

กรอบและนโยบายการบริหารความเสี่ยง ประจำปี 2569

บริษัท ไทยรี กรุ๊ป โฮลดิ้งส์ จำกัด (มหาชน)

Thaire Group Holdings Public Company Limited

สารบัญ

	หน้า
วัตถุประสงค์ของการบริหารความเสี่ยง	3
กรอบการบริหารความเสี่ยง	4
โครงสร้างพื้นฐานของการบริหารความเสี่ยง	5
วิสัยทัศน์และพันธกิจ	5
กรอบระดับความเสี่ยงที่ยอมรับได้	5
นโยบายการบริหารความเสี่ยง	7
ระบบสารสนเทศ	8
โครงสร้างการกำกับดูแลและวัฒนธรรมการบริหารความเสี่ยง	9
โครงสร้างการกำกับดูแลการบริหารความเสี่ยง	9
การสนับสนุนจากผู้บริหาร	14
การบูรณาการการบริหารความเสี่ยง	15
การสร้างวัฒนธรรมและความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยง	15
ขอบเขตของการบริหารความเสี่ยง	16
ประเภทของความเสี่ยง	16
กิจกรรมหลัก	17
กระบวนการการบริหารความเสี่ยง	18
การระบุความเสี่ยง	18
การประเมินความเสี่ยง	18
การตอบสนองความเสี่ยง	18
การควบคุมดูแลและติดตามความเสี่ยง	19
การรายงานข้อมูลการบริหารความเสี่ยง	19

วัตถุประสงค์ของการบริหารความเสี่ยง

บริษัท ไทยรี กรุ๊ป โฮลดิ้งส์ จำกัด (มหาชน) (บริษัทฯ) ถูกจัดตั้งขึ้นเพื่อเป็นบริษัทที่เน้นการลงทุนในธุรกิจรับประกันภัยต่อด้านประกันวินาศภัย ซึ่งเป็นธุรกิจที่ช่วยเพิ่มขีดความสามารถในการรับความเสี่ยงไว้ในประเทศ และช่วยส่งเสริมสนับสนุนการประกอบธุรกิจของบริษัทประกันวินาศภัยในฐานะหุ้นส่วนธุรกิจ

ในการดำเนินการเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวนี้ บริษัทฯ ต้องเผชิญกับความท้าทายทั้งภายในและภายนอกองค์กรอันเนื่องมาจากการเปลี่ยนแปลงทางสังคม การเมือง เศรษฐกิจ สิ่งแวดล้อม และเทคโนโลยี รวมถึงการเกิดขึ้นของความเสี่ยงอุบัติใหม่ ซึ่งส่งผลให้การประกอบธุรกิจในปัจจุบันต้องเผชิญกับสถานการณ์ที่ต่างไปจากที่เคยเกิดในอดีต และก่อให้เกิดความซับซ้อนซึ่งยากต่อการคาดการณ์ผลลัพธ์ที่จะเกิดขึ้นในอนาคต

ด้วยเหตุนี้ บริษัทฯ จึงต้องมีการบริหารความเสี่ยงที่มีประสิทธิภาพและประสิทธิผล เพื่อให้บริษัทฯ สามารถบรรลุวิสัยทัศน์และพันธกิจขององค์กรได้ และช่วยให้ผลการดำเนินงานของบริษัทฯ เป็นไปตามเป้าหมายที่กำหนดไว้ สามารถรักษาความมั่นคงทางการเงิน ชื่อเสียง ภาพลักษณ์ ความได้เปรียบในการแข่งขัน และตอบสนองความต้องการของผู้มีส่วนได้ส่วนเสียหลักแต่ละกลุ่มได้อย่างเหมาะสม

กรอบการบริหารความเสี่ยง

บริษัทฯ ได้กำหนดกรอบการบริหารความเสี่ยงขึ้นเพื่อเป็นแนวทางในการบริหารความเสี่ยงแบบบูรณาการภายในองค์กร กรอบการบริหารความเสี่ยงของบริษัทฯ ถูกพัฒนาขึ้นจากกรอบการบริหารความเสี่ยงที่เป็นมาตรฐานสากล อาทิเช่น The Committee of Sponsoring Organizations of the Treadway Commission (COSO) บริษัทจัดอันดับความน่าเชื่อถือ Standard and Poor's A.M. Best และ Fitch Ratings รวมถึงกฎหมายที่เกี่ยวข้องกับการบริหารความเสี่ยงแบบองค์รวมของหน่วยงานกำกับดูแลด้วย

กรอบการบริหารความเสี่ยงของบริษัทฯ ประกอบด้วย 4 องค์ประกอบหลัก ได้แก่ 1) โครงสร้างพื้นฐานของการบริหารความเสี่ยง 2) โครงสร้างการกำกับดูแลและวัฒนธรรมการบริหารความเสี่ยง 3) ขอบเขตการบริหารความเสี่ยง และ 4) กระบวนการการบริหารความเสี่ยง



ส่วนที่ 1 – โครงสร้างพื้นฐานของการบริหารความเสี่ยง

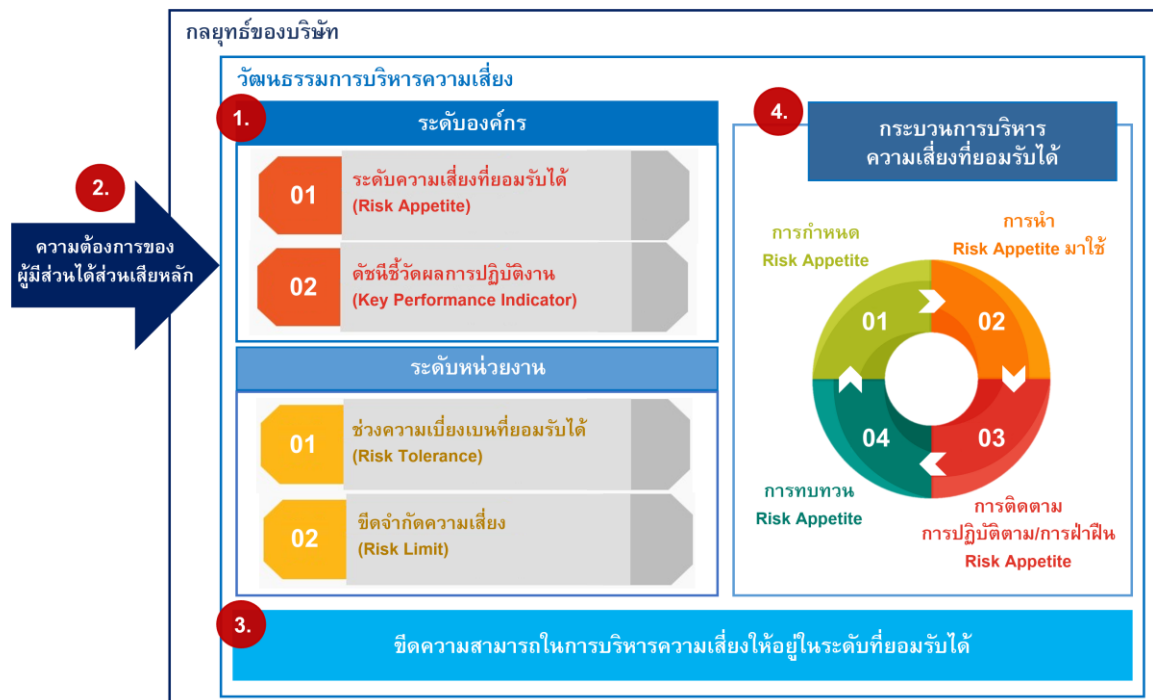
โครงสร้างพื้นฐานของการบริหารความเสี่ยงเกี่ยวข้องกับปัจจัยพื้นฐานที่เกื้อหนุนต่อความสำเร็จของการบริหารความเสี่ยง ซึ่งประกอบไปด้วยองค์ประกอบต่อไปนี้

วิสัยทัศน์และพันธกิจ (Vision and Mission)

