TECHNOLOGIES

บริษัท เอทู เทคโนโลยี จำกัด และกลุ่ม EPC

คู่มือบริหารความเสี่ยง

Risk Management Manual

การอนุมัติ

Prepared by	คณะทำงานบริหารความเสี่ยง	Date	9 พ.ค. 67
Approved by	คณะกรรมการบริษัท	Date	9 พ.ค. 67
Version No.	2	Date	9 พ.ค. 67

คู่มือบริหารความเสี่ยง (Risk Management Manual) ผ่านการอนุมัติ โดยมติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 3/2567 วันที่ 9 พฤษภาคม 2567 ให้มีผลบังคับใช้ตั้งแต่วันที่ได้รับอนุมัติเป็นต้นไป

.....

คุณพิมพฤดา พิทักษ์ธีระธรรม

ประธานกรรมการ

บันทึกการเปลี่ยนแปลง

Version No.	วันที่	ผู้ทำการเปลี่ยนแปลง	รายละเอียด
1	1 ก.ย. 62	คณะทำงานบริหารความเสี่ยง	จัดทำใหม่
2	9 พ.ค. 67	คณะทำงานบริหารความเสี่ยง	1. ปรับปรุงคำจำกัดความ “กลุ่ม EPC” 2. ปรับปรุงตาราง “ผังแสดงระดับความเสี่ยง (Risk Profile)”

สารบัญ

ส่วนที่ 1 บททั่วไป

คณะกรรมการบริษัท ได้ตระหนักและเล็งเห็นความสำคัญของการบริหารความเสี่ยงขององค์กร (Enterprise Risk Management) เป็นอย่างมาก จึงได้แต่งตั้งคณะทำงานบริหารความเสี่ยงขึ้นมาในองค์กร ซึ่งประกอบด้วยผู้บริหารระดับสูงในแต่ละหน่วยงานที่มีความรู้ความเข้าใจในการดำเนินงานของบริษัทมาร่วมกันบริหารความเสี่ยงในระดับองค์กร และระดับหน่วยงาน เพื่อให้เกิดการกำกับดูแลอย่างจริงจัง และครอบคลุมทั่วทั้งองค์กร

ในการบริหารความเสี่ยงนั้น ทางคณะกรรมการบริหารความเสี่ยงได้วางรากฐานการบริหารความเสี่ยง โดยการนำองค์ประกอบการบริหารความเสี่ยงของระดับองค์กรตามมาตรฐานของ The Committee of Sponsoring Organizations of the Treadway Commission : COSO [อ้างอิงตามกรอบการบริหารความเสี่ยง Enterprise Risk Management 2017 : ERM 2017) มาประยุกต์ใช้ในการบริหารจัดการความเสี่ยงให้อยู่ในระดับที่เหมาะสม หรือยอมรับได้ เพื่อให้บรรลุวัตถุประสงค์ กลยุทธ์ พันธกิจ และวิสัยทัศน์ตามที่คณะกรรมการกำหนดไว้

คู่มือการบริหารความเสี่ยงเล่มนี้ ประกอบด้วยเนื้อหาในส่วนของ คำนิยาม องค์ประกอบการบริหารความเสี่ยง โครงสร้าง บทบาท-ขอบเขตหน้าที่ รวมถึงกระบวนการและขั้นตอนการบริหารความเสี่ยง เพื่อให้หน่วยงานเจ้าของความเสี่ยงใช้เป็นแนวทางการบริหารความเสี่ยง ซึ่งเป็นเครื่องมือที่ช่วยให้ทุกภาคส่วนของบริษัทฯ บรรลุวัตถุประสงค์ / เป้าหมายและประสบความสำเร็จในการดำเนินงานอันนำไปสู่การสร้างมูลค่าเพิ่มและการเติบโตขององค์กรอย่างยั่งยืน

1. วัตถุประสงค์ของการบริหารความเสี่ยง

คณะกรรมการบริหารความเสี่ยง ได้กำหนดวัตถุประสงค์ของการบริหารความเสี่ยงให้สอดคล้องกับวิสัยทัศน์ พันธกิจ กลยุทธ์ และเป้าหมายของบริษัท ดังนี้

1.1 เพื่อใช้เป็นแนวทางสำหรับการจัดการความเสี่ยงของบริษัทฯ และกลุ่ม EPC

1.2 เพื่อใช้เป็นแนวทางการปฏิบัติงานในกระบวนการบริหาความเสี่ยง ให้มีความสอดคล้องกัน และนำไปปฏิบัติได้ทั่วทั้งองค์กร โดยอยู่บนพื้นฐานของกฎหมาย กฎระเบียบ ข้อกำหนด ของหน่วยงานกำกับที่เกี่ยวข้องรวมทั้งการต่อต้านการทุจริตคอร์รัปชั่นตามหลากการกำกับดูแลกิจการที่ดี

1.3 เพื่อให้มีเกิดการติดตาม ตรวจสอบ ประเมินผล สื่อสาร และสร้างความเข้าใจแก่บุคลากรอย่างเป็นระบบ

2. คำจำกัดความเกี่ยวกับการบริหารความเสี่ยง

2.1 บริษัทฯ หมายถึง บริษัท เอทู เทคโนโลยี จำกัด

2.2 กลุ่ม EPC หมายถึง บริษัท เอทู วอเตอร์ เมเนจเม้นท์ จำกัด บริษัท เอพีซีเอส เทคโนโลยี จำกัด และบริษัท เอเซีย เวสต์ เอ็นเนอร์ยี่ จำกัด

2.3 คณะกรรมการ หมายถึง คณะกรรมการบริษัทฯ และกลุ่ม EPC

2.4 ผู้บริหาร หมายถึง ประธานกรรมการ, กรรมการผู้จัดการ, รองกรรมการผู้จัดการ และพนักงานระดับผู้จัดการขึ้นไปของบริษัทฯ และกลุ่ม EPC

2.5 พนักงาน หมายถึง พนักงานของบริษัทฯ และกลุ่ม EPC

2.6 ความเสี่ยง (Risk) หมายถึง เหตุการณ์ที่มีความไม่แน่นอน ซึ่งมีโอกาสที่เกิดขึ้นในอนาคต และมีผลกระทบทั้งทางบวกและลบ โดยผลกระทบทางลบจะส่งผลให้การดำเนินงานของบริษัทไม่ประสบความสำเร็จตามวัตถุประสงค์ที่กำหนดไว้ ซึ่งสร้างความเสียหายต่อองค์กร ในด้านที่เป็นตัวเงิน หรือภาพลักษณ์ชื่อเสียงขององค์กร รวมถึงทางด้านกฎหมาย จึงจำเป็นต้องพิจารณาโอกาส (Likelihood) และผลกระทบ (Impact) ที่จะเกิดเหตุการณ์นั้น ๆ ขึ้น

2.7 ปัจจัยความเสี่ยง หมายถึง สาเหตุของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ตามขั้นตอนการดำเนินงานหลักที่กำหนดไว้ทั้งที่เป็นปัจจัยภายใน และปัจจัยภายนอกองค์กร

(1) <u>ปัจจัยภายใน</u> เช่น

- ปัจจัยเสี่ยงด้านเทคโนโลยี เช่น การเลือกใช้เทคโนโลยีไม่เหมาะสม, การล้าหลังของเทคโนโลยี ฯลฯ
- ปัจจัยเสี่ยงด้านการดำเนินงาน เช่น การขาดแคลนบุคลากร, การเปลี่ยนแปลงบุคลากรที่ดำเนินงาน, กระบวนการทำงานไม่เหมาะสม ฯลฯ

