นโยบายการบริหารความเสี่ยงองค์กร
(Enterprise Risk Management Policy : ERM)
บริษัท ไอร่า แฟคตอริ่ง จำกัด (มหาชน)

สารบัญ

ส่วนที่ 1 : บทนำ

1.1 **หลักการและเหตุผล**

การเปลี่ยนแปลงสภาพแวดล้อมในการดำเนินงานขององค์กร ทั้งปัจจัยภายใน อาทิ การปรับเปลี่ยนพันธกิจ กลยุทธ์ โครงสร้าง การบริหารทรัพยากรภายใน รวมถึงปัจจัยภายนอก อาทิ การเปลี่ยนแปลงของนโยบายภาครัฐ กฎ ระเบียบ หลักเกณฑ์ ข้อบังคับของหน่วยงานกำกับ หรือ สภาพแวดล้อมทางสังคม เศรษฐกิจ การเมือง ซึ่งมีการปรับเปลี่ยนจนอาจส่งผลกระทบให้การดำเนินงานขององค์กรไม่เป็นไปตามเป้าหมายตามที่กำหนดไว้ในแผนยุทธศาสตร์หรือแผนธุรกิจประจำปี ซึ่งก่อให้เกิดความเสี่ยงต่อองค์กรในภาพรวม ดังนั้น การบริหารความเสี่ยงจึงมีความจำเป็นและเป็นองค์ประกอบหนึ่งที่สำคัญในการบริหารจัดการองค์กรเชิงบูรณาการและการกำกับดูแลกิจการที่ดี ซึ่งนอกจากจะช่วยทำให้องค์กรบรรลุผลตามเป้าหมายแล้ว ยังอาจเป็นส่วนสนับสนุนให้เกิดการสร้างมูลค่าเพิ่มให้กับองค์กรและผู้มีส่วนได้ส่วนเสียอีกทางหนึ่ง บริษัท ไอร่า แฟคตอริ่ง จำกัด (มหาชน) จึงได้นำกรอบการบริหารความเชิงบูรณาการ (Enterprise Risk Management Integrate Framework) ตามแนวทาง COSO ERM มาประยุกต์ใช้เป็นแนวทางในการบริหารความเสี่ยงองค์กร เพื่อให้ผู้บริหารและบุคลากรภายในองค์กรตระหนักถึงความสำคัญของการบริหารความเสี่ยงและมีความเข้าใจตรงกันในคำนิยาม เป้าหมาย และ วัตถุประสงค์ อันจะเป็นการสร้างความรับผิดชอบอย่างทั่วถึงและเป็นไปในทิศทางเดียวกันทั่วทั้งองค์กรได้อย่างมีประสิทธิภาพ

1.2 **วัตถุประสงค์**

1.2.1 เพื่อเป็นกรอบการบริหารความเสี่ยงขององค์กร และเป็นแนวปฏิบัติสำหรับการจัดทำแผนบริหารความเสี่ยงขององค์กร โดยเป็นไปตามมาตรฐานการบริหารความเสี่ยงระดับสากล ซึ่งจะทำให้สามารถจัดการความเสี่ยงได้อย่างเหมาะสม และบรรลุเป้าหมายองค์กร

1.2.2 เพื่อเป็นแนวทางการบริหารความเสี่ยงที่ดีให้กับการกำกับดูแล และการกำหนดกระบวนการบริหารความเสี่ยงอื่นๆ ขององค์กรให้เป็นมาตรฐาน

1.3 **ขอบเขต**

นโยบายฉบับนี้ จัดทำขึ้นเพื่อใช้เป็นแนวทางในการบริหารความเสี่ยงองค์กรของบริษัท ไอร่า แฟคตอริ่ง จำกัด (มหาชน) โดยมีการกำหนดบทบาท หน้าที่ และความรับผิดชอบของคณะกรรมการฯ และหน่วยงานต่างๆ ที่เกี่ยวข้องกับความเสี่ยงองค์กร รวมถึงกำหนดแนวทางการประเมิน ควบคุม ติดตาม และการรายงานความเสี่ยงองค์กรตามกรอบแนวทางบริหารความเสี่ยงองค์กรที่เป็นมาตรฐานสากล

1.4 **คำจำกัดความ**

1.4.1 ความเสี่ยง (Risk) หมายความว่า ความเป็นไปได้ของเหตุการณ์ที่อาจเกิดขึ้นและเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ขององค์กร