วิสัยทัศน์และพันธกิจเป็นสิ่งที่กำหนดทิศทางและจุดหมาย ตลอดจนขอบเขตการดำเนินงานและสิ่งที่บริษัท ต้องการจะบรรลุในอนาคต บริษัท มีการกำหนดกลยุทธ์ เป้าหมาย และแผนการดำเนินงานเพื่อให้บรรลุวิสัยทัศน์และพันธกิจได้ มีการวิเคราะห์และประเมินสถานะแวดล้อมทั้งภายในและภายนอกเพื่อระบุความเสี่ยงหลัก กำหนดดัชนีชี้วัดความเสี่ยง มาตรการในการบริหารจัดการความเสี่ยง และติดตามผลการบริหารความเสี่ยงอย่างต่อเนื่อง เพื่อให้บริษัท สามารถบริหารจัดการความเสี่ยงหลักขององค์กรให้อยู่ในระดับที่ยอมรับได้

กรอบระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite Framework)

บริษัท มีการกำหนดกรอบระดับความเสี่ยงที่ยอมรับได้ โดยมีคณะกรรมการบริษัทและผู้บริหารทำหน้าที่กำหนดทิศทางในการจัดทำกรอบฯ ดังกล่าว เพื่อใช้เป็นแนวทางในการดำเนินการภายในองค์กร กรอบระดับความเสี่ยงที่ยอมรับได้ของบริษัท ต้องมีการบูรณาการกลยุทธ์ขององค์กร เงินกองทุน และการบริหารความเสี่ยงเข้าด้วยกันเพื่อให้บริษัท สามารถมองเห็นภาพความเสี่ยงรวม ผนวกแนวคิดของการบริหารความเสี่ยง และเงินกองทุนเข้าไปในการปฏิบัติงาน วิเคราะห์การเปลี่ยนแปลงของความเสี่ยงอย่างต่อเนื่อง และบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้



ในการจัดทำกรอบระดับความเสี่ยงที่ยอมรับได้ บริษัทฯ จะต้องพิจารณาปัจจัยดังต่อไปนี้

1. ความต้องการของผู้มีส่วนได้ส่วนเสียหลักของบริษัทฯ (Stakeholder Interest) – บริษัทฯ ควรพิจารณาความต้องการของผู้มีส่วนได้ส่วนเสียหลักของบริษัทฯ ที่หลากหลายและนำมารวบรวมและกำหนดระดับความเสี่ยงที่ยอมรับได้ที่เหมาะสม เพื่อให้สามารถสร้างความสมดุลของกลยุทธ์ เงินกองทุน และความเสี่ยงที่เกี่ยวข้อง
2. ระดับความเสี่ยงที่ยอมรับได้และช่วงความเบี่ยงเบนที่ยอมรับได้ (Risk Appetite and Risk Tolerance) – ความต้องการของผู้มีส่วนได้ส่วนเสียหลัก กลยุทธ์ และแผนธุรกิจของบริษัทฯ จะเป็นสิ่งที่กำหนดดัชนีชี้วัดผลการปฏิบัติงานในระดับองค์กรและระดับหน่วยงาน ซึ่งจะนำไปสู่การกำหนดระดับความเสี่ยงที่ยอมรับได้และช่วงความเบี่ยงเบนที่ยอมรับได้ของแต่ละความเสี่ยงหลักที่เหมาะสมและสอดคล้องไปในทิศทางเดียวกัน
3. ชีตความสามารถในการบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (Required Capabilities) – ในการบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้นั้น บริษัทฯ จะต้องมีการกำหนดนโยบายการบริหารความเสี่ยงและแนวทางการทำงานที่เกี่ยวข้อง มีการกำหนดระดับความเสี่ยงที่ยอมรับได้ ช่วงความเบี่ยงเบนที่ยอมรับได้ ดัชนีชี้วัดความเสี่ยง และขีดจำกัดความเสี่ยง รวมทั้งติดตามวัดผลค่าดังกล่าวอย่างต่อเนื่อง มีการสื่อสารระดับความเสี่ยงที่ยอมรับได้ไปยังผู้ที่เกี่ยวข้องเพื่อให้เกิดความเข้าใจที่ตรงกัน และมีกลไกในการยกระดับความสำคัญหากมีการฝ่าฝืนระดับความเสี่ยงที่ยอมรับได้และช่วงความเบี่ยงเบนที่ยอมรับได้
4. กระบวนการบริหารระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite Management Process) – กระบวนการบริหารระดับความเสี่ยงที่ยอมรับได้ ประกอบด้วย 1) การกำหนดระดับความเสี่ยงที่ยอมรับได้ของบริษัทฯ 2) การนำระดับความเสี่ยงที่ยอมรับได้มาใช้เป็นกรอบในการดำเนินธุรกิจ 3) การติดตามการปฏิบัติตาม/การฝ่าฝืนระดับความเสี่ยงที่ยอมรับได้ และ 4) การทบทวนระดับความเสี่ยงที่ยอมรับได้

ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) หมายถึง ระดับความเสี่ยงในภาพรวมที่บริษัทฯ เต็มใจยอมรับเพื่อให้บรรลุภารกิจ วิสัยทัศน์ วัตถุประสงค์ และเป้าหมายทางธุรกิจ บริษัทฯ ต้องมีการกำหนดระดับความเสี่ยงที่ยอมรับได้สำหรับภาพความเสี่ยงรวม โดยคณะกรรมการบริษัทจะเป็นผู้พิจารณาอนุมัติระดับความเสี่ยงที่ยอมรับได้ และผู้บริหารระดับสูง คณะกรรมการบริหารความเสี่ยง เจ้าของความเสี่ยง รวมถึงหน่วยงานที่เกี่ยวข้อง จะนำระดับความเสี่ยงที่ยอมรับได้มาใช้เป็นกรอบในการดำเนินงานและการบริหารจัดการความเสี่ยงหลักที่เกี่ยวข้อง

ระดับความเสี่ยงที่ยอมรับได้จะถูกใช้เป็นเกณฑ์ที่กำหนดว่ากิจกรรมและการดำเนินการใดเป็นสิ่งที่ยอมรับได้ขององค์กร ทั้งยังช่วยในการตัดสินใจสำหรับการจัดสรรเงินกองทุนและทรัพยากรอื่นที่มีอยู่ เพื่อให้บริษัทฯ สามารถบรรลุเป้าหมายและบริหารจัดการความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้

บริษัทฯ ยังมีการกำหนดช่วงความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance) ซึ่งเป็นระดับความเสี่ยงที่กำหนดย่อยลงมาจากระดับความเสี่ยงที่ยอมรับได้ สำหรับทุกความเสี่ยงหลักของบริษัทฯ เพื่อกำหนดกรอบในการดำเนินงานเพื่อให้ได้ผลลัพธ์ตามที่ต้องการ และใช้ดัชนีชี้วัดความเสี่ยง (Key Risk Indicator) ในการติดตามสถานะหรือแนวโน้มของความเสี่ยงและการเปลี่ยนแปลงความเสี่ยงหลักของบริษัทฯ นอกจากนี้ บริษัทฯ จะต้องมีการกำหนดขีดจำกัดความเสี่ยง (Risk Limit) ซึ่งเป็นเกณฑ์ที่กำหนดไว้สำหรับดัชนีชี้วัดความเสี่ยง เพื่อช่วยให้บริษัทฯ สามารถบริหารจัดการความเสี่ยงให้อยู่ภายในช่วงความเบี่ยงเบนที่ยอมรับได้และระดับความเสี่ยงที่ยอมรับได้

หากกิจกรรมหรือการดำเนินการใดมีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ บริษัทฯ จะต้องเสนอความเป็นไปได้ของการละเมิดดังกล่าวต่อคณะกรรมการบริษัทเพื่อพิจารณาอนุมัติการดำเนินการเพิ่มเติมที่จำเป็น รวมถึงพิจารณาความจำเป็นในการทบทวนระดับความเสี่ยงที่ยอมรับได้ของบริษัทฯ เพื่อให้เหมาะสมกับภูมิทัศน์ความเสี่ยงที่เปลี่ยนไป

นโยบายการบริหารความเสี่ยง (Enterprise Risk Management)