เป็นต้น

(2) <u>ปัจจัยภายนอก</u> เช่น

- ปัจจัยเสี่ยงทางด้านการเมืองและสังคม เช่น ความต่อเนื่องในเชิงนโยบายของรัฐบาล
- ปัจจัยเสี่ยงทางด้านการเงินและเศรษฐกิจ เช่น ความผันผวนของภาวะเศรษฐกิจ ราคาน้ำมัน ความผันผวนของอัตราดอกเบี้ย
- ปัจจัยเสี่ยงทางด้านกฎหมาย เช่น ความคลุมเครือของกฎหมายที่เกี่ยวข้อง การเปลี่ยนแปลงกฎระเบียบต่าง ๆ ข้อบังคับที่ล้าหลัง

เป็นต้น

2.8 การประเมินความเสี่ยง หมายถึง การระบุความเสี่ยงและวิเคราะห์เพื่อจัดลำดับความเสี่ยงที่จะมีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร โดยการประเมินจาก ปัจจัยดังนี้

(1) โอกาสที่จะเกิดเหตุการณ์ หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง

(2) ผลกระทบ หมายถึง ขนาดของความรุนแรง ความเสียหายที่จะเกิดขึ้น หากเกิดเหตุการณ์ความเสี่ยง

2.9 การทุจริต หมายถึง การกระทำโดยเจตนา เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองและผู้อื่น ทั้งนี้ การทุจริตสามารถแบ่งได้เป็น 3 ประเภท

(1) การยักยอกทรัพย์สิน หมายถึง การกระทำใดๆ ก็ตามที่นำไปสู่การครอบครองทรัพย์สินของบริษัทอย่างไม่ถูกต้อง หรือเป็นเหตุให้บริษัทสูญเสียทรัพย์สิน โอกาส หรือผลประโยชน์ใด โดยมีเจตนาที่จะหาประโยชน์ต่อตนเองและผู้อื่น (เช่น คนในครอบครัว ญาติ มิตร เป็นต้น)

(2) การคอร์รัปชัน หมายถึง การใช้อำนาจโดยมิชอบกระทำการใดๆ เพื่อให้ได้มาซึ่งประโยชน์อันมิควรได้ ทั้งต่อองค์กร ตนเอง หรือผู้อื่น ทั้งนี้ การคอร์รัปชัน ครอบคลุมถึงการให้และ/หรือการรับสินบน การขัดแย้งทางผลประโยชน์ การข่มขู่และ/หรือเรียกร้องผลประโยชน์ และการจ่ายเงินเพื่อให้ได้รับความสะดวก

(3) การทุจริตในการรายงาน หมายถึง การปรับปรุงแก้ไขรายงานต่างๆ ไม่ว่าจะเป็นทางการเงิน เช่น งบการเงิน บันทึกการเงิน หรือรายงานที่ไม่ใช่ทางการเงิน เพื่อปิดบังการยักยอกทรัพย์หรือการกระทำที่ไม่เหมาะสม หรือเพื่อหาประโยชน์ต่อตนเองและผู้อื่น ซึ่งส่งผลให้งบการเงิน บันทึกการเงิน หรือรายงานต่างๆ ของบริษัท ไม่ถูกต้องตามความเป็นจริง

ส่วนที่ 2 นโยบายการบริหารความเสี่ยงของบริษัท

1. การบริหารความเสี่ยง

บริษัทฯ กำหนดนโยบายและกรอบการดำเนินงานการบริหารความเสี่ยงให้ครอบคลุมทุกด้าน ทั้งปัจจัยความเสี่ยงที่เกี่ยวข้องกับวิสัยทัศน์ เป้าหมาย กลยุทธ์ทางธุรกิจ การเงิน การทุจริตคอร์รัปชั่น และการปฏิบัติการด้านอื่น ๆ รวมถึงการพิจารณาโอกาสที่จะเกิดความเสี่ยง และระดับความรุนแรงของผลกระทบ เพื่อกำหนดมาตรการในการป้องกันการแก้ไขและมอบหมายผู้รับผิดชอบที่ชัดเจน รวมทั้งกำหนดให้มีการรายงานและการติดตามประเมินผล เพื่อปรับปรุงแก้ไขให้สามารถบรรลุวัตถุประสงค์ ดังนั้น บริษัทฯ จึงกำหนดนโยบายบริหารความเสี่ยงองค์กร โดยมีรายละเอียด ดังนี้

1. ผู้บริหารและพนักงานทุกคนมีหน้าที่รับผิดชอบการบริหารความเสี่ยงในหน่วยงานของตน โดยปฏิบัติตามนโยบายบริหารความเสี่ยงองค์กรรวมทั้งมีส่วนร่วมในการพัฒนาการบริหารความเสี่ยงเพื่อเพิ่มโอกาสแห่งความสำเร็จและลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานให้บรรลุเป้าหมาย

2. ฝ่ายบริหารจัดให้มีการบริหารความเสี่ยงของบริษัท และกลุ่ม EPC โดยวิเคราะห์ความเชื่อมโยงของปัจจัยความเสี่ยงต่าง ๆ รวมถึงบริษัทในเครือที่มีผลต่อความเสี่ยงขององค์กรในภาพรวมพร้อมทั้งกำกับดูแลให้มีการบริหารจัดการในแต่ละความเสี่ยงตามหน้าที่ความรับผิดชอบสอดคล้องกับนโยบายต่าง ๆ ของบริษัทฯ เพื่อให้บรรลุตามเป้าหมายที่กำหนดไว้ขององค์กร

3. บริษัทฯ กำหนดให้มีการประเมินความเสี่ยงที่พิจารณาปัจจัยทั้งภายนอกและภายในองค์กรที่อาจส่งผลให้บริษัทฯ ไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ครอบคลุมความเสี่ยงใน 5 ด้าน ได้แก่ 1) ความเสี่ยงด้านกลยุทธ์ 2) ความเสี่ยงด้านธุรกิจ 3) ความเสี่ยงด้านปฏิบัติการ 4) ความเสี่ยงด้านการเงิน และ 5) ความเสี่ยงด้านการทุจริต

4. พิจารณาการกำหนดความเสี่ยงที่ยอมรับได้ของความเสี่ยงที่สำคัญขององค์กร รวมทั้งสนับสนุนส่งเสริมให้มีเครื่องมือ คู่มือ และกระบวนการบริหารความเสี่ยงที่มีประสิทธิภาพ เหมาะสมตามสภาพการเปลี่ยนแปลงของการดำเนินธุรกิจรวมทั้งการรายงานผลการปฏิบัติงานของการบริหารความเสี่ยงต่อคณะกรรมการบริษัทอย่างต่อเนื่อง

5. บริษัทฯ กำหนดให้มีการบริหารความเสี่ยงทั่วทั้งองค์กรเป็นไปตามมาตรฐานสากลพร้อมทั้งจัดทำความสี่ยงที่ยอมรับได้เชิงกลยุทธ์เพื่อใช้เป็นเกณฑ์ในการคัดเลือกกลยุทธ์ที่เหมาะสมให้สอดคล้องกับวัตถุประสงค์เป้าหมายหลักขององค์กรและเป็นกรอบการปฏิบัติงานความเสี่ยงของพนักงานทุกคนในองค์กรให้เป็นไปในทิศทางเดียวกัน

6. ส่งเสริมและสร้างจิตสำนึกให้ผู้บริหารและพนักงานทุกคนมีความตระหนักถึงความสำคัญของการบริหารความเสี่ยงและนำไปปฏิบัติอย่างสม่ำเสมอหรือตามความเหมาะสม