1.4.2 การบริหารจัดการความเสี่ยง หมายความว่า กระบวนการบริหารจัดการเหตุการณ์ที่อาจเกิดขึ้น และส่งผลกระทบต่อองค์กร เพื่อให้สามารถดำเนินงานให้บรรลุวัตถุประสงค์ขององค์กร รวมถึงเพื่อเพิ่มศักยภาพ และขีดความสามารถให้องค์กร

1.4.3 การบริหารจัดการความเสี่ยงองค์กร (Enterprise Risk Management) หมายความว่า การบริหารความเสี่ยงโดยมีแนวทางในการบริหารความเสี่ยงแบบบูรณาการ ซึ่งจะครอบคลุมความเสี่ยงทั้งหมดที่องค์กรต้องเผชิญ จะมีการกระทำอย่างต่อเนื่อง เพื่อลดโอกาสและผลกระทบที่อาจเกิดขึ้นกับองค์กรให้อยู่ในระดับที่องค์กรยอมรับได้ โดยได้รับการสนับสนุน และการมีส่วนร่วมในการบริหารความเสี่ยงจากหน่วยงานทุกระดับในองค์กร

1.4.4 ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite : RA) หมายความว่า ระดับความเสี่ยงที่องค์กรจะยอมรับได้ โดยที่องค์กรยังสามารถดำเนินงานให้บรรลุเป้าหมายที่ได้กำหนดไว้

1.4.5 ระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance : RT) หมายความว่า ระดับความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ ซึ่งทำให้องค์กรมั่นใจได้ว่าองค์กรได้ดำเนินการบริหารความเสี่ยงอยู่ภายในเกณฑ์ที่ยอมรับได้

1.4.6 หน่วยงานเจ้าของความเสี่ยง (Risk Owner) หมายความว่า หน่วยงานที่ทำให้เกิดความเสี่ยง หรือหน่วยงานที่ได้รับผลกระทบโดยตรงจากความเสี่ยงที่ถูกระบุขึ้น และเป็นผู้ประเมินความเสี่ยง จัดทำแผนบริหารความเสี่ยง และให้ข้อเสนอแนะ รวมทั้งติดตามประเมินผลการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อให้ผลการบริหารความเสี่ยงบรรลุเป้าหมายที่ตั้งไว้

ส่วนที่ 2 : บทบาทหน้าที่ของคณะกรรมการและหน่วยงานที่เกี่ยวข้อง

2.1 การกำหนดบทบาท และแบ่งแยกหน้าที่

องค์กรได้มีการจัดโครงสร้างองค์กรที่สนับสนุนการควบคุมภายใน และส่งเสริมให้เกิดการบริหารความเสี่ยงอย่างมีประสิทธิภาพ โดยมีการแบ่งแยกสายการบังคับบัญชา และหน่วยงานในการบริหารความเสี่ยงที่ทำหน้าที่ในการวัด ติดตาม และควบคุมความเสี่ยง ออกจากหน่วยงานที่ก่อให้เกิดความเสี่ยง โดยมีการกำกับดูแลโดยคณะกรรมการที่ได้รับมอบหมาย

2.2 บทบาทหน้าที่ของคณะกรรมการและหน่วยงานที่เกี่ยวข้อง

องค์กรได้จัดให้มีการกำหนด และแบ่งแยกภาระหน้าที่ของคณะกรรมการ และหน่วยงานต่างๆ ในองค์กรอย่างชัดเจนเป็นลายลักษณ์อักษร และประกาศให้ทราบอย่างทั่วถึงภายในองค์กร โดยได้มีการกำหนดภาระหน้าที่ของคณะกรรมการ และหน่วยงานที่เกี่ยวข้องกับการก่อให้เกิดความเสี่ยง และการบริหารจัดการความเสี่ยง

2.2.1 บทบาทหน้าที่ของคณะกรรมการที่เกี่ยวข้อง

สรุปภาระหน้าที่หลักที่เกี่ยวข้องของคณะกรรมการต่างๆ ดังนี้

1) คณะกรรมการบริษัท

- กำหนดนโยบาย เป้าหมาย แนวทาง ทิศทาง กลยุทธ และงบประมาณของบริษัท ตลอดจนควบคุมกำกับ ดูแลการบริหารและจัดการของคณะกรรมการชุดย่อยให้เป็นไปตามนโยบายที่ได้รับมอบหมาย