บริษัทฯ ต้องมีการจัดทำนโยบายการบริหารความเสี่ยงที่ผ่านการอนุมัติจากคณะกรรมการบริษัท เพื่อใช้เป็นแนวทางในการดำเนินการบริหารความเสี่ยงให้เหมาะสมและสอดคล้องกับกลยุทธ์และระดับความเสี่ยงที่ยอมรับได้ เกิดประสิทธิผลในการบริหารความเสี่ยงของทุกหน่วยงานภายในบริษัท นอกจากนี้ บริษัทฯ ยังต้องมีการจัดทำกรอบระดับความเสี่ยงที่ยอมรับได้ เพื่อใช้เป็นกรอบในการดำเนินธุรกิจและการตัดสินใจขององค์กร

การบริหารความเสี่ยงของบริษัทฯ จะต้องมีการบูรณาการการบริหารความเสี่ยง การบริหารเงินกองทุน และแผนธุรกิจเข้าด้วยกัน เพื่อที่จะบรรลุเป้าหมายที่ได้กำหนดไว้และสามารถบริหารความเสี่ยงขององค์กรให้อยู่ในระดับที่ยอมรับได้ บริษัทฯ จะต้องนำกลยุทธ์และแผนธุรกิจมาวิเคราะห์เพื่อระบุและประเมินความเสี่ยงหลักที่บริษัทฯ เผชิญอยู่และอาจเกิดขึ้นในอนาคต และกำหนดมาตรการการบริหารความเสี่ยงหลักของบริษัทฯ ควบคู่กัน โดยกระบวนการในการวิเคราะห์เพื่อประเมินความเสี่ยงและกำหนดมาตรการดังกล่าวนั้น ให้เป็นไปตามกระบวนการในการบริหารความเสี่ยงดังที่ได้ระบุไว้ในกรอบการบริหารความเสี่ยงของบริษัทฯ

บริษัทฯ ต้องจัดให้มีการจัดทำนโยบายการบริหารความเสี่ยงสำหรับกิจกรรมหลักของบริษัทฯ และครอบคลุมทุกประเภทความเสี่ยงสำคัญที่มีอยู่ในกิจกรรมและกระบวนการดำเนินงานของบริษัทฯ ซึ่งประกอบด้วย 1) ความเสี่ยงด้านกลยุทธ์ 2) ความเสี่ยงด้านปฏิบัติการ 3) ความเสี่ยงด้านตลาด 4) ความเสี่ยงด้านเครดิต 5) ความเสี่ยงด้านสภาพคล่อง 6) ความเสี่ยงด้านชื่อเสียง 7) ความเสี่ยงด้านเทคโนโลยีสารสนเทศ 8) ความเสี่ยงอุบัติใหม่ และ 9) ความเสี่ยงภายในกลุ่มธุรกิจ

บริษัทฯ จะต้องจัดทำทะเบียนความเสี่ยงเพื่อใช้ในการติดตามและรายงานข้อมูลสถานะความเสี่ยงหลัก และการปฏิบัติตามนโยบายการบริหารความเสี่ยง โดยทะเบียนความเสี่ยงจะต้องครอบคลุมข้อมูลเกี่ยวกับความเสี่ยง สาเหตุของความเสี่ยง ประเภทความเสี่ยง เจ้าของความเสี่ยง ดัชนีชี้วัดความเสี่ยง ขีดจำกัดความเสี่ยง มาตรการจัดการความเสี่ยงที่ใช้ในปัจจุบัน และมาตรการบริหารความเสี่ยงที่อาจจะมีเพิ่มเติมในอนาคต

นอกจากนี้ บริษัทฯ ต้องจัดให้มีการวิเคราะห์ความต่อเนื่องในการดำเนินธุรกิจ ซึ่งครอบคลุมถึงการทดสอบภาวะวิกฤตตามระยะเวลาที่สอดคล้องกับแผนธุรกิจและระดับความเสี่ยงที่ยอมรับได้ เพื่อให้มั่นใจว่า บริษัทฯ มีความมั่นคงทางการเงิน และมาตรการบริหารความเสี่ยงของบริษัทฯ มีประสิทธิภาพและประสิทธิผล โดยจัดให้มีการทดสอบภาวะวิกฤตอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงทางการเงินหรือภาพรวมของความเสี่ยงของบริษัทฯ อย่างมีนัยสำคัญ และหากผลการทดสอบนั้นละเมิดความเสี่ยงที่ยอมรับได้ บริษัทฯ จะต้องมีการนำเสนอแผนการดำเนินการและรายงานต่อคณะกรรมการบริหารความเสี่ยงให้รับทราบ

บริษัทฯ ต้องมีการกำหนดโครงสร้างการกำกับดูแลการบริหารความเสี่ยงและระบุบทบาทหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องอย่างชัดเจน ผู้บริหารและพนักงานทุกคนต้องปฏิบัติตามนโยบาย กรอบ และหลักเกณฑ์ที่ได้กำหนดไว้ในนโยบายนี้ ตลอดจนมีส่วนร่วมในการบริหารความเสี่ยงที่สอดคล้องกับบทบาทและหน้าที่ความรับผิดชอบที่ได้กำหนดไว้ และช่วยสร้างวัฒนธรรมการบริหารความเสี่ยงเพื่อให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการทำงานของผู้บริหารและพนักงานทุกคนในองค์กร

ระบบสารสนเทศ (Information System)

การเก็บข้อมูลและสถิติที่มีคุณภาพถือเป็นพื้นฐานสำคัญสำหรับการบริหารความเสี่ยง เนื่องจากข้อมูลและสถิติเหล่านี้ก่อให้เกิดฐานข้อมูลที่มีประโยชน์ต่อการวิเคราะห์และการตัดสินใจ ระบบสารสนเทศของบริษัทต้องได้รับการพัฒนาให้มีประสิทธิภาพเพื่อให้มั่นใจได้ว่าการจัดเก็บข้อมูลของบริษัทที่จะถูกนำไปใช้ในการวิเคราะห์และการตัดสินใจเพื่อสนับสนุนการประกอบธุรกิจและการบริหารความเสี่ยงของแต่ละหน่วยงานนั้น มีความครบถ้วน ถูกต้อง เป็นปัจจุบัน มีความพร้อมใช้ ปลอดภัย และเหมาะสมกับสภาวะแวดล้อมที่เปลี่ยนแปลงไป

ระบบสารสนเทศของบริษัท ต้องรองรับการบริหารความเสี่ยงขององค์กร และมีความน่าเชื่อถือเหมาะสม สอดคล้องกับขนาด ลักษณะ และความซับซ้อนของธุรกิจที่ดำเนินการอยู่รวมถึงแผนงานในอนาคต รวมถึงมีระบบสำรองข้อมูลและระบบการกู้คืนข้อมูลในกรณีที่เกิดเหตุฉุกเฉิน มีการกำหนดมาตรการในการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลและระบบสารสนเทศ รวมถึงการกำหนดสิทธิในการเข้าถึงข้อมูลของบุคลากรที่เกี่ยวข้องและบังคับใช้มาตรการดังกล่าวอย่างเคร่งครัด

บริษัท ต้องคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินธุรกิจ รวมถึงการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยไซเบอร์ ซึ่งจะมีผลกระทบต่อระบบ กระบวนการปฏิบัติงาน และชื่อเสียงของบริษัท และต้องดำเนินการตามมาตรการบริหารความเสี่ยงที่กำหนดไว้อย่างเคร่งครัดเพื่อให้ความเสี่ยงดังกล่าวถูกบริหารจัดการอยู่ในระดับที่ยอมรับได้

ส่วนที่ 2 – โครงสร้างการกำกับดูแลและวัฒนธรรมการบริหารความเสี่ยง

บริษัท ต้องจัดให้มีโครงสร้างการกำกับดูแลที่เหมาะสมเพื่อให้เกิดระบบ Check and Balance ขึ้นในบริษัท และเพื่อให้มั่นใจว่าการบริหารความเสี่ยงของบริษัท เป็นไปอย่างบูรณาการ มีประสิทธิภาพและประสิทธิผล ผู้บริหารของบริษัท ต้องให้ความสำคัญกับการสร้างวัฒนธรรมการบริหารความเสี่ยงภายในองค์กร มีการกระตุ้นและส่งเสริมให้พนักงานทุกคนของบริษัท มีจิตสำนึกและมีส่วนร่วมในการบริหารความเสี่ยงที่เกี่ยวข้องกับหน่วยงานที่ตนรับผิดชอบ และดำเนินการเพื่อให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการทำงานของพนักงาน

โครงสร้างการกำกับดูแลการบริหารความเสี่ยง (Risk Governance)

โครงสร้างการกำกับดูแลการบริหารความเสี่ยงของบริษัท อยู่บนหลักการ Three Lines of Defense โดยการกำกับดูแลส่วนที่ 1 จะเป็นการบริหารความเสี่ยงในการปฏิบัติงานของแต่ละหน่วยงาน ซึ่งอยู่ภายใต้การควบคุมดูแลของคณะกรรมการบริษัท ประธานเจ้าหน้าที่บริหาร และผู้บริหาร การกำกับดูแลส่วนที่ 2 เป็นการกำกับดูแลประสิทธิภาพและประสิทธิผลของการบริหารความเสี่ยงทั่วทั้งองค์กรโดยคณะกรรมการบริหารความเสี่ยง ฝ่ายบริหารความเสี่ยง และฝ่ายดูแลการปฏิบัติตามกฎหมาย และการกำกับดูแลส่วนที่ 3 จะเกี่ยวข้องกับ การสร้างความเชื่อมั่นเกี่ยวกับประสิทธิผลของการบริหารความเสี่ยงผ่านกลไกการตรวจสอบ ซึ่งประกอบด้วย คณะกรรมการตรวจสอบ ฝ่ายตรวจสอบภายใน และผู้ตรวจสอบภายนอก

การกำกับดูแลส่วนที่ 1 การปฏิบัติงาน ของแต่ละหน่วยงาน	การกำกับดูแลส่วนที่ 2 การกำกับดูแล การบริหารความเสี่ยง	การกำกับดูแลส่วนที่ 3 การสร้างความเชื่อมั่น ผ่านกลไกการตรวจสอบ
คณะกรรมการบริษัท	คณะกรรมการบริหารความเสี่ยง	คณะกรรมการตรวจสอบ
ประธานเจ้าหน้าที่บริหาร / ผู้บริหาร	ฝ่ายบริหารความเสี่ยง	ฝ่ายตรวจสอบภายใน
ฝ่าย / หน่วยงาน	ฝ่ายดูแลการปฏิบัติตามกฎหมาย	ผู้ตรวจสอบภายนอก

การกำกับดูแลส่วนที่ 1 – การบริหารความเสี่ยงในการปฏิบัติงานของแต่ละหน่วยงาน คณะกรรมการบริษัท

คณะกรรมการบริษัทมีหน้าที่ความรับผิดชอบดังนี้

1. กำหนดกลยุทธ์ในการดำเนินธุรกิจให้สอดคล้องกับกรอบและนโยบายการบริหารความเสี่ยง รวมถึงระดับความเสี่ยงที่ยอมรับได้ของบริษัท
2. พิจารณานุมัติกรอบและนโยบายการบริหารความเสี่ยง กลยุทธ์และแผนธุรกิจ และระดับความเสี่ยงที่ยอมรับได้ของบริษัท
3. กำกับดูแลบริษัท ในเรื่องต่อไปนี้
 - * การบริหารความเสี่ยงของบริษัท ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้
 - * การจัดทำรายงานสรุปสถานะความเสี่ยงที่ผ่านการกลั่นกรองจากคณะกรรมการบริหารความเสี่ยง เสนอต่อคณะกรรมการบริษัทเพื่อพิจารณาอย่างน้อยไตรมาสละหนึ่งครั้ง
 - * การทบทวนกรอบและนโยบายการบริหารความเสี่ยง อย่างน้อยปีละหนึ่งครั้ง และเมื่อเกิดเหตุการณ์สำคัญที่อาจส่งผลกระทบต่อความมั่นคงทางการเงินของบริษัท อย่างมีนัยสำคัญ
 - * การรักษาเงินกองทุนของบริษัท ให้อยู่ในระดับที่มั่นคงและเพียงพอที่จะรองรับการดำเนินธุรกิจทั้งในปัจจุบันและอนาคตอย่างเหมาะสม
 - * การสนับสนุนการดำเนินงานของคณะกรรมการบริหารความเสี่ยงและฝ่ายบริหารความเสี่ยงให้สามารถปฏิบัติตามหน้าที่อย่างมีประสิทธิภาพและสมบูรณ์ และได้รับการจัดสรรทรัพยากรให้เพียงพอ

ประธานเจ้าหน้าที่บริหารและผู้บริหาร

ประธานเจ้าหน้าที่บริหารและผู้บริหารมีหน้าที่ความรับผิดชอบดังนี้

1. กำหนดทิศทางในการจัดทำกรอบระดับความเสี่ยงที่ยอมรับได้
2. รับผิดชอบการดำเนินธุรกิจประจำวันให้สอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจ กรอบและนโยบายการบริหารความเสี่ยง
3. จัดให้มีการให้ความรู้แก่บุคลากรเกี่ยวกับกรอบและนโยบายการบริหารความเสี่ยง และทำให้มั่นใจว่าบุคลากรนำไปใช้ปฏิบัติงานจริง

ฝ่าย/หน่วยงาน

ฝ่าย/หน่วยงาน มีหน้าที่ความรับผิดชอบดังนี้

1. เป็นเจ้าของความเสี่ยงในหน่วยงานของตนเอง
2. บูรณาการกลยุทธ์ การบริหารความเสี่ยง และการบริหารเงินกองทุนในการทำงาน และควบคุมดูแลให้ความเสี่ยงในหน่วยงานของตนเองอยู่ในระดับความเสี่ยงที่ยอมรับได้
3. ทบทวนและปรับปรุงมาตรการบริหารความเสี่ยงให้มีความเหมาะสมและทันกาลอย่างต่อเนื่อง

การกำกับดูแลส่วนที่ 2 – การกำกับดูแลประสิทธิภาพและประสิทธิผลของการบริหารความเสี่ยงทั่วทั้งองค์กร

คณะกรรมการบริหารความเสี่ยง

บริษัทฯ ต้องจัดให้มีคณะกรรมการบริหารความเสี่ยงอย่างน้อยห้าคน ให้เหมาะสมกับขนาด ลักษณะ และความซับซ้อนของกิจกรรมของบริษัทฯ ตามหลักเกณฑ์ดังต่อไปนี้

1. ได้รับมติแต่งตั้งจากคณะกรรมการบริษัทหรือที่ประชุมผู้ถือหุ้นให้เป็นกรรมการบริหารความเสี่ยง
2. กรรมการบริหารความเสี่ยงอย่างน้อยหนึ่งคนต้องเป็นกรรมการในคณะกรรมการบริษัท
3. กรรมการบริหารความเสี่ยงรายอื่นต้องเป็นกรรมการในคณะกรรมการบริษัท หรือเป็นผู้บริหารของบริษัทฯ หรือเป็นผู้ทรงคุณวุฒิที่มีความรู้ความเข้าใจเกี่ยวกับความเสี่ยงในการดำเนินธุรกิจของบริษัทฯ