2. ประเภทของความเสี่ยง

ความเสี่ยงแบ่งความออกเป็น 5 ประเภท ดังนี้

2.1 **ความเสี่ยงด้านกลยุทธ์** หมายถึง ความเสี่ยงที่เกี่ยวข้องกับการกำหนดกลยุทธ์และการตัดสินใจด้านกลยุทธ์ซึ่งรวมถึงความไม่สอดคล้องกันระหว่างนโยบาย เป้าหมาย กลยุทธ์โครงสร้างองค์กร ภาวการณ์แข่งขัน และ สภาพแวดล้อมอันส่งผลกระทบต่อองค์กร ได้แก่ ความเสี่ยงที่เกี่ยวข้องกับนโยบายรัฐบาล ความเสี่ยงเกี่ยวข้องกับสภาพเศรษฐกิจและการเมือง ความเสี่ยงเกี่ยวข้องกับชื่อเสียง ความเสี่ยงเกี่ยวข้องกับผู้มีส่วนได้เสีย ความเสี่ยงเกี่ยวกับการแข่งขันทางธุรกิจ ความเสี่ยงเกี่ยวกับการบริหารจัดการ เป็นต้น

2.2 **ความเสี่ยงด้านการปฏิบัติงาน** หมายถึง ความเสี่ยงที่เกิดจากการปฏิบัติงานทั้งในส่วนของการบริหารงานบุคลากร และเทคโนโลยีที่ใช้ในการทำงาน ได้แก่ ความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติงาน ความเสี่ยงเกี่ยวกับการจัดการทรัพย์สิน ความเสี่ยงเกี่ยวกับการทุจริต ความเสี่ยงเกี่ยวกับบุคลากร ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นต้น

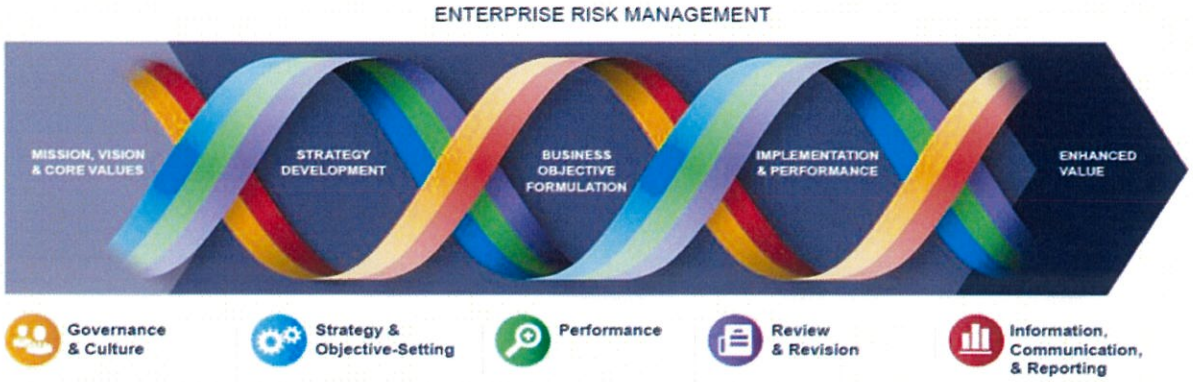
2.3 **ความเสี่ยงด้านการเงิน** หมายถึง ความเสี่ยงเกี่ยวกับนโยบายและขั้นตอนการบริหารจัดการด้านการเงินและการลงทุน ได้แก่ความเสี่ยงเกี่ยวกับโครงสร้างเงินทุน ความเสี่ยงเกี่ยวกับการจัดทำบัญชีและรายงานทางการเงิน ความเสี่ยงเกี่ยวกับสภาพคล่องทางการเงิน ความเสี่ยงจากอัตราแลกเปลี่ยน/อัตราดอกเบี้ย/อัตราเงินเฟ้อ

2.4 **ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบข้อบังคับ** หมายถึง ความเสี่ยงจากการฝ่าฝืนหรือไม่สามารถปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับต่าง ๆ หรือกฎหมาย/ระเบียบที่มีอยู่ไม่เหมาะสมหรือเป็นอุปสรรคในการปฏิบัติงาน

2.5 **ความเสี่ยงด้านการทุจริตคอร์รัปชั่น** หมายถึง โอกาสที่จะเกิดเหตุการณ์ หรือการกระทำโดยเจตนาแสวงหาประโยชน์ที่มิควรได้รับโดยชอบด้วยกฎหมายสำหรับตนเองและผู้อื่น

3. กรอบการบริหารความเสี่ยง

กรอบการบริหารความเสี่ยงขององค์กรที่ได้รับการยอมรับว่าเป็นแนวทางในการส่งเสริมการบริหารความเสี่ยงและเป็นหลักปฏิบัติที่เป็นสากลคือ กรอบการบริหารความเสี่ยงองค์กร (COSO - ERM 2017 : The Committee of Sponsoring Organization of the Treadway Commission - Enterprise Risk Management 2017) ซึ่งประกอบด้วย 5 องค์ประกอบ ตามกระบวนการพัฒนากลยุทธ์ ซึ่งมีรายละเอียด 20 หลักการ (ตามรายละเอียดด้านล่าง)

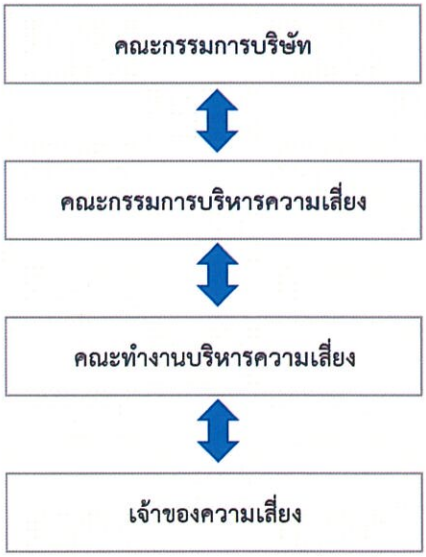


1. การกำกับดูแลกิจการและวัฒนธรรมองค์กร (Governance & Culture)	หลักการที่ 1 คณะกรรมการบริษัทกำกับดูแลความเสี่ยง (Exercise Board Oversight) หลักการที่ 2 จัดโครงสร้างสายการบังคับบัญชา (Establishes Operating Structure) หลักการที่ 3 กำหนดวัฒนธรรมองค์กร (Defines Desired Culture) หลักการที่ 4 แสดงความมุ่งมั่นในค่านิยมองค์กร (Demonstrate Commitment to Core Values) หลักการที่ 5 จูงใจ พัฒนา และรักษาไว้ซึ่งบุคลากรที่มีความสามารถ (Attracts, Develops, and Retains Capable Individuals)
2. กลยุทธ์และวัตถุประสงค์องค์กร (Strategy & Objective Setting)	หลักการที่ 6 วิเคราะห์โครงสร้างของธุรกิจ (Analyze Business Context) หลักการที่ 7 ระบุความเสี่ยงที่องค์กรยอมรับได้ (Define Risk Appetite) หลักการที่ 8 ประเมินกลยุทธ์ในรูปแบบต่างๆ (Evaluate Alternative strategies) หลักการที่ 9 กำหนดวัตถุประสงค์ในการดำเนินธุรกิจ (Formulate Business
3. เป้าหมายผลการดำเนินงาน (Performance)	หลักการที่ 10 ระบุความเสี่ยง (Identify Risk) หลักการที่ 11 ประเมินความรุนแรงความเสี่ยง (Assesses Severity of Risk) หลักการที่ 12 จัดลำดับความสำคัญของความเสี่ยง (Prioritize Risk) หลักการที่ 13 ดำเนินการตอบสนองต่อความเสี่ยง (Implements Risk Response) หลักการที่ 14 จัดทำภาพรวมความเสี่ยงขององค์กร (Develops Portfolio view)