- มีอำนาจหน้าที่สอบทานความเพียงพอและความเหมาะสมของระบบควบคุมภายในและการบริหารความเสี่ยงของบริษัท

2) คณะกรรมการตรวจสอบ

- สอบทานให้บริษัทมีการรายงานทางการเงินอย่างถูกต้องและเพียงพอ

- สอบทานให้บริษัทมีระบบการควบคุมภายใน (Internal Control) การบริหารความเสี่ยง (Risk Management) และการตรวจสอบภายใน (Internal Audit) ที่เหมาะสมและมีประสิทธิผล

3) คณะกรรมการสินเชื่อ

- ให้คำปรึกษาหรือแนะนำการบริหารความเสี่ยงด้านสินเชื่อแก่ฝ่ายจัดการ เพื่อประโยชน์ในการสร้างฐานลูกค้าและลูกหนี้ที่มีคุณภาพของบริษัท

4) คณะอนุกรรมการบริหารความเสี่ยง

- กำหนดแนวทางและเครื่องมือการบริหารความเสี่ยง ให้สอดคล้องกับกรอบการกำกับดูแลความเสี่ยงของบริษัท

- พิจารณากลั่นกรองนโยบาย และแนวทางการบริหารความเสี่ยงของบริษัท ซึ่งต้องครอบคลุมถึงความเสี่ยงประเภทต่างๆ ที่สำคัญ

- ควบคุมดูแลให้บริษัทมีการบริหารความเสี่ยงตามนโยบายและกลยุทธ์การบริหารความเสี่ยง

- ทบทวนความเพียงพอของนโยบายและระบบการบริหารความเสี่ยง โดยรวมถึงความมีประสิทธิผลของระบบการปฏิบัติตามนโยบายที่กำหนด

5) คณะจัดการ

มีหน้าที่ในการติดตามการดำเนินการตามแผนบริหารความเสี่ยงองค์กร โดยมอบหมายความรับผิดชอบไปยังหน่วยงานเจ้าของความเสี่ยง (Risk owner)

2.2.2 **บทบาทหน้าที่ของหน่วยงานที่เกี่ยวข้อง**

1) หน่วยงานเจ้าของความเสี่ยง (Risk Owner)

รับผิดชอบในการประเมินและวิเคราะห์ความเสี่ยง กำหนดมาตรการ/กิจกรรมที่ใช้ในการจัดการความเสี่ยง วิเคราะห์ Cost - Benefit ของแต่ละทางเลือก ติดตามผลการประเมินความเสี่ยง

2) หน่วยงานบริหารความเสี่ยง

พัฒนาระบบบริหารความเสี่ยงให้มีประสิทธิภาพ ประสิทธิผล ติดตามผลการบริหารความเสี่ยงจาก Risk Owners เพื่อจัดทำรายงานความเสี่ยงเสนอฝ่ายจัดการ คณะอนุกรรมการบริหารความเสี่ยง คณะกรรมการตรวจสอบ และคณะกรรมการบริษัท

3) ฝ่ายตรวจสอบภายใน

มีหน้าที่ในการตรวจสอบและสอบทานกระบวนการปฏิบัติงานว่าเป็นไปตามนโยบาย ระเบียบปฏิบัติ เพื่อให้มั่นใจการควบคุมภายใน/การจัดการความเสี่ยงที่เพียงพอและเหมาะสม และรายงานต่อคณะกรรมการตรวจสอบ

ส่วนที่ 3 : เนื้อหานโยบาย

การบริหารจัดการความเสี่ยงองค์กร อ้างอิงตามแนวทาง COSO ERM เพื่อให้องค์กรมีการบริหารความเสี่ยงทั่วทั้งองค์กรแบบบูรณาการ และสามารถปฏิบัติได้ โดยให้ทุกหน่วยงานในองค์กรตระหนักถึงความสำคัญของการบริหารความเสี่ยง และการพัฒนาระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ เพื่อสนับสนุนการบริหารความเสี่ยง และนำมาใช้ในการบริหารจัดการ

3.1 **หลักการบริหารจัดการความเสี่ยงองค์กร**

3.1.1 มุ่งเน้นการบริหารความเสี่ยงที่มีผลกระทบต่อยุทธศาสตร์ การบรรลุวัตถุประสงค์และเป้าหมายหลักขององค์กร

