความเสี่ยงขององค์กร

แผนภาพระบบการบริหารความเสี่ยง



หมายเหตุ : RMC หมายถึง คณะอนุกรรมการบริหารความเสี่ยง

กรอบการบริหารความเสี่ยงขององค์กรฉบับนี้ ได้รับอนุมัติจากที่ประชุมคณะอนุกรรมการบริหารความเสี่ยง ครั้งที่ 1/2568 เมื่อวันที่ 14 พฤษภาคม 2568 และมีผลบังคับใช้ตั้งแต่ วันที่ 15 พฤษภาคม 2568

ลงชื่อ .....

(นายศักดิ์ชาย วงศ์ชัยสุริยะ)

ประธานคณะอนุกรรมการบริหารความเสี่ยง

ลงชื่อ .....

(นายประยุทธ วิบูลย์ศิริชัย)

อนุกรรมการบริหารความเสี่ยง

ลงชื่อ .....

(นายวันชัย เหลืองวิริยะ)

อนุกรรมการบริหารความเสี่ยง