4. การทบทวนและการปรับปรุง (Review & Revision)	หลักการที่ 15 ประเมินการเปลี่ยนแปลงที่มีสาระสำคัญ (Assesses Substantial Change) หลักการที่ 16 ทบทวนความเสี่ยงและผลการดำเนินงาน (Reviews Risk and Performance) หลักการที่ 17 หาแนวทางในการปรับปรุงการบริหารความเสี่ยงขององค์กร (Pursue Improvement in ERM)
5. สารสนเทศ การสื่อสาร และการรายงาน (Information, Communication & Reporting)	หลักการที่ 18 ผลักดันการใช้เทคโนโลยีสารสนเทศ (Leverage Information Technology) หลักการที่ 19 สื่อสารข้อมูลความเสี่ยง (Communicate Risk Information) หลักการที่ 20 รายงานความเสี่ยง วัฒนธรรม และผลการดำเนินงาน (Reports on Risks, Culture, and Performance)

4. โครงสร้างการบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยงกำหนดขึ้นตามกรอบการบริหารความเสี่ยง เพื่อสนับสนุนกระบวนการบริหารความเสี่ยงในการกำกับดูแล ติดตาม รายงานผลการบริหารความเสี่ยง และการปฏิบัติตามแผนงาน หรือมาตรการที่กำหนดไว้ ทำให้มั่นใจว่าการบริหารความเสี่ยงของทุกหน่วยงานในบริษัทฯ และกลุ่ม EPC ดำเนินการอย่างมีประสิทธิภาพ



5. บทบาทหน้าที่และความรับผิดชอบ

การบริหารความเสี่ยง ถือเป็นหน้าที่ของบุคลากรของบริษัททุกระดับทุกคน รวมทั้งผู้ทำหน้าที่ที่ปรึกษา ผู้กระทำการแทนหรือผู้ได้รับมอบหมายให้กระทำหน้าที่ในนามบริษัท โดยมีบทบาทหน้าที่ความรับผิดชอบ ดังนี้

5.1 คณะกรรมการบริษัท

(1) อนุมัตินโยบายการบริหารความเสี่ยงและนโยบายต่อต้านการทุจริตคอร์รัปชั่น และระดับความเสี่ยงที่บริษัทยอมรับได้

(2) กำกับดูแลการบริหารความเสี่ยงเพื่อให้มั่นใจว่านโยบายการบริหารความเสี่ยงได้รับการนำไปปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง

(3) ติดตามความเสี่ยงที่สำคัญของบริษัท เพื่อให้มั่นใจว่าความเสี่ยงได้รับการจัดการให้อยู่ในระดับที่บริษัทยอมรับได้

(4) พิจารณาความเสี่ยงโดยรวมของบริษัทและเปรียบเทียบกับระดับความเสี่ยงที่บริษัทสามารถยอมรับได้

(5) รับรายงานจากคณะกรรมการบริหารความเสี่ยง เกี่ยวกับการนำนโยบายการบริหารความเสี่ยงไปปฏิบัติ รวมทั้งข้อเสนอแนะต่าง ๆ จากคณะกรรมการบริหารความเสี่ยง

5.2 คณะกรรมการบริหารความเสี่ยง

(1) นำเสนอคณะกรรมการบริษัทในกำหนดนโยบายการบริหารความเสี่ยง และระดับความเสี่ยงที่สามารถยอมรับได้

(2) ประเมินความเสี่ยงจากการทุจริตคอร์รัปชั่น ซึ่งบริษัทฯ ให้ความสำคัญต่อการดำเนินการ เพื่อให้มีความชัดเจนในการปฏิบัติ การกำหนดมาตรการป้องกันและลดความเสี่ยงที่มีประสิทธิภาพรวมถึงติดตามประเมินผล และรายงานผล

(3) สอบทานรายงานการบริหารความเสี่ยง และดำเนินการเพื่อให้มั่นใจได้ว่าการจัดการความเสี่ยงมีความเพียงพอและเหมาะสม สามารถจัดการให้อยู่ในระดับที่ยอมรับได้ และการบริหารความเสี่ยงได้ถูกนำไปปฏิบัติอย่างต่อเนื่อง

(4) ประสานงานร่วมกับคณะกรรมการตรวจสอบอย่างสม่ำเสมอ โดยแลกเปลี่ยนความรู้และข้อมูลเกี่ยวกับความเสี่ยงและการควบคุมภายในที่มีผลกระทบต่อบริษัท

(5) ปฏิบัติงานอื่นใดเกี่ยวกับการบริหารความเสี่ยงที่คณะกรรมการบริษัทมอบหมาย

(6) ประชุมคณะกรรมการบริหารความเสี่ยง อย่างน้อยปีละ 2 ครั้ง

5.3 คณะทำงานบริหารความเสี่ยง

(1) นำเสนอกลยุทธ์และแผนต่อกรรมการผู้จัดการ พร้อมทั้งระบุความเสี่ยงที่สำคัญที่อาจมีผลต่อกลยุทธ์และแผนธุรกิจ รวมถึงความเสี่ยงอันเกิดจากการทุจริตคอร์รัปชั่น

(2) นำนโยบายและกรอบการบริหารความเสี่ยงที่ได้รับการอนุมัติจากคณะกรรมการบริษัทแล้วไปพัฒนาให้เกิดการปฏิบัติในสายการบังคับบัญชาที่ตนรับผิดชอบ

(3) พิจารณาปรับปรุงคู่มือการบริหารความเสี่ยงประจำปี

(4) วิเคราะห์ ประเมินผล แนวโน้มความเสี่ยงที่อาจเกิดขึ้นทั้งจากปัจจัยภายในและภายนอก รวมทั้งจัดทำลำดับความเสี่ยงที่สำคัญของหน่วยงานจากมากไปน้อย

(5) ติดตามผลการบริหารความเสี่ยง โดยจัดทำรายงานการติดตามผลการดำเนินงานตามแผนบริหารความเสี่ยงเสนอต่อคณะกรรมการบริหารความเสี่ยง

(6) ประสานงานและให้ความร่วมมือกับเจ้าของความเสี่ยง / หน่วยงานที่รับผิดชอบการบริหารความเสี่ยงจัดการความเสี่ยงและควบคุมภายในเพื่อให้บรรลุผลสำเร็จตามเป้าหมาย

(7) ปฏิบัติการอื่นใดเกี่ยวกับการบริหารความเสี่ยงที่คณะกรรมการบริหารความเสี่ยงมอบหมาย

5.4 เจ้าของความเสี่ยง

(1) วิเคราะห์และประเมินความเสี่ยงของแต่ละส่วนงานที่รับผิดชอบ

(2) จัดทำแผนและมาตรการควบคุมในการบริหารจัดการความเสี่ยง รวมถึงวางแผนและจัดทำงบประมาณในการดำเนินงานบริหารความเสี่ยงของบริษัทฯ

(3) วิเคราะห์ข้อมูลความเสี่ยงที่สำคัญ หรือเกี่ยวข้องกับการดำเนินธุรกิจ รวมทั้งความก้าวหน้าของการบริหารความเสี่ยงของบริษัทฯ ร่วมกับเจ้าของความเสี่ยงเพื่อรายงานต่อคณะทำงานบริหารความเสี่ยง