3.1.2 พัฒนาการบริหารความเสี่ยง และการควบคุมภายในให้มีความเหมาะสม และพร้อมรับกับสถานการณ์การดำเนินปกติ และสถานการณ์พิเศษ หรือฉุกเฉิน

3.1.3 การบริหารความเสี่ยงเป็นหนึ่งในวัฒนธรรมที่สำคัญขององค์กร ที่จำเป็นต้องดำเนินการอย่างมีประสิทธิภาพ และประสิทธิผล โดยผู้บริหาร และบุคลากรทุกคนในองค์กรเป็นเจ้าของความเสี่ยง (Risk Owner) มีหน้าที่รับผิดชอบในการปฏิบัติตามนโยบายการบริหารความเสี่ยง

3.1.4 ให้ความสำคัญกับการพัฒนาระบบเทคโนโลยีที่สนับสนุนการบริหารความเสี่ยงองค์กร และการนำเทคโนโลยีมาปรับใช้กับการดำเนินงานขององค์กร

3.2 **การบริหารจัดการความเสี่ยงขององค์กรตามหลักมาตรฐาน COSO ERM**

ในการบริหารจัดการความเสี่ยงองค์กร องค์กรได้นำกรอบการบริหารความเสี่ยงตามหลักมาตรฐาน COSO ซึ่งเป็นหลักการที่มีการยอมรับให้เป็นแนวปฏิบัติสากล ทั้งนี้ จะต้องมีการบูรณาการบริหารความเสี่ยงองค์กรนี้กับการวางแผนยุทธศาสตร์ และการปฏิบัติงาน เนื่องจากความเสี่ยงมีผลกระทบต่อยุทธศาสตร์ และการปฏิบัติงานขององค์กร โดยมีการแบ่งองค์ประกอบออกเป็น 5 ส่วนที่สัมพันธ์กัน ซึ่งในแต่ละส่วนประกอบด้วย ชุดของหลักการที่จะทำให้องค์กรมีความเข้าใจ และมีความพยายามในการบริหารความเสี่ยงที่เกี่ยวข้องกับยุทธศาสตร์ และวัตถุประสงค์ทางธุรกิจขององค์กร

3.2.1 การกำกับ และดูแลวัฒนธรรม (Governance and Culture) การกำกับดูแลกำหนดท่าทีขององค์กร เสริมสร้างความสำคัญ รวมทั้งกำหนดความรับผิดชอบในการควบคุม ดูแล สำหรับการบริหารความเสี่ยงขององค์กร วัฒนธรรมเกี่ยวข้องกับคุณค่าทางจริยธรรม พฤติกรรมที่พึงประสงค์ และความเข้าใจในความเสี่ยงของกิจการ ประกอบด้วยหลักการย่อย ดังนี้

1) ควบคุมดูแลความเสี่ยงโดยคณะกรรมการ
2) จัดตั้งโครงสร้างการดำเนินงาน
3) กำหนดวัฒนธรรมที่พึงประสงค์
4) แสดงให้เห็นถึงการยึดมั่นต่อคุณค่าหลัก
5) ดึงดูด พัฒนา และรักษาบุคคลที่มีความสามารถ

3.2.2 กลยุทธ์ และการกำหนดวัตถุประสงค์ (Strategy and Objective Setting) กระบวนการวางแผนกลยุทธ์เป็นการทำงานร่วมกันของการบริหารความเสี่ยงขององค์กร กลยุทธ์ และการกำหนดวัตถุประสงค์ องค์กรกำหนดระดับความเสี่ยงที่ยอมรับได้ให้สอดคล้องกับกลยุทธ์ วัตถุประสงค์ทางธุรกิจทำให้เกิดการดำเนินการตามกลยุทธ์ ในขณะเดียวกันก็ใช้เป็นเกณฑ์ในการระบุ ประเมิน และตอบสนองความเสี่ยง ประกอบด้วยหลักการย่อย ดังนี้

1) วิเคราะห์บริบททางธุรกิจ
2) กำหนดระดับความเสี่ยงที่ยอมรับได้
3) ประเมินกลยุทธ์ทางเลือก
4) กำหนดวัตถุประสงค์ทางธุรกิจ