คณะกรรมการบริหารความเสี่ยงมีหน้าที่ความรับผิดชอบดังนี้

1. กำหนดกรอบและนโยบายการบริหารความเสี่ยง เสนอต่อคณะกรรมการบริษัทเพื่อพิจารณาอนุมัติ โดยต้องครอบคลุมความเสี่ยงที่สำคัญตามที่เห็นเหมาะสม
2. กำกับดูแลการบริหารความเสี่ยงโดยรวมของบริษัทฯ และทำให้มั่นใจว่าบริษัทฯ ได้ดำเนินกิจการภายใต้กรอบและนโยบายการบริหารความเสี่ยง
3. ประชุมเป็นประจําอย่างน้อยไตรมาสละหนึ่งครั้งเพื่อติดตามสถานะความเสี่ยงและการเปลี่ยนแปลงความเสี่ยงของบริษัทฯ รวมถึงติดตามความคืบหน้าในการบริหารความเสี่ยง และให้ข้อเสนอแนะในสิ่งที่ต้องดำเนินการเพิ่มเติม เพื่อให้สอดคล้องกับกรอบและนโยบายการบริหารความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้ของบริษัทฯ และรายงานให้คณะกรรมการบริษัททราบอย่างน้อยไตรมาสละหนึ่งครั้ง
4. ประเมินความเสี่ยงพอ ประสิทธิภาพ และประสิทธิผลในการบริหารความเสี่ยงของบริษัทฯ รวมถึงทบทวนความถูกต้องเหมาะสมของกรอบและนโยบายการบริหารความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อเกิดเหตุการณ์สำคัญที่อาจส่งผลกระทบต่อความมั่นคงทางการเงินของบริษัทฯ อย่างมีนัยสำคัญ
5. ควบคุมดูแลให้การบริหารความเสี่ยงของบริษัทฯ ดำเนินการสอดคล้องกับกฎเกณฑ์การกำกับดูแลและแนวปฏิบัติที่ดีของหน่วยงานกำกับดูแลและองค์กรอื่นที่เกี่ยวข้อง
6. ปฏิบัติงานอื่นใดตามที่คณะกรรมการบริษัทมอบหมาย

ฝ่ายบริหารความเสี่ยง

ฝ่ายบริหารความเสี่ยงมีหน้าที่ความรับผิดชอบหรือจัดให้มีการดำเนินการดังต่อไปนี้

1. สนับสนุนการทำงานของคณะกรรมการบริษัท คณะกรรมการบริหารความเสี่ยง และผู้บริหาร ในประเด็นที่เกี่ยวข้องกับการบริหารความเสี่ยงของบริษัทฯ
2. ระบุความเสี่ยงที่สำคัญที่บริษัทฯ เผชิญอยู่ในปัจจุบัน และที่คาดว่าจะเกิดขึ้นในอนาคต
3. ประเมิน รวบรวม และติดตาม รวมถึงช่วยให้หน่วยงานภายในบริษัทฯ สามารถบริหารความเสี่ยงของบริษัทฯ ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้

4. สร้างแนวทางการประเมินลักษณะความเสี่ยงของบริษัทฯ ที่เป็นการคาดการณ์ไปข้างหน้า โดยการประเมินสภาพแวดล้อมความเสี่ยงทั้งภายในและภายนอกอย่างต่อเนื่อง เพื่อระบุและประเมินความเสี่ยงที่มีโอกาสจะเกิดขึ้นได้ทันทั้งที่
5. จัดทำการวิเคราะห์สถานการณ์และการทดสอบภาวะวิกฤตภายใต้กรอบและนโยบายการบริหารความเสี่ยง
6. จัดทำรายงานสถานะความเสี่ยงที่ระบุถึงความเสี่ยงที่บริษัทฯ เผชิญอยู่ และรายงานการปฏิบัติตามนโยบายการบริหารความเสี่ยง นำเสนอแก่คณะกรรมการบริษัทและผู้บริหาร
7. จัดทำเอกสารและรายงานการเปลี่ยนแปลงสำคัญที่ส่งผลกระทบต่อกรอบและนโยบายการบริหารความเสี่ยง ต่อคณะกรรมการบริหารความเสี่ยง เพื่อให้มั่นใจว่ามีการนำไปใช้จริงและมีการปรับปรุงอยู่เสมอ
8. ดำเนินการอื่นใดเพื่อให้บริษัทฯ สามารถดำรงภาพรวมของลักษณะความเสี่ยงที่ยอมรับได้ทั้งระดับบริษัท และระดับกลุ่มธุรกิจ
9. ประเมินตนเองในเรื่องของคุณภาพการทำงาน และติดตามการปรับปรุงใดๆ ที่จำเป็นเพื่อเพิ่มประสิทธิภาพของฝ่ายบริหารความเสี่ยง

หัวหน้าฝ่ายบริหารความเสี่ยง

บริษัทฯ ต้องจัดให้มีหัวหน้าฝ่ายบริหารความเสี่ยงซึ่งเป็นผู้ที่มีความรู้ ความเข้าใจ และทักษะที่จำเป็นต่อการบริหารความเสี่ยงจากการประกอบธุรกิจประจักษ์ของบริษัทฯ และสามารถเข้าถึงแหล่งข้อมูลที่เกี่ยวข้องได้อย่างสมบูรณ์

หัวหน้าฝ่ายบริหารความเสี่ยงมีหน้าที่ความรับผิดชอบดังนี้

1. จัดให้มีการนำเสนอผลการบริหารความเสี่ยงต่อคณะกรรมการบริหารความเสี่ยงและผู้บริหารเป็นประจำอย่างน้อยไตรมาสละหนึ่งครั้ง โดยมีรายละเอียดดังต่อไปนี้เป็นอย่างน้อย
 - * การรายงานกิจกรรมที่เกี่ยวข้องการบริหารความเสี่ยงแบบองค์รวมของบริษัทฯ รวมถึงการเปลี่ยนแปลงของกรอบการบริหารความเสี่ยง นโยบายบริหารความเสี่ยง และแผนธุรกิจ
 - * การแสดงหลักฐานของกระบวนการติดตามความเสี่ยงหลักจากทะเบียนความเสี่ยง
2. จัดให้มีการรายงานผลการบริหารความเสี่ยงเพื่อทบทวนความเพียงพอของกรอบและนโยบายการบริหารความเสี่ยงต่อคณะกรรมการบริหารความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงทางการเงินหรือภาพรวมของความเสี่ยงของบริษัทฯ อย่างมีนัยสำคัญ

ฝ่ายดูแลการปฏิบัติตามกฎหมาย

ฝ่ายดูแลการปฏิบัติตามกฎหมายมีหน้าที่ความรับผิดชอบดังนี้

1. เป็นศูนย์กลางในการให้คำแนะนำ คำปรึกษาเกี่ยวกับการปฏิบัติตามกฎหมาย รวมถึงจัดทำคู่มือการปฏิบัติตามกฎหมายเป็นลายลักษณ์อักษร และอบรมให้ความรู้พนักงานอย่างสม่ำเสมอ
2. พัฒนาระบบบริหารความเสี่ยงด้านการปฏิบัติตามกฎหมายโดยระบุความเสี่ยง ประเมินความเสี่ยง กำหนดวิธีการจัดการความเสี่ยง ติดตาม รายงานผลการประเมินการเปลี่ยนแปลงความเสี่ยงด้านการปฏิบัติตามกฎหมาย ซึ่งระบุสาเหตุการไม่ปฏิบัติตามกฎหมายและแนวทางการแก้ไข รวมถึงปัญหาที่ได้รับการแก้ไขแล้ว เสนอต่อผู้บริหาร คณะกรรมการชด้อยที่มีหน้าที่ติดตามการดำเนินงานของหน่วยธุรกิจที่มีความเป็นกลาง หรือคณะกรรมการบริษัท

3. ประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อจัดทำและดำเนินแผนการบริหารความเสี่ยงด้านการปฏิบัติตามกฎหมายเป็นประจำทุกปี รวมถึงการดำเนินการแก้ไขปัญหที่อาจทำให้ไม่สามารถปฏิบัติตามกฎหมายได้
4. ติดตามให้มีการปฏิบัติตามกฎหมายและรายงานผลการปฏิบัติตามกฎหมายประจำปีต่อคณะกรรมการบริษัทหรือคณะกรรมการชุดย่อยที่มีหน้าที่ติดตามการดำเนินงานของหน่วยธุรกิจซึ่งมีความเป็นกลาง รวมถึงรายงานการฝ่าฝืนกฎหมายและการสอบสวนผู้บริหาร และรายงานการถูกปรับหรือถูกดำเนินการทางกฎหมายใด ๆ โดยหน่วยงานกำกับดูแลหรือหน่วยงานราชการอื่นที่เกี่ยวข้อง
5. เป็นผู้ประสานงานกับหน่วยงานกำกับดูแลในนามของบริษัท และปฏิบัติงานในหน้าที่เฉพาะ อาทิ งานในด้านการป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย
6. ส่งเสริมและรักษาไว้ซึ่งวัฒนธรรมองค์กรที่มีจริยธรรมซึ่งให้ความสำคัญกับการประพฤติปฏิบัติที่มีความรับผิดชอบและปฏิบัติตามข้อผูกพันภายในและภายนอก
7. ระบุ ประเมิน รายงาน และปฏิบัติตามข้อบังคับทางกฎหมายและกฎระเบียบข้อบังคับที่สำคัญรวมถึงภาระหน้าที่ที่มีต่อหน่วยงานกำกับดูแลและความเสี่ยงที่เกี่ยวข้อง
8. ทำให้มั่นใจว่าบริษัทฯ มีการติดตามดูแลและมีนโยบาย กระบวนการทำงานและการควบคุมที่เหมาะสมในส่วนที่สำคัญตามกฎหมาย กฎระเบียบ ข้อบังคับ และจริยธรรม
9. จัดให้มีการฝึกอบรมอย่างสม่ำเสมอเกี่ยวกับข้อบังคับทางกฎหมายและกฎระเบียบ ข้อบังคับที่สำคัญให้แก่พนักงานในตำแหน่งที่มีความรับผิดชอบสูง หรือพนักงานที่เกี่ยวข้องกับกิจกรรมที่มีความเสี่ยงสูง
10. ประสานงานและสนับสนุนการดำเนินงานเกี่ยวกับการรายงานที่มีชั้นความลับเพื่อป้องกันการรั่วไหลของข้อมูล และให้มั่นใจว่ามีการจัดส่งรายงานที่กฎหมายกำหนด
11. กำกับดูแล ติดตามข้อบกพร่องและการละเมิดการปฏิบัติตามกฎระเบียบ รวมถึงทำให้มั่นใจว่ามีการดำเนินการทางวินัยอย่างเพียงพอและมีการรายงานที่จำเป็นตามเงื่อนไขของกฎหมายต่อหน่วยงานกำกับดูแล
12. ประเมินตนเองในเรื่องของกระบวนการติดตามการปฏิบัติตามกฎหมายของบริษัทฯ และติดตามการปรับปรุงใด ๆ ที่จำเป็นเพื่อเพิ่มประสิทธิภาพของหน่วยงานดูแลการปฏิบัติตามกฎหมาย

การกำกับดูแลส่วนที่ 3 – การสร้างความเชื่อมั่นเกี่ยวกับประสิทธิผลของการบริหารความเสี่ยงผ่านกลไกการตรวจสอบ

คณะกรรมการตรวจสอบ

คณะกรรมการตรวจสอบมีหน้าที่ความรับผิดชอบในการสอบทานและประเมินผลให้บริษัทฯ มีระบบการควบคุมภายใน ระบบการตรวจสอบภายใน และระบบการบริหารความเสี่ยงที่เหมาะสม มีประสิทธิผล และรัดกุมตามกรอบที่ได้รับการยอมรับเป็นมาตรฐานสากลและกฎเกณฑ์การกำกับดูแลที่เกี่ยวข้อง

ฝ่ายตรวจสอบภายใน

ฝ่ายตรวจสอบภายในมีหน้าที่ความรับผิดชอบดังนี้

1. ตรวจสอบให้บริษัทฯ มีระบบการควบคุมภายในที่เพียงพอ มีประสิทธิภาพ และประสิทธิผลเพื่อบริหารความเสี่ยงให้อยู่ในระดับที่ควบคุมได้และเป็นไปตามกระบวนการกำกับดูแลกิจการที่ดี
2. ตรวจสอบการปฏิบัติงานของหน่วยงานภายในบริษัทฯ ว่ามีการปฏิบัติตามกฎหมายที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัทฯ
3. ตรวจสอบประสิทธิภาพ และประสิทธิผลของระบบการบริหารความเสี่ยงตามกรอบและนโยบายการบริหารความเสี่ยงรวมที่ได้รับความเห็นชอบจากคณะกรรมการบริษัท
4. ตรวจสอบ ประเมินความเสี่ยงและแนวทางการบริหารจัดการการทุจริต และการเกิดข้อผิดพลาด การละเลย และรายการผิดปกติดังอื่น ๆ
5. กำหนด นำไปใช้ และรักษาไว้ซึ่งแผนการตรวจสอบตามระดับความเสี่ยง (Risk-Based Audit Plan)
6. ติดตามและประเมินความเพียงพอและประสิทธิผลของนโยบาย กระบวนการทำงาน และการจัดทำเอกสาร รวมถึงการควบคุมการดำเนินงานทั้งในระดับบริษัทและระดับกลุ่มธุรกิจ
7. ประเมินความน่าเชื่อถือ ความถูกต้องสมบูรณ์ และประสิทธิผลของกระบวนการในการจัดการสารสนเทศ รวมถึงวิธีการที่ใช้ในการระบุ วัตถุประสงค์ จำแนกประเภท และรายงานข้อมูลที่ใช้ในบริษัทฯ
8. ติดตามและประเมินประสิทธิผลของหน่วยงานของบริษัทฯ และเปิดเผยประเด็นสำคัญที่พบให้แก่หน่วยงานดังกล่าว เพื่อให้ทำการปรับปรุงต่อไป
9. ประสานงานกับผู้ตรวจสอบภายนอกเพื่อเพิ่มประสิทธิภาพการตรวจสอบและลดความซ้ำซ้อนของกิจกรรมการตรวจสอบ
10. ประเมินคุณภาพของการทำงานของผู้ตรวจสอบภายนอก (หากเกี่ยวข้อง)
11. สรุปการรายงานผลการตรวจสอบภายในประจำปีจัดทำขึ้น ซึ่งผ่านการพิจารณาจากคณะกรรมการตรวจสอบหรือคณะกรรมการบริษัทอย่างน้อยปีละหนึ่งครั้ง

ผู้ตรวจสอบภายนอก

ผู้ตรวจสอบภายนอกมีหน้าที่ความรับผิดชอบในการรายงานผลเกี่ยวกับความเสี่ยงและความล้มเหลวของกระบวนการควบคุม รวมถึงจุดบกพร่องของการกำกับดูแลกิจการที่ดี (หากตรวจพบ) ต่อคณะกรรมการตรวจสอบอย่างน้อยปีละหนึ่งครั้ง

การสนับสนุนจากผู้บริหาร (Tone at the Top)

การสนับสนุนจากผู้บริหารระดับสูงถือเป็นปัจจัยสำคัญต่อความสำเร็จของการบริหารความเสี่ยง การสนับสนุนจากผู้บริหารจะช่วยให้เกิดการบริหารความเสี่ยงอย่างเป็นรูปธรรมในบริษัทฯ และช่วยยกระดับความสำคัญของการบริหารความเสี่ยง ผู้บริหารต้องเป็นผู้นำในการบริหารความเสี่ยงและสนับสนุนให้มีการปลูกฝังวัฒนธรรมการบริหารความเสี่ยงในบริษัทฯ อย่างต่อเนื่อง การขาดการสนับสนุนจากผู้บริหารจะทำให้บุคลากรในองค์กรขาดความรู้ความเข้าใจและความกระตือรือร้น มองข้ามความสำคัญของการบริหารความเสี่ยง และทำให้การปลูกฝังวัฒนธรรมการบริหารความเสี่ยงเป็นไปได้ยาก

ผู้บริหารต้องกำหนดทิศทาง นโยบาย และแนวปฏิบัติในการบริหารความเสี่ยงและสื่อสารวัตถุประสงค์และประโยชน์ที่จะได้รับจากการบริหารความเสี่ยงขององค์กรไปยังพนักงานทุกคนเพื่อให้เกิดความตระหนักและเห็นคุณค่าของการบริหารความเสี่ยง

การบูรณาการการบริหารความเสี่ยง (Risk Management Integration)

บริษัท ต้องมีการบูรณาการการบริหารความเสี่ยงเข้ากับการตัดสินใจทางธุรกิจ การดำรงเงินกองทุน การกำกับดูแลกิจการ และการควบคุมภายในของบริษัท เพื่อให้ความเสี่ยงขององค์กรที่มีอยู่ถูกจัดการอย่างเป็นระบบ และการตัดสินใจทางธุรกิจได้พิจารณาความเสี่ยงและผลตอบแทนที่จะได้รับควบคู่กัน