(4) ดำเนินการติดตาม ทบทวนความเสี่ยง และแผนบริหารความเสี่ยงของหน่วยงานที่รับผิดชอบประจำอย่างต่อเนื่อง

(5) รายงานความเสี่ยงที่อาจจะเกิดขึ้นให้ผู้บังคับบัญชารับทราบอย่างสม่ำเสมอ

ส่วนที่ 3 กระบวนการบริหารความเสี่ยงขององค์กร

บริษัทฯ ได้นำการบริหารความเสี่ยงที่สอดคล้องกับหลักการ COSO ERM 2017 (COSO: Enterprise Risk Management 2017) ซึ่งกำหนดวิธีการปฏิบัติในแต่ละขั้นตอนของการบริหารความเสี่ยงมาปรับใช้ในการพัฒนากระบวนการบริหารความเสี่ยงของบริษัทฯ ซึ่งมี 5 องค์ประกอบ 20 หลักการ ในการบริหารความเสี่ยง ดังนี้

องค์ประกอบที่ 1 การกำกับดูแลกิจการและวัฒนธรรมองค์กร (Governance and Culture)

หลักการที่ 1 คณะกรรมการบริษัทกำกับดูแลความเสี่ยง

คณะกรรมการบริษัทมีหน้าที่ในการกำกับดูแลกลยุทธ์ขององค์กร รวมถึงรับผิดชอบด้านการกำกับดูแลและสนับสนุนผู้บริหารขององค์กร เพื่อให้สามารถดำเนินธุรกิจให้บรรลุตามกลยุทธ์และวัตถุประสงค์ทางธุรกิจที่กำหนดไว้

หลักการที่ 2 จัดโครงสร้างสายการบังคับบัญชา

องค์กรกำหนดโครงสร้างการดำเนินงานที่เหมาะสม เพื่อให้สามารถบรรลุกลยุทธ์และวัตถุประสงค์ทางธุรกิจได้ โดยกำหนดโครงสร้างการดำเนินงานนั้น จะต้องพิจารณาจากกลยุทธ์และเป้าหมายที่ได้กำหนดไว้ ลักษณะการประกอบธุรกิจ ขนาดขององค์กร แหล่งที่ตั้ง ผลิตภัณฑ์/บริการ ช่องทางการจำหน่าย อำนาจหน้าที่ ความรับผิดชอบ สายงานการบังคับบัญชาและการรายงาน รวมถึงข้อกำหนด และนโยบายที่เกี่ยวข้อง

หลักการที่ 3 กำหนดวัฒนธรรมองค์กร

องค์กรกำหนดพฤติกรรมที่พึงประสงค์เพื่อนำไปสู่วัฒนธรรมที่พึงประสงค์ขององค์กร โดยผู้บริหารเป็นผู้นำในการแสดงพฤติกรรมดังกล่าว และให้ความสำคัญกับการทำธุรกิจและการดำเนินการที่มีมาตรฐานที่ดี ผู้บริหารระดับกลางต้องเป็นผู้เชื่อมประสานระหว่างผู้บริหารกับพนักงานและนำกลยุทธ์และเป้าหมายทางธุรกิจมาแปลงเป็นแนวปฏิบัติที่สอดคล้องกับแผนการดำเนินงาน รวมทั้งมีการควบคุมดูแลให้พนักงานปฏิบัติตามแผนและเป้าหมายที่กำหนดไว้

หลักการที่ 4 แสดงความมุ่งมั่นในค่านิยมขององค์กร

องค์กรยึดมั่นต่อค่านิยมขององค์กรที่กำหนดไว้ และสร้างให้บุคลากรมีความตระหนักถึงความเสี่ยงในการทำงานของตน มีการนำความเสี่ยงและผลตอบแทนที่จะได้รับไปประกอบการตัดสินใจจนเป็นกิจวัตร

หลักการที่ 5 จูงใจ พัฒนา และรักษาไว้ซึ่งบุคลากรที่มีความสามารถ

องค์กรยึดมั่นในการสร้างบุคลากรที่มีขีดความสามารถที่จะนำพาให้องค์กรสามารถบรรลุกลยุทธ์ และเป้าหมายทางธุรกิจได้ และมีการจัดทำแผนสืบทอดตำแหน่งสำคัญไว้อย่างเป็นลายลักษณ์อักษร

องค์ประกอบที่ 2 กลยุทธ์และวัตถุประสงค์องค์กร (Strategy and Objective-Setting)

หลักการที่ 6 วิเคราะห์โครงสร้างของธุรกิจ

องค์กรพิจารณาผลกระทบที่อาจจะเกิดขึ้นจากบริบทในการประกอบธุรกิจต่อภาพรวมความเสี่ยงของบริษัท (Risk Profile) โดยพิจารณาทั้งปัจจัยภายนอกองค์กร (สังคม เทคโนโลยี เศรษฐกิจ สิ่งแวดล้อม การเมือง และกฎหมาย) และปัจจัยภายในองค์กร (เงินกองทุน สินทรัพย์ บุคลากร กระบวนการ ระบบงาน ระบบสารสนเทศ และเทคโนโลยี)

หลักการที่ 7 ระบุความเสี่ยงที่องค์กรยอมรับได้

องค์กรกำหนดระดับความเสี่ยงที่ยอมรับได้ซึ่งจะ (ช่วย/สามารถ) สร้างคุณค่า รักษาคุณค่า และก่อให้เกิดการตระหนักในคุณค่าขององค์กรที่มีได้ โดยมีการกำหนดระดับความเสี่ยงที่ยอมรับได้ในระดับองค์กร และระดับย่อย

หลักการที่ 8 ประเมินกลยุทธ์ในรูปแบบต่าง ๆ

องค์กรมีการประเมินกลยุทธ์ทางเลือกต่าง ๆ รวมถึงวิเคราะห์ผลกระทบทั้งเชิงบวกและเชิงลบที่คาดว่าจะเกิดขึ้นจากการเลือกใช้แต่ละกลยุทธ์ต่อภาพความเสี่ยงรวม

หลักการที่ 9 การกำหนดวัตถุประสงค์ในการดำเนินธุรกิจ

การกำหนดวัตถุประสงค์ หมายถึง การเข้าใจถึงภารกิจ วัตถุประสงค์ เป้าหมาย และกลยุทธ์ในการดำเนินงานขององค์กร รวมทั้งสภาพแวดล้อมของการดำเนินงาน ซึ่งสิ่งต่าง ๆ เหล่านี้ได้มีการระบุไว้ในแผน รวมถึงเป้าหมายการดำเนินงานตามบันทึกข้อตกลงประเมินผลการดำเนินงานด้วย ซึ่งการกำหนดวัตถุประสงค์ เป็นการกำหนดวัตถุประสงค์โดยรวมขององค์กร รวมถึงกระบวนการหลักต่าง ๆ ให้สอดคล้องกับวัตถุประสงค์ขององค์กร ได้แก่

(1) วัตถุประสงค์ด้านกลยุทธ์ เป็นวัตถุประสงค์ในระดับสูง ซึ่งเชื่อมโยงและสนับสนุนภารกิจขององค์กร โดยองค์กรกำหนดวัตถุประสงค์ด้านกลยุทธ์เพื่อแสวงหาทางเลือกหรือวิธีการในการสร้างมูลค่าเพิ่มให้แก่ผู้มีส่วนได้เสีย