3.2.3 ผลการปฏิบัติงาน (Performance) ความเสี่ยงที่อาจมีผลกระทบต่อความสำเร็จของกลยุทธ์ และวัตถุประสงค์ทางธุรกิจจำเป็นต่อถูกระบุ และประเมิน ความเสี่ยงจะถูกจัดลำดับความสำคัญตามความรุนแรงในบริบทของระดับความเสี่ยงที่ยอมรับได้ ต่อจากนั้น องค์กรจึงคัดเลือกวิธีการตอบสนองความเสี่ยง และพิจารณาภาพรวมของค่าความเสี่ยงที่องค์กรรับไว้ ผลของกระบวนการข้างต้นนี้จะรายงานต่อผู้มีส่วนได้เสียสำคัญของความเสี่ยง

1) ระบุความเสี่ยง
2) ประเมินความรุนแรงของความเสี่ยง
3) จัดลำดับความสำคัญของความเสี่ยง
4) นำวิธีการตอบสนองความเสี่ยงไปปฏิบัติ
5) พัฒนาภาพรวมความเสี่ยง

3.2.4 การสอบทาน และการแก้ไขปรับปรุง (Review and Revision) โดยการสอบทานผลการปฏิบัติงานของกิจการ องค์กรจะสามารถพิจารณาได้ว่าองค์ประกอบของการบริหารความเสี่ยงขององค์กรมีประสิทธิภาพในการบริหารความเสี่ยงในช่วงที่ผ่านมา และเมื่อเกิดการเปลี่ยนแปลงที่สำคัญ รวมทั้งมีสิ่งที่จำเป็นต้องมีการแก้ไขปรับปรุง

1) ประเมินการเปลี่ยนแปลงที่สำคัญ
2) สอบทานความเสี่ยง และผลการปฏิบัติงาน
3) พยายามปรับปรุงการบริหารความเสี่ยงขององค์กรอย่างต่อเนื่อง

3.2.5 สารสนเทศ การสื่อสาร และการรายงาน (Information, Communication and Reporting) การบริหารความเสี่ยงขององค์กรจำเป็นต้องมีกระบวนการที่ต่อเนื่อง เพื่อการได้มา และการใช้สารสนเทศที่จำเป็นร่วมกัน ทั้งสารสนเทศจากแหล่งภายใน และภายนอกซึ่งไหลเวียนอยู่ทั่วองค์กร

1) ใช้ประโยชน์จากสารสนเทศ และเทคโนโลยี
2) สื่อสารสารสนเทศด้านความเสี่ยง
3) รายงานความเสี่ยง วัฒนธรรม และผลการปฏิบัติงาน

3.3 **ประเภทความเสี่ยง**

องค์กรมีการกำหนดประเภทความเสี่ยงที่มีนัยสำคัญออกเป็น 4 ความเสี่ยงหลัก (S-O-F-C) ได้แก่

3.3.1 ความเสี่ยงด้านกลยุทธ์ (Strategic Risk: S) คือ ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ แผนดำเนินงาน และการนำไปปฏิบัติไม่เหมาะสม หรือไม่สอดคล้องกับปัจจัยภายใน และสภาพแวดล้อมภายนอก จนส่งผลกระทบต่อรายได้ และการดำรงอยู่ของกิจการ หรือเป็นการพิจารณาว่าสิ่งที่องค์กรทำอยู่ หรือมีผลต่อความอยู่รอดเจริญเติบโตอย่างมั่นคงแข็งแรง

3.3.2 ความเสี่ยงด้านปฏิบัติการ (Operational Risk: O) คือ ความเสี่ยงที่จะเกิดความเสียหายอันเนื่องมาจากการขาดการกำกับดูแลกิจการที่ดี หรือขาดธรรมาภิบาลในองค์กร และการขาดการควบคุมที่ดีโดยเกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน คน ระบบงาน หรือเหตุการณ์ภายนอก และส่งผลกระทบต่อการดำเนินงานขององค์กร

นอกจากนี้ ความเสี่ยงด้านการทุจริต (Fraud Risk) ได้มีความสำคัญเพิ่มมากขึ้น โดยสามารถพิจารณาได้จากความโปร่งใสของการใช้อำนาจหน้าที่ การเอื้อประโยชน์ให้แก่ตนเอง หรือพวกพ้อง และการบริหารจัดการต่างๆ รวมทั้งแนวโน้มการพึ่งพาและใช้ระบบเทคโนโลยีสารสนเทศในองค์กร จะส่งผลให้ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (IT Risk) มีบทบาทสำคัญมากขึ้น ทั้งในด้านของความพร้อมใช้งาน การรักษาความมั่นคงปลอดภัย และความถูกต้องน่าเชื่อถือของข้อมูล

