กรอบการบริหารความเสี่ยง

บริษัท กรุงเทพประกันสุขภาพ จำกัด (มหาชน) (บริษัทฯ) จัดทำกรอบการบริหารความเสี่ยงฉบับนี้ขึ้น เพื่อใช้เป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจในขั้นตอนการบริหารความเสี่ยงระดับองค์กรแก่ผู้บริหารและบุคลากรของบริษัทฯ รวมทั้งใช้เป็นเครื่องมือในการติดตามการดำเนินการตามมาตรการลดความเสี่ยงเพื่อนำไปสู่การบรรลุผลตามแผนบริหารความเสี่ยงต่อไป

1. คำนิยาม

ความเสี่ยง หมายถึง โอกาส/เหตุการณ์ที่มีความไม่แน่นอน หรือสิ่งที่ทำให้แผนงานหรือการดำเนินการอยู่ ณ ปัจจุบันไม่บรรลุวัตถุประสงค์/เป้าหมายที่กำหนดไว้ โดยก่อให้เกิดผลกระทบหรือความเสียหายต่อองค์กรในที่สุดทั้งในแง่ของผลกระทบที่เป็นตัวเงิน หรือ ผลกระทบที่มีต่อภาพลักษณ์และชื่อเสียงองค์กร ซึ่งอาจมีสาเหตุจากเหตุการณ์ภายในหรือเหตุการณ์ภายนอก

การบริหารความเสี่ยงองค์กร คือ กระบวนการที่ปฏิบัติโดยคณะกรรมการ ผู้บริหารและบุคลากรทุกคนในองค์กร เพื่อช่วยในการกำหนดกลยุทธ์และการดำเนินงาน โดยกระบวนการบริหารความเสี่ยงได้รับการออกแบบ เพื่อให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อองค์กร และสามารถจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ เพื่อให้ได้รับความมั่นใจอย่างสมเหตุสมผล ในการบรรลุวัตถุประสงค์ที่กำหนดไว้

2. โครงสร้างการกำกับดูแลการบริหารความเสี่ยง

โครงสร้างการกำกับดูแลการบริหารความเสี่ยงที่มีประสิทธิผลจะช่วยในการประเมิน ควบคุม และติดตามความเสี่ยงของแต่ละฝ่ายงาน และทำให้เกิดความมั่นใจว่าการปฏิบัติงานในการบริหารความเสี่ยงโดยทุกคนในองค์กรอยู่ภายใต้กรอบเดียวกัน

โครงสร้างการกำกับดูแลการบริหารความเสี่ยงของบริษัทฯ ประกอบด้วย

2.1 **คณะกรรมการบริษัทฯ** มีหน้าที่รับผิดชอบ ดังนี้

1) พิจารณาอนุมัติ

ก. กรอบการบริหารความเสี่ยงที่บริษัทจัดทำ

ข. นโยบายการบริหารความเสี่ยงและนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ค. กลยุทธ์และแผนธุรกิจ

ง. ระดับความเสี่ยงที่ยอมรับได้

จ. รายงานการบริหารความเสี่ยงแบบองค์รวมและการประเมินความเสี่ยงและความมั่นคงทางการเงินและความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท

2) กำหนดกลยุทธ์ในการดำเนินธุรกิจให้สอดคล้องกับกรอบการบริหารความเสี่ยงและนโยบายการบริหารความเสี่ยง รวมถึงระดับความเสี่ยงที่ยอมรับได้ของบริษัท

3) กำกับดูแลในเรื่อง ดังต่อไปนี้

ก. การบริหารความเสี่ยงของบริษัทให้อยู่ในระดับที่ยอมรับได้

ข. การจัดทำรายงานสรุปสถานะความเสี่ยง และสรุปรายงานการปฏิบัติตามมาตรการบริหารความเสี่ยงที่เหมาะสมและมีประสิทธิภาพ ที่ผ่านการกลั่นกรองจากคณะกรรมการบริหารความเสี่ยง และเสนอต่อคณะกรรมการบริษัทเพื่อพิจารณาอย่างน้อยไตรมาสละหนึ่งครั้ง

ค. การทบทวนกรอบการบริหารความเสี่ยงและนโยบายการบริหารความเสี่ยงอย่างน้อยปีละครั้งหรือทุกครั้งที่เกิดเหตุการณ์สำคัญที่อาจส่งผลกระทบต่อความมั่นคงทางการเงินของบริษัทอย่างมีนัยสำคัญ

ง. กำกับดูแลฐานะเงินกองทุนของบริษัท ให้อยู่ในระดับที่มั่นคงและเพียงพอที่จะรองรับการดำเนินธุรกิจทั้งในปัจจุบันและอนาคตอย่างเหมาะสม

จ. สนับสนุนการดำเนินงานของคณะกรรมการบริหารความเสี่ยงและหน่วยงานบริหารความเสี่