(2) วัตถุประสงค์ด้านการปฏิบัติงาน เป็นวัตถุประสงค์ในระดับของการปฏิบัติงานที่มุ่งเน้นการใช้ทรัพยากรอย่างมีประสิทธิภาพและประสิทธิผล

(3) วัตถุประสงค์ด้านการรายงาน เป็นวัตถุประสงค์ที่มุ่งเน้นการจัดทำรายงาน ทั้งรายงานทางการเงินและรายงานที่ไม่ใช่ทางการเงิน ซึ่งนำเสนอต่อผู้ใช้ทั้งภายในและภายนอกให้มีความน่าเชื่อถือ โดยมีข้อมูลที่ถูกต้อง สมบูรณ์ และทันเวลา เพื่อสามารถนำไปใช้ในการตัดสินใจต่าง ๆ ได้อย่างเหมาะสม

(4) วัตถุประสงค์ด้านการปฏิบัติตามกฎระเบียบข้อบังคับ เป็นวัตถุประสงค์ที่มุ่งเน้นการปฏิบัติตามกฎหมาย หรือกฎระเบียบที่เกี่ยวข้อง

(5) วัตถุประสงค์ด้านการทุจริต เป็นวัตถุประสงค์ที่มุ่งเน้นให้ทุกหน่วยงานในองค์กรดำเนินการเชิงรุกเพื่อระบุ ประเมินและทบทวนความเสี่ยงด้านการทุจริตขององค์กร รวมทั้งสร้างความตระหนักถึงความเสี่ยงด้านการทุจริตที่อาจเกิดขึ้น และผลกระทบต่อวัตถุประสงค์และการดำเนินงานขององค์กร เพื่อให้มั่นใจว่าความเสี่ยงด้านการทุจริตได้ถูกระบุและจัดการอย่างทันท่วงที

ผลของการกำหนดวัตถุประสงค์ จะทำให้ทราบปัจจัยความสำเร็จ เหตุการณ์ที่มีผลกระทบต่อความสำเร็จของเป้าหมาย หน่วยวัดความสำเร็จ และระดับความคลาดเคลื่อนจากหน่วยวัดที่ยอมรับได้ ทั้งนี้การกำหนดวัตถุประสงค์สำหรับการบริหารความเสี่ยงจะกำหนดจากเป้าหมายการดำเนินงานตามที่กำหนดไว้ในพันธกิจ วิสัยทัศน์ และเป้าหมายอื่น ๆ ตามที่คณะกรรมการบริหารกำหนดเพิ่มเติม

องค์ประกอบที่ 3 เป้าหมายผลการดำเนินงาน (Performance)

หลักการที่ 10 ระบุความเสี่ยง

ระบุความเสี่ยง คือ การพิจารณาเหตุการณ์ที่นำไปสู่ความเสียหาย ซึ่งก่อนขั้นตอนการระบุความเสี่ยงจะต้องดำเนินการ คือกำหนดวัตถุประสงค์ของการดำเนินงานเสียก่อน จากนั้นจึงทำการวิเคราะห์หาเหตุการณ์ที่จะทำให้ไม่สามารถดำเนินงานได้ตามเป้าหมายที่กำหนดไว้ การระบุความเสี่ยงจะต้องพิจารณาปัจจัยทั้งจากภายในและภายนอกองค์กร ดังนี้

(1) ปัจจัยภายในองค์กร : วัตถุประสงค์ขององค์กร นโยบายและกลยุทธ์ การดำเนินงาน กระบวนการทำงาน ประสบการณ์การทำงาน โครงสร้างองค์กรและระบบการบริหารงาน การเงิน วัฒนธรรมขององค์กร สภาพทางภูมิศาสตร์ เทคโนโลยีสารสนเทศ กฎหมาย และระเบียบที่เกี่ยวข้องภายในองค์กร

(2) ปัจจัยภายนอกองค์กร : นโยบายของรัฐบาล สภาวะเศรษฐกิจ การดำเนินการของหน่วยงานที่เกี่ยวข้อง กฎระเบียบภายนอกองค์กร เหตุการณ์ธรรมชาติ สภาพสังคมและการเมือง เป็นต้น

การระบุความเสี่ยงควรเริ่มจากเหตุการณ์ที่มีความชัดเจนหรือมีนัยสำคัญก่อน และจะต้องรวมถึงเหตุการณ์ที่มีโอกาสเกิดขึ้นต่ำแต่มีความเสียหายสูง หรือมีผลกระทบต่อเป้าหมายที่สำคัญด้วย การระบุความเสี่ยงสามารถทำได้หลายแนวทาง ได้แก่ การสัมภาษณ์ (Interviews) การใช้ดุลยพินิจจากประสบการณ์ทำงาน การระดมความคิดจากส่วนงานต่าง ๆ (Brainstorming) การประชุมเชิงปฏิบัติการ (Workshop) การจัดตั้งคณะทำงานที่ประกอบด้วยบุคลากรที่มีความรู้ความสามารถในด้านต่าง ๆ การวิเคราะห์จากข้อมูลในอดีต เป็นต้น นอกจากนี้อาจมี

การระบุความเสี่ยงจากภายนอก เช่น การเปรียบเทียบกับเกณฑ์หรือมาตรฐานสากล การใช้ข้อมูลจากธุรกิจลักษณะเดียวกัน และการมีที่ปรึกษาให้คำแนะนำ เป็นต้น

หลักการที่ 11 การประเมินความเสี่ยง

(1) การประเมินระดับความเสี่ยง จะพิจารณาจากองค์ประกอบ 2 ประการ คือ

(1.1) **โอกาสที่จะเกิดความเสี่ยง (Likelihood)** หมายถึง ความเป็นไปได้ที่ความเสี่ยงหรือเหตุการณ์นั้นจะเกิดขึ้น ซึ่งในการพิจารณาระดับของโอกาสที่จะเกิดขึ้นมักจะใช้ข้อมูลที่ผ่านมา อย่างไรก็ตามในกรณีที่เป็นเหตุการณ์ที่ไม่เคยมีมาก่อน อาจจะใช้ข้อมูลของเหตุการณ์ในลักษณะเดียวกันที่ได้เคยเกิดขึ้นในหน่วยงานอื่น ข้อมูลที่ได้จากการค้นคว้า หรือประสบการณ์ของผู้ประเมิน

(1.2) **ผลกระทบที่เกิดขึ้น (Impact)** หมายถึง ผลกระทบหรือความเสียหายจากความเสี่ยงที่จะเกิดขึ้น ซึ่งอาจเป็นมูลค่าความเสียหาย ความมีนัยสำคัญต่อเป้าหมาย ความอ่อนไหว (Sensitive) ต่อประชาชน ซึ่งในการพิจารณาผลกระทบที่คาดว่าจะเกิดตามมาจะต้องพิจารณาให้ครอบคลุมผลกระทบ 5 ด้าน ซึ่งได้แก่

(1.2.1) ผลกระทบด้านการเงิน คือ ผลกระทบที่ก่อให้เกิดความเสียหายทางการเงิน หรือเกิดความเสียหายอื่น ๆ ซึ่งสามารถแปลงให้อยู่ในรูปของตัวเงินได้

(1.2.2) ผลกระทบด้านการดำเนินงาน คือ ผลกระทบที่ก่อให้เกิดความล่าช้าในการดำเนินงานของบริษัทฯ ได้แก่ผลกระทบจากการดำเนินการผลิต ดำเนินโครงการต่าง ๆ และผลกระทบจากการให้บริการ