3.3.3 ความเสี่ยงด้านการเงิน (Financial Risk: F) คือ ความเสี่ยงที่เกิดจากการบริหารจัดการด้านการเงินขององค์กร และส่งผลกระทบต่อผลการดำเนินงานด้านการเงินขององค์กร (รายได้ ค่าใช้จ่าย กำไรสุทธิ) ประกอบด้วย ความเสี่ยงด้านเครดิต ความเสี่ยงด้านสภาพคล่อง และความเสี่ยงด้านตลาด

3.3.4 ความเสี่ยงด้านการปฏิบัติตามกฎเกณฑ์ (Compliance Risk: C) คือ ความเสี่ยงที่เกิดจากการฝ่าฝืน หรือไม่สามารถปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หรือมาตรฐานที่เกี่ยวข้องกับการดำเนินงาน หรือรวมทั้งไม่สามารถปฏิบัติตามนโยบาย และวิธีการปฏิบัติงานที่องค์กรได้กำหนดขึ้น รวมถึงความเสี่ยงที่เกิดขึ้นจากการขาดการกำกับดูแลกิจการที่ดี ขาดธรรมาภิบาลในองค์กร

องค์กรได้จัดให้มีกลไกการบริหารความจัดการความเสี่ยงที่เหมาะสมกับลักษณะความเสี่ยง ในแต่ละประเภท และสอดคล้องกับกรอบการบริหารจัดการความเสี่ยงองค์กรในภาพรวม

3.4 **กระบวนการบริหารจัดการความเสี่ยงองค์กร**

องค์กรได้กำหนดขั้นตอนกระบวนการบริหารความเสี่ยงองค์กรออกเป็น 6 ขั้นตอน เพื่อบริหารความเสี่ยงขององค์กรอย่างเป็นระบบ ตั้งแต่การกำหนดทิศทางการดำเนินงาน การระบุความเสี่ยง การประเมินความเสี่ยง การตอบสนองต่อความเสี่ยง การติดตาม และรายงานความเสี่ยง และการสื่อสาร และส่งเสริมวัฒนธรรมความเสี่ยง ซึ่งจะเป็นขั้นตอนที่เป็นวัฏจักรที่ต้องดำเนินการอย่างต่อเนื่อง และมีความเชื่อมโยง เพื่อให้องค์กรสามารถตัดสินใจ และตอบสนองต่อความเสี่ยง และโอกาสได้อย่างทันการณ์

1) การกำหนดทิศทางการดำเนินงานขององค์กร

ขั้นตอนการกำหนดทิศทางการดำเนินงานขององค์กรเป็นขั้นตอนการรวบรวม และวิเคราะห์บริบท และสภาพแวดล้อมทั้งจากภายใน และภายนอก การประเมินโครงสร้างองค์กร และนโยบาย หรือกลไกการบริหารความเสี่ยงในปัจจุบันขององค์กร และระบุวัตถุประสงค์ หรือขอบเขตในการบริหารความเสี่ยงในภาพรวม

ทั้งนี้ แผนยุทธศาสตร์องค์กร วัตถุประสงค์ และเป้าหมายองค์กรจะเป็นตัวขับเคลื่อนการบริหารความเสี่ยงขององค์กร ซึ่งส่งผลกระทบต่อการกำหนดระดับความเสี่ยงที่ยอมรับได้ และระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ ไปถึงการระบุความเสี่ยง ปัจจัยเสี่ยง และสาเหตุความเสี่ยง และวิธีการจัดการความเสี่ยง องค์กรสามารถเข้าใจถึงความเสี่ยงที่ผลกระทบต่อวัตถุประสงค์ทางธุรกิจ และแผนยุทธศาสตร์องค์กร ระดับความเสี่ยงที่องค์กรได้รับจากการดำเนินการทางธุรกิจ และผลตอบแทนที่คาดว่าจะได้รับจากการลงทุนหลังจากที่ได้ปรับความเสี่ยง