บริษัท ต้องประมาณการเงินกองทุนที่จำเป็นในการประกอบธุรกิจ พิจารณาคุณภาพและความสามารถในการเข้าถึงแหล่งเงินทุนของบริษัท ข้อจำกัดในการเพิ่มเงินทุน และจัดให้มีกลไกควบคุมความสามารถในการเพิ่มเงินทุนในกรณีที่มีความเร่งด่วน รวมทั้งจัดให้มีการวิเคราะห์ความต่อเนื่องในการดำเนินธุรกิจ โดยกำหนดปัจจัยที่ใช้ในการทดสอบสถานการณ์ที่เหมาะสม

บริษัท ต้องจัดทำแผนการดำเนินการ (Management Action) อันเป็นผลมาจากการวิเคราะห์ความต่อเนื่องในการดำเนินธุรกิจ ในกรณีที่ผลการทดสอบสถานการณ์ดังกล่าวละเมิดระดับความเสี่ยงที่ยอมรับได้ของบริษัท รวมทั้งต้องจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ในกรณีที่เกิดเหตุการณ์ที่ทำให้บริษัท ไม่สามารถดำเนินธุรกิจประจำวันได้อย่างต่อเนื่องและเป็นไปตามปกติ

การสร้างความตระหนักและความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยง (Risk Management Awareness)

บริษัท ต้องจัดให้มีการอบรมพัฒนาบุคลากรของบริษัท ให้มีความรู้ ความเข้าใจ ความระมัดระวัง และความตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นและมีผลกระทบต่อฝ่าย/หน่วยงาน ต่อองค์กร และต่อผู้เกี่ยวข้อง รวมทั้งส่งเสริมให้มีการแลกเปลี่ยนข้อมูลความเสี่ยงระหว่างฝ่าย/หน่วยงานต่างๆ ภายในองค์กร เพื่อให้บริษัทสามารถบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

บริษัท ต้องปลูกฝังให้การตัดสินใจใดก็ตามในบริษัท ต้องคำนึงถึงความเสี่ยงที่เกี่ยวข้อง ต้นทุน และผลประโยชน์ที่จะได้รับควบคู่กันเสมอ

ส่วนที่ 3 – ขอบเขตของการบริหารความเสี่ยง

ขอบเขตการบริหารความเสี่ยงของบริษัทฯ ต้องครอบคลุมความเสี่ยงและกิจกรรมหลักที่เกี่ยวข้อง ดังนี้

ประเภทของความเสี่ยง (Types of Risk)

การบริหารความเสี่ยงของบริษัทฯ ครอบคลุมความเสี่ยง 9 ประเภท ดังนี้

1. **ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)** หมายถึง ความเสี่ยงอันเนื่องมาจากการดำเนินนโยบาย การกำหนดแผนกลยุทธ์ แผนการดำเนินงาน และการนำไปปฏิบัติที่ไม่เหมาะสม หรือไม่สอดคล้องกับปัจจัยภายในและสภาพแวดล้อมภายนอก
2. **ความเสี่ยงด้านปฏิบัติการ (Operational Risk)** หมายถึง ความเสี่ยงอันเนื่องมาจากการขาดการกำกับดูแลหรือการควบคุมที่ดี ที่เกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน บุคลากร ระบบงาน ระบบเทคโนโลยีสารสนเทศ การกำกับดูแลข้อมูล ความปลอดภัยของข้อมูล หรือเหตุการณ์ภายนอก
3. **ความเสี่ยงด้านตลาด (Market Risk)** หมายถึง ความเสี่ยงอันเนื่องมาจากการเปลี่ยนแปลงของอัตราดอกเบี้ย อัตราแลกเปลี่ยนเงินตราต่างประเทศ ราคาของสินทรัพย์ที่ลงทุน ราคาตราสารในตลาดเงินตลาดทุน และราคาสินค้าโภคภัณฑ์
4. **ความเสี่ยงด้านเครดิต (Credit Risk)** หมายถึง ความเสี่ยงอันเนื่องมาจากคู่สัญญาไม่สามารถปฏิบัติตามภาระผูกพันที่ได้ตกลงไว้กับบริษัทฯ รวมถึงการที่คู่สัญญาอาจถูกปรับอันดับความเสี่ยงด้านเครดิต
5. **ความเสี่ยงด้านสภาพคล่อง (Liquidity Risk)** หมายถึง ความเสี่ยงอันเนื่องมาจากการที่บริษัทฯ ไม่สามารถชำระหนี้สินและภาระผูกพันเมื่อถึงกำหนด เนื่องจากไม่สามารถเปลี่ยนสินทรัพย์เป็นเงินสดได้ หรือสามารถจัดหาเงินมาชำระได้แต่ด้วยต้นทุนที่สูงเกินกว่าระดับที่ยอมรับได้
6. **ความเสี่ยงด้านชื่อเสียง (Reputation Risk)** หมายถึง ความเสี่ยงที่เกิดจากความเสียหายต่อบริษัทฯ อันเนื่องมาจากการเสื่อมเสียชื่อเสียงเนื่องจากลูกค้า คู่ค้า ผู้ถือหุ้น และ/หรือหน่วยงานกำกับดูแล ที่มีมุมมองภาพลักษณ์ต่อบริษัทฯ ในแง่ลบ
7. **ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)** หมายถึง ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินธุรกิจ ซึ่งจะมีผลกระทบต่อชื่อเสียง ระบบ หรือการปฏิบัติงานของบริษัทฯ รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์
8. **ความเสี่ยงอุบัติใหม่ (Emerging Risk)** หมายถึง ความเสี่ยงที่อาจเกิดใหม่ซึ่งเป็นความสูญเสียที่ไม่เคยปรากฏขึ้นมาก่อน และยากต่อการประมาณการทั้งในเชิงโอกาสและความรุนแรงในการเกิด เนื่องมาจากการเปลี่ยนแปลงของปัจจัยแวดล้อม อาทิ การเมือง กฎหมาย สังคม เทคโนโลยี สภาพแวดล้อมทางกายภาพ รวมถึงการเปลี่ยนแปลงทางธรรมชาติ

9. **ความเสี่ยงภายในกลุ่มธุรกิจ (Group Risk)** หมายถึง ความเสี่ยงที่บริษัท อาจได้รับผลกระทบเชิงลบจากเหตุการณ์ (ทั้งที่เป็นทางการเงินและที่ไม่ใช่ทางการเงิน) จากธุรกิจในกลุ่มเดียวกัน นอกจากนี้ ยังรวมถึงความเสี่ยงที่เกิดจากความมั่นคงทางการเงินของกลุ่มธุรกิจทั้งหมด หรือบริษัทภายในกลุ่มธุรกิจซึ่งได้รับผลกระทบจากเหตุการณ์ของธุรกิจใดธุรกิจหนึ่ง ซึ่งเป็นทั้งเหตุการณ์ที่เกิดขึ้นภายในกลุ่มธุรกิจเอง หรือเหตุการณ์ภายนอกที่กระทบต่อกลุ่มธุรกิจ

กิจกรรมหลัก (Core Activity)

การบริหารความเสี่ยงของบริษัท จะต้องครอบคลุมกิจกรรมหลักที่เกี่ยวข้องอย่างครบถ้วน

ส่วนที่ 4 – กระบวนการการบริหารความเสี่ยง

บริษัท ต้องมีการดำเนินการตามกระบวนการบริหารความเสี่ยงซึ่งประกอบด้วยขั้นตอนดังต่อไปนี้

1. การระบุความเสี่ยง (Risk Identification)

บริษัท ต้องระบุว่ามีความเสี่ยงใดที่อาจเกิดขึ้นทั้งภายในและภายนอกองค์กรซึ่งจะมีผลกระทบต่อชื่อเสียง กลยุทธ์ การดำเนินงาน และการบรรลุวัตถุประสงค์ของบริษัท ทั้งด้านการเงินและที่ไม่ใช่ด้านการเงิน และอาจทำให้ภาพความเสี่ยงรวมของบริษัท เปลี่ยนแปลงไป