(1.2.3) ผลกระทบด้านชื่อเสียง คือ ผลกระทบที่ก่อให้เกิดความเสียหายต่อชื่อเสียง และภาพพจน์ของบริษัทฯ ไม่ว่าจะเป็นผลจากการดำเนินงานทั้งทางตรงและทางอ้อม

(1.2.4) ผลกระทบด้านเทคโนโลยีสารสนเทศ คือ ผลกระทบที่ก่อให้เกิดปัญหาหรือความเสียหายต่อระบบสารสนเทศ ระบบงานต่าง ๆ และข้อมูลสารสนเทศ

(1.2.5) ผลกระทบด้านการบริหารจัดการภายในองค์กร คือ ผลกระทบที่ก่อให้เกิดปัญหาหรือความไม่พึงพอใจในการทำงาน

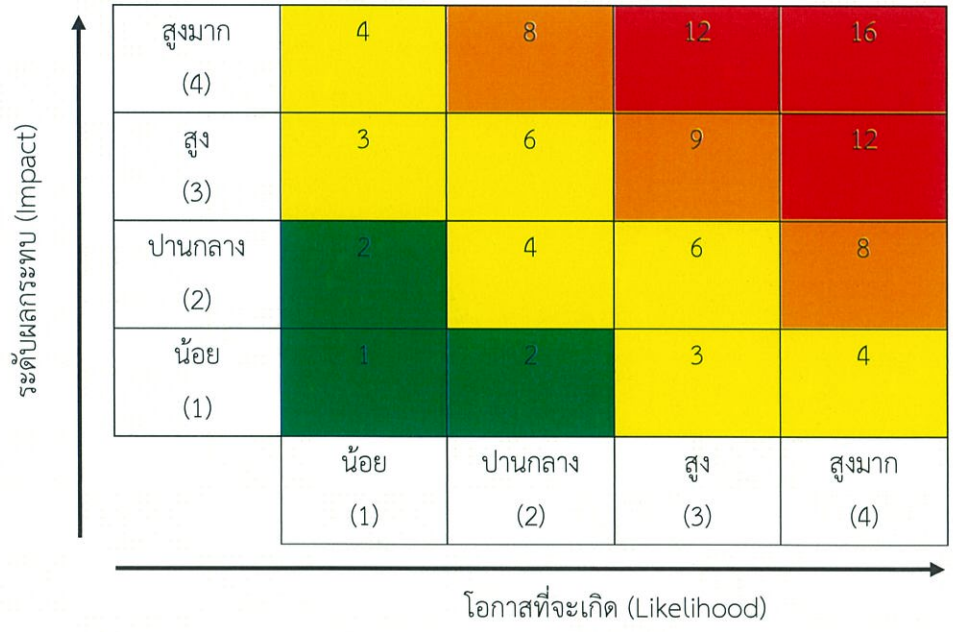
(2) ระดับความเสี่ยง (Level of Risk) คือ ตัวชี้วัดที่ใช้ในการกำหนดความสำคัญของความเสี่ยงโดยค่าระดับความเสี่ยงได้จากการนำโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงมาพิจารณาร่วมกัน ดังนี้

ระดับความเสี่ยง (R) = ระดับโอกาสที่จะเกิดความเสี่ยง (L) x ระดับผลกระทบที่เกิดขึ้น(I)

ระดับความเสี่ยงที่ได้จากการคำนวณตามสูตรข้างต้น หากมีค่าต่ำหมายถึงความเสี่ยงอยู่ในระดับต่ำ และหากมีค่าสูงขึ้นความเสี่ยงจะมีระดับสูงขึ้น

การวัดระดับความเสี่ยง

ผังแสดงระดับความเสี่ยง (Risk Profile)



ความหมายของแต่ละระดับความเสี่ยง

ระดับความเสี่ยงโดยรวม	ระดับคะแนน	ความหมาย
ต่ำ (Low)	1 - 2	ระดับความเสี่ยงที่ยอมรับได้ โดยไม่ต้องมีการควบคุมความเสี่ยงหรือไม่ต้องจัดการเพิ่มเติม
ปานกลาง (Medium)	3 – 7	ระดับความเสี่ยงที่ยอมรับได้ โดยต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
สูง (High)	8 - 9	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ โดยต้องมีการจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
สูงมาก (Extreme)	10-16	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที

หลักการที่ 12 จัดลำดับความสำคัญความเสี่ยง

องค์กรมีการจัดลำดับความสำคัญของความเสี่ยง เพื่อจะได้ใช้ประกอบการเลือกมาตรการตอบสนองความเสี่ยงที่เหมาะสมกับแต่ละความเสี่ยงและสภาวะแวดล้อม

หลักการที่ 13 ดำเนินการตอบสนองความเสี่ยง

หลังจากประเมินความเสี่ยง และมีการจัดลำดับความสำคัญของความเสี่ยงแล้วจะมีการพิจารณากำหนดกลยุทธ์ในการจัดการความเสี่ยงโดยจะเลือกใช้กลยุทธ์ใดกลยุทธ์หนึ่ง หรือหลายกลยุทธ์รวมกันก็ได้เพื่อให้ระดับความเสี่ยงลดลงมาอยู่ในระดับที่ยอมรับได้ซึ่งกลยุทธ์ในการจัดการความเสี่ยงได้แก่

(1) การหลีกเลี่ยงความเสี่ยง (Avoidance) เป็นการกำจัดความเสี่ยงออกไปหรือหลีกเลี่ยงความเสี่ยงเนื่องจากมีโอกาสเกิดขึ้นสูง และมีผลกระทบสูง เช่น เปลี่ยนเป้าหมาย การยกเลิกโครงการหรือแผนงาน การเปลี่ยนรูปแบบการดำเนินโครงการ เป็นต้น

(2) การถ่ายโอนความเสี่ยง (Sharing) เป็นการลดโอกาสที่จะเกิดความเสี่ยง และ/หรือลดผลกระทบที่จะเกิดขึ้นจากความเสี่ยง โดยการถ่ายโอนหรือแบ่งภาระบางส่วนให้ผู้อื่นรับผิดชอบ เช่น การทำประกันภัย การโอนความรับผิดชอบไปยังผู้รับเหมา การโอนงานไปยังผู้รับสัมปทานการจ้างเหมา (Outsourcing) เป็นต้น

(3) การควบคุมความเสี่ยง (Reduction) เป็นการลดโอกาสของการเกิดความเสี่ยง และ/หรือผลกระทบที่จะเกิดขึ้นจากความเสี่ยงโดยปรับเปลี่ยนการทำงานหรือเตรียมแผนการต่าง ๆ รองรับ เช่น

การปรับวิธีการทำงาน การกำหนดมาตรการติดตามตรวจสอบ การปรับโครงสร้าง การให้ความรู้แก่พนักงาน เป็นต้น

(4) การยอมรับความเสี่ยง (Acceptance) เป็นการยอมรับความเสี่ยงที่จะเกิดขึ้น กลยุทธ์นี้จะไม่มีการดำเนินการใดเพื่อลดโอกาส หรือผลกระทบเนื่องจากระดับความเสี่ยงที่เหลืออยู่ อยู่ในระดับต่ำ หรืออยู่ในระดับที่ยอมรับได้หรือมีค่าใช้จ่ายในการบริหารจัดการความเสี่ยงสูงกว่าผลลัพธ์ที่จะได้