2) การระบุความเสี่ยง

ขั้นตอนระบุความเสี่ยงเป็นขั้นตอนที่สำคัญ โดยจะทำการวิเคราะห์สภาพแวดล้อมภายนอกองค์กร ปัจจัยภายในองค์กร กลยุทธ์ หรือยุทธศาสตร์ขององค์กร เพื่อระบุปัจจัยเสี่ยงที่จะส่งผลกระทบต่อการดำเนินงาน หรือเป้าหมายขององค์กร รวมทั้งการวิเคราะห์ถึงสาเหตุของความเสี่ยง และความสัมพันธ์ต่อปัจจัยเสี่ยง และต้องมีการพิจารณาปัจจัยเสี่ยงระดับองค์กรของแต่ละความเสี่ยงให้ครบถ้วน

3) การประเมินระดับความเสี่ยง

ขั้นตอนการประเมินระดับความเสี่ยง เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยง โดยการพิจารณาผ่านเกณฑ์การประเมิน 2 เกณฑ์ คือ

3.1.1) การประเมินระดับความเสี่ยงที่ยอมรับได้ และความเสี่ยงที่ยอมให้เบี่ยงเบนได้โดยเชื่อมโยงกับวัตถุประสงค์ และเป้าหมายขององค์กร

3.1.2) การประเมินความเป็นไปได้ที่ความเสี่ยง หรือเหตุการณ์จะเกิดขึ้นในช่วงเวลาหนึ่ง (Likelihood) และผลกระทบของความเสี่ยงอาจจะเกิดขึ้น (Impact) เพื่อให้สามารถประเมินความรุนแรงของความเสี่ยงซึ่งถือว่าเป็นความเสี่ยงตั้งต้น (Inherent Risk)

4) การตอบสนองต่อความเสี่ยง

4.1) ขั้นตอนการตอบสนองต่อความเสี่ยงจะพิจารณาผลการประเมิน และจัดลำดับความสำคัญของปัจจัยเสี่ยง เพื่อกำหนดแนวทางการควบคุม หรือจัดการความเสี่ยง องค์กรสามารถพิจารณาผลการวิเคราะห์ความสัมพันธ์ของปัจจัย และสาเหตุความเสี่ยงในเชิงทางการเงิน และที่มิใช่การเงิน เพื่อให้สามารถจัดการความเสี่ยงอย่างเหมาะสม โดยมีผลลัพธ์ที่สามารถเพิ่มผลตอบแทน และสามารถลดความเสียหายกับองค์กรมากที่สุด ทั้งนี้ องค์กรจะต้องประเมินความเสี่ยงคงเหลือ (Residual Risk) เพื่อให้แน่ใจว่ามีกลยุทธ์การจัดการความเสี่ยงให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้ (Risk Appetite : RA)

4.2) แนวทางการตอบสนองต่อความเสี่ยง ประกอบด้วย

4.2.1) การหลีกเลี่ยงความเสี่ยง (Avoid) ความเสี่ยงที่ไม่สามารถยอมรับได้ จะมีการหลีกเลี่ยงการดำเนินงานที่ต่อให้เกิดความเสี่ยง เช่น การหยุดกิจกรรม หรือกลยุทธ์ การเปลี่ยนแปลงแนวทางการดำเนินงานใหม่ เป็นต้น

4.2.2) การถ่ายโอนความเสี่ยง (Transfer) การโอนความเสี่ยงไปให้กับหน่วยงาน หรือองค์กรอื่น เช่น การทำประกัน การจ้างผู้ว่าจ้างจากภายนอก เป็นต้น

4.2.3) การควบคุมความเสี่ยง (Reduce) การจัดทำแผน หรือกิจกรรมควบคุม เพื่อลดระดับความเสี่ยงลงให้อยู่ในระดับที่ยอมรับได้ เช่น การเพิ่มขั้นตอนการตรวจสอบ (Review) การจัดทำมาตรฐานการปฏิบัติงาน เป็นต้น

4.2.4) การยอมรับความเสี่ยง (Accept) ในกรณีที่ความเสี่ยงอยู่ในระดับที่ยอมรับได้ อาจไม่ต้องเพิ่มกระบวนการ หรือกิจกรรมเพื่อลดความเสี่ยง แต่ควรมีการติดตามระดับความเสี่ยงอยู่เป็นประจำ และทบทวนประสิทธิผลของการควบคุมที่มีอยู่

แนวทางการตอบสนองต่อความเสี่ยงจะมีหลายทางเลือก องค์กรจะมีการพิจารณาเลือกใช้ให้เหมาะสมกับประสิทธิภาพในการจัดการความเสี่ยง ภายใต้การวิเคราะห์ความคุ้มค่าและประโยชน์ที่จะได้รับ