ในการระบุความเสี่ยงนั้น จะต้องมีการระบุสาเหตุที่เกี่ยวข้อง และผลกระทบของความเสี่ยงที่จะเกิดขึ้นในด้านต่าง ๆ อาทิเช่น ผลกระทบด้านชื่อเสียง ผลกระทบด้านการเงิน (เงินกองทุน รายได้ ผลกำไร และสภาพคล่อง) ผลกระทบด้านการดำเนินงาน (การหยุดชะงักของธุรกิจ) และผลกระทบด้านบุคลากร ควบคุมด้วย

ฝ่ายบริหารความเสี่ยงเป็นผู้ดำเนินการให้มีการระบุความเสี่ยงโดยใช้เทคนิควิธีการระบุความเสี่ยงที่เหมาะสม อาทิเช่น การจัดทำแบบสอบถามเพื่อสำรวจความคิดเห็นจากผู้บริหาร การใช้ข้อมูลภายในบริษัท เพื่อประกอบการตัดสินใจ การใช้ข้อมูลจากภายนอกเพื่อให้ทราบถึงสถานการณ์และแนวโน้มของความเสี่ยงอุบัติใหม่ที่เกิดขึ้น และการจัดประชุมเพื่อระดมและสรุปความคิดเห็น

ฝ่ายบริหารความเสี่ยงเป็นผู้นำเสนอผลสรุปของการระบุความเสี่ยงหลักต่อคณะกรรมการบริหารความเสี่ยงเพื่อพิจารณาจัดลำดับความสำคัญและสรุปความเสี่ยงหลักของบริษัท ในแต่ละปี ทั้งนี้ คณะกรรมการบริหารความเสี่ยงจะเป็นผู้พิจารณากำหนดเจ้าของความเสี่ยง (Risk Owner) เพื่อรับผิดชอบในการบริหารความเสี่ยงหลักแต่ละความเสี่ยงให้อยู่ในระดับที่ยอมรับได้และช่วงความเบี่ยงเบนที่ยอมรับได้สำหรับแต่ละความเสี่ยง

2. การประเมินความเสี่ยง (Risk Assessment)

หลังจากที่ได้ระบุความเสี่ยงหลักของบริษัท แล้ว เจ้าของความเสี่ยงจะต้องประเมินความเสี่ยง โดยการประเมินโอกาส และ/หรือ ผลกระทบของความเสี่ยงที่มีต่อบริษัท อย่างต่อเนื่อง

เจ้าของความเสี่ยงเป็นผู้รับผิดชอบในการนำเสนอช่วงความเบี่ยงเบนที่ยอมรับได้ และกำหนดดัชนีชี้วัดความเสี่ยงและขีดจำกัดความเสี่ยงที่เหมาะสมและสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้และช่วงความเบี่ยงเบนที่ยอมรับได้ และนำช่วงความเบี่ยงเบนที่ยอมรับได้ ดัชนีชี้วัดความเสี่ยง และขีดจำกัดความเสี่ยงที่ได้รับการอนุมัติจากคณะกรรมการบริหารความเสี่ยง มาใช้ในการติดตามสถานะความเสี่ยงและการเปลี่ยนแปลงของความเสี่ยงหลักของบริษัท ตามรอบระยะเวลาที่เหมาะสม

3. การตอบสนองความเสี่ยง (Risk Response)

บริษัท จะต้องมีการตอบสนองความเสี่ยงให้สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ ช่วงความเบี่ยงเบนที่ยอมรับได้ และขีดจำกัดความเสี่ยงที่ได้กำหนดไว้ โดยเจ้าของความเสี่ยงต้องประเมินมาตรการที่ใช้ในการบริหารความเสี่ยงในปัจจุบันว่ามีประสิทธิภาพและประสิทธิผลเพียงใดทั้งในระยะสั้นและระยะยาว

การตอบสนองความเสี่ยงของบริษัทฯ ควรเน้นการหาวิธีการป้องกันสาเหตุที่ก่อให้เกิดความเสี่ยง แต่หากการป้องกันนั้นยังไม่มีประสิทธิผลเพียงพอหรือเกิดเหตุการณ์ที่นอกเหนือการควบคุมและก่อให้เกิดความเสี่ยงที่ไม่พึงประสงค์ เจ้าของความเสี่ยงควรดำเนินการตอบสนองความเสี่ยงตามมาตรการที่มีอยู่ในปัจจุบันและพิจารณาหามาตรการบริหารความเสี่ยงที่จะดำเนินการเพิ่มในอนาคตพร้อมทั้งกำหนดระยะเวลาแล้วเสร็จ เพื่อให้มั่นใจว่าจะสามารถบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ในที่สุด

4. การควบคุมดูแลและติดตามความเสี่ยง (Risk Control and Monitoring)

บริษัทฯ จะต้องมีการควบคุมและติดตามประเมินผลการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการตอบสนองความเสี่ยงเป็นไปอย่างที่ได้วางแผนไว้ และความเสี่ยงหลักของบริษัทฯ ได้รับการบริหารจัดการให้อยู่ในระดับที่ยอมรับได้

เนื่องจากสภาวะแวดล้อมทั้งภายในและภายนอกองค์กรมีการเปลี่ยนแปลงอยู่ตลอดเวลา ความเสี่ยงเดิมที่บริษัทฯ เผชิญอยู่อาจมีการเปลี่ยนแปลงหรือมีความเสี่ยงรูปแบบใหม่เกิดขึ้น การเปลี่ยนแปลงของเทคนิคความรู้ และความก้าวหน้าทางเทคโนโลยี อาจก่อให้เกิดเทคนิคหรือมาตรการใหม่ในการบริหารความเสี่ยงที่มีประสิทธิภาพดียิ่งขึ้น ดังนั้น บริษัทฯ จึงต้องมีการควบคุมดูแลและติดตามความเสี่ยงอย่างต่อเนื่อง มีการทบทวนความเสี่ยงหลักที่จะส่งผลกระทบต่อองค์กรในอนาคต และเตรียมพร้อมหาวิธีและมาตรการในการจัดการล่วงหน้า รวมถึงการทบทวนและปรับปรุงมาตรการบริหารความเสี่ยง ดัชนีชี้วัดความเสี่ยง และขีดจำกัดความเสี่ยงให้มีความเหมาะสมกับสถานการณ์อยู่เสมอ

5. การรายงานข้อมูลการบริหารความเสี่ยง (Risk Reporting)

บริษัทฯ จะต้องมียระบบการรายงานข้อมูลการบริหารความเสี่ยงและสถานะความเสี่ยงดังต่อไปนี้

ลำดับ	รายงาน	ข้อกำหนด	การรายงานข้อมูล
1	รายงานผลการบริหารความเสี่ยงซึ่งครอบคลุมถึงสถานะความเสี่ยง ดัชนีชี้วัดความเสี่ยง ประสิทธิภาพ และประสิทธิผลของมาตรการบริหารความเสี่ยง	อย่างน้อย ไตรมาสละหนึ่งครั้ง	ผู้บริหาร และคณะกรรมการบริหาร ความเสี่ยง
2	รายงานเหตุการณ์สำคัญอันอาจส่งผลกระทบต่อความมั่นคงทางการเงินของบริษัทฯ อย่างมีนัยสำคัญ (ถ้ามี)	อย่างน้อย ไตรมาสละหนึ่งครั้ง	ผู้บริหาร และคณะกรรมการบริหาร ความเสี่ยง
3	สรุปรายงานสถานะความเสี่ยง และสรุปรายงานการปฏิบัติตามนโยบายการบริหารความเสี่ยง	อย่างน้อย ไตรมาสละหนึ่งครั้ง	คณะกรรมการบริษัท
4	รายงานผลการบริหารความเสี่ยง เพื่อประกอบการพิจารณาทบทวนความเพียงพอของกรอบการบริหารความเสี่ยงและนโยบายการบริหารความเสี่ยง	อย่างน้อย ปีละหนึ่งครั้ง	คณะกรรมการ บริหารความเสี่ยง และคณะกรรมการบริษัท
5	สรุปรายงานผลการประเมินการตรวจสอบรายปี รับผิดชอบโดยฝ่ายตรวจสอบภายใน	อย่างน้อยปีละหนึ่งครั้ง	คณะกรรมการตรวจสอบ และคณะกรรมการบริษัท