หลักการที่ 14 จัดทำภาพรวมความเสี่ยงขององค์กร

องค์กรจัดทำภาพความเสี่ยงรวมของบริษัทและประเมินสถานะความเสี่ยงและภาพความเสี่ยงรวมในปัจจุบัน โดยพิจารณาในภาพรวมของกลยุทธ์ ภาพรวมของเป้าหมายทางธุรกิจระดับองค์กร เป้าหมาย ทางธุรกิจในด้านต่าง ๆ และความเสี่ยงที่เกี่ยวข้อง

องค์ประกอบที่ 4 การทบทวนและการปรับปรุงแก้ไข (Review & Revision)

หลักการที่ 15 ประเมินการเปลี่ยนแปลงที่มีสาระสำคัญ

เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อม วิธีการจัดการความเสี่ยงที่กำหนดไว้อาจจะไม่เหมาะสม กิจกรรมควบคุมอาจมีประสิทธิภาพน้อยลง หรือเป้าหมายการดำเนินงานอาจมีการเปลี่ยน ดังนั้นจึงต้องมีการติดตามตรวจสอบว่าการบริหารความเสี่ยงในแต่ละขั้นตอนยังคงมีประสิทธิภาพอยู่หรือไม่

การติดตามตรวจสอบสามารถทำได้ 2 วิธีคือ ติดตามตรวจสอบระหว่างการปฏิบัติงาน (Ongoing Monitoring) และการประเมินผลเป็นช่วง ๆ (Separate Evaluation)

การติดตามตรวจสอบระหว่างการปฏิบัติงานเป็นการติดตามตรวจสอบอย่างต่อเนื่องในทุกขั้นตอนของการบริหารความเสี่ยง ในขณะที่การประเมินผลเป็นช่วง ๆ จะกระทำเป็นครั้ง ๆ ไปตามช่วงเวลาที่กำหนด ดังนั้นการติดตามตรวจสอบระหว่างการปฏิบัติงานจะมีประสิทธิภาพมากกว่า นอกจากนี้หากมีการตรวจสอบระหว่างการปฏิบัติงานมากเท่าไร การตรวจสอบในลักษณะการประเมินผลเป็นช่วง ๆ ก็จะน้อยลงเท่านั้น

หลักการที่ 16 ทบทวนความเสี่ยงและผลการดำเนินงาน

องค์กรทบทวนผลการดำเนินงานที่เกิดขึ้นและวิเคราะห์ถึงความเสี่ยงที่ทำให้ผลการดำเนินงานไม่เป็นไปตามที่ได้กำหนดไว้ รวมทั้งวิเคราะห์ความเสี่ยงที่องค์กรมีอยู่เทียบกับระดับความเสี่ยงที่ยอมรับได้ รวมถึงความถูกต้องในการประเมินมูลค่าความเสี่ยงขององค์กร

หลักการที่ 17 หาแนวทางในการปรับปรุงการบบริหารความเสี่ยงขององค์กร

องค์กรทบทวนการบริหารความเสี่ยงที่ได้ดำเนินการไปแล้ว และประเมินประสิทธิภาพ และประสิทธิผลของการดำเนินการเพื่อการปรับปรุงแก้ไขในอนาคต รวมถึงพิจารณาเทคโนโลยีใหม่ที่อาจนำมาใช้เป็นเครื่องมือ เพื่อช่วยเพิ่มประสิทธิภาพและประสิทธิผลในการบริหารความเสี่ยง การปรับโครงสร้างองค์กรเพื่อให้สอดคล้องกับกลยุทธ์และสภาวะแวดล้อมที่เปลี่ยนแปลงไป การทบทวนระดับความเสี่ยงที่ยอมรับได้ การพิจารณาความเสี่ยงอุบัติใหม่ประกอบการบริหาร ความเสี่ยงในอนาคต ประสิทธิภาพของการสื่อสาร และการเปรียบเทียบการบริหารความเสี่ยงกับองค์กรอื่นๆ

องค์ประกอบที่ 5 สารสนเทศ การสื่อสาร และการรายงานผล (Information, Communication & Reporting)

หลักการที่ 18 ผลักดันการใช้เทคโนโลยีสารสนเทศ

องค์กรใช้ประโยชน์จากระบบเทคโนโลยีสารสนเทศที่มีอยู่ โดยการนำข้อมูลมาวิเคราะห์เพื่อหาข้อมูลเชิงลึก รวมถึงมีการเก็บรวบรวมสารสนเทศสำคัญที่เกี่ยวข้อง อาทิ สภาพรวมของตลาด อัตราการเจริญเติบโต ผลประกอบการโดยรวม ข้อมูลการประกอบธุรกิจของคู่แข่งในอุตสาหกรรมเดียวกัน แนวโน้มการเติบโตของธุรกิจ หรือแนวโน้มการดำเนินการด้านการบริหารความเสี่ยงในอนาคต

หลักการที่ 19 สื่อสารข้อมูลความเสี่ยง

สื่อสารข้อมูลความเสี่ยง หมายถึง การจัดให้มีการสื่อสารและระบบสารสนเทศความเสี่ยงที่ดีเพื่อให้มั่นใจว่าผู้บริหารและพนักงานทุกคนเข้าใจกระบวนการและบทบาทหน้าที่ความรับผิดชอบของตนเกี่ยวกับการบริหารความเสี่ยง ได้แก่

(1) คณะกรรมการและผู้บริหารระดับสูงมีการสื่อสารเกี่ยวกับนโยบายการบริหารความเสี่ยง และสถานะของความเสี่ยงให้พนักงานทุกคนเข้าใจและดำเนินการบริหารความเสี่ยงตามบทบาทหน้าที่

(2) จัดให้มีช่องทางในการสื่อสารสองทางที่มีประสิทธิภาพระหว่างผู้บริหารและพนักงาน

(3) มีการประสานงานระหว่างงานบริหารความเสี่ยงกับงานตรวจสอบเพื่อที่จะได้เกิดการแลกเปลี่ยนข้อมูลที่เป็นประโยชน์ระหว่างกัน

(4) มีการสื่อสารข้อมูลที่เกี่ยวข้องกับการบริหารความเสี่ยงทั้งจากภายในและภายนอกองค์กรผ่านระบบสารสนเทศและการสื่อสารภายในองค์กร เพื่อให้พนักงานได้รับทราบข้อมูลเกี่ยวกับการบริหารความเสี่ยง ตลอดจนสาระความรู้เกี่ยวกับการบริหารความเสี่ยงอย่างสม่ำเสมอและทันต่อเหตุการณ์

หลักการที่ 20 รายงานความเสี่ยง วัฒนธรรม และผลการดำเนินงาน

องค์กรรายงานผลเกี่ยวกับการบริหารความเสี่ยง การพัฒนาวัฒนธรรมองค์กรให้พนักงานมีความรู้ความเข้าใจเกี่ยวกับความเสี่ยงในงานของตนและนำการบริหารความเสี่ยงไปใช้เป็นเครื่องมือในการทำงาน รวมถึงมีการสื่อสารผลการดำเนินงานและผลการบริหารความเสี่ยงไปยังบุคลากรทุกระดับรวมถึงองค์กรภายนอกที่เกี่ยวข้อง

คณะทำงานบริหารความเสี่ยงมีหน้าที่รับผิดชอบหลัก คือ การรายงานผลการบริหารความเสี่ยงระดับองค์กรให้คณะกรรมการบริหารได้ทราบทุก ๆ 6 เดือน เป็นอย่างน้อย อย่างไรก็ตามหากมีความเสี่ยงที่มีนัยสำคัญเกิดขึ้นหรือการจัดการความเสี่ยงที่นำมาใช้ไม่มีประสิทธิภาพจะต้องรายงานให้คณะกรรมการบริหารทราบในทันที