5) การติดตาม และประเมินผล

ขั้นตอนการติดตาม และประเมินผลบริหารความเสี่ยงเป็นส่วนสำคัญในการบริหารความเสี่ยงขององค์กร เพื่อให้องค์กรสามารถติดตาม และควบคุมความเสี่ยงให้อยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite : RA) และสามารถปรับแนวทางการจัดการที่เหมาะสมเมื่อระดับความเสี่ยงเกินจากระดับความเสี่ยงที่ยอมรับได้ การรายงานสถานะความเสี่ยง และผลการดำเนินงานตามแผนการจัดการความเสี่ยงที่กำหนดไว้จึงเป็นข้อมูลสำคัญ เพื่อให้องค์กรสามารถทบทวนแผนการจัดการความเสี่ยง เพื่อให้สามารถบรรลุตามแผนยุทธศาสตร์ และวัตถุประสงค์ทางธุรกิจอย่างมีประสิทธิภาพ

6) สื่อสาร และส่งเสริมวัฒนธรรมความเสี่ยง

ขั้นตอนการสื่อสาร และส่งเสริมวัฒนธรรมความเสี่ยงเป็นส่วนประกอบ ในการทำงานอยู่ในทุกขั้นตอนในการบริหารความเสี่ยงขององค์กร เพื่อให้พนักงาน หรือผู้ที่เกี่ยวข้องเข้าใจถึงทิศทาง และแผนการจัดการความเสี่ยง รวมทั้ง สร้างความตระหนักรู้ถึงความเสี่ยงที่เกี่ยวข้อง หรือองค์กรจะต้องเผชิญ และแนวทางในการจัดการ และตอบสนองต่อความเสี่ยงที่เหมาะสม นอกจากนี้ ยังควรส่งเสริม และสร้างวัฒนธรรมความเสี่ยงขององค์กรให้เกิดขึ้น และการให้คุณค่ากับพนักงานที่มีวัฒนธรรมความเสี่ยงที่ดี

ทั้ง 6 กระบวนการบริหารความเสี่ยง องค์กรจะมีการนำไปประยุกต์ใช้ในการบริหารจัดการความเสี่ยงที่มีนัยสำคัญขององค์กร เพื่อให้สามารถวิเคราะห์ และจัดการความเสี่ยงได้อย่างครบถ้วนและเป็นระบบ ในขณะที่พิจารณาเครื่องมือ แนวทางการวัดความเสี่ยง หรือแผนการจัดการความเสี่ยงจะมีการกำหนด ให้เหมาะสมกับประเภทของแต่ละความเสี่ยง เพื่อให้เกิดประสิทธิภาพ และประสิทธิผลในการบริหารจัดการความเสี่ยง

3.5 **การจัดทำแผนบริหารความเสี่ยงองค์กร**

3.5.1 การจัดทำแผนบริหารความเสี่ยงขององค์กร เป็นไปตามแนวทางการบริหารความเสี่ยงระดับสากล และมีความเชื่อมโยงไปยังยุทธศาสตร์ขององค์กร

3.5.2 ให้ทุกหน่วยงาน รวมทั้งผู้บริหารระดับสูงเข้าใจ และให้ความสำคัญกับกระบวนการในการจัดทำแผนบริหารความเสี่ยงขององค์กรที่เป็นแนวทางเดียวกัน

3.5.3 ให้มีการติดตาม ประเมินผลการบริหารจัดการความเสี่ยง และรายงานผลการบริหารจัดการความเสี่ยงเสนอต่อคณะอนุกรรมการกำกับความเสี่ยง คณะกรรมการตรวจสอบ และคณะกรรมการบริษัท

3.5.4 ให้มีการทบทวนแผนการบริหารจัดการความเสี่ยงเมื่อมีการเปลี่ยนแปลงจากปัจจัยภายใน หรือปัจจัยภายนอกที่ส่งผลกระทบที่มีนัยสำคัญต่อเป้าหมายขององค์กร เช่น การเปลี่ยนแปลงกลยุทธ์องค์กรระหว่างปี การปรับเป้าหมายการดำเนินงาน คุณภาพพอร์ตฟอลิโอขององค์กร ผลการดำเนินงาน สถานการณ์เศรษฐกิจที่เปลี่ยนแปลง เป็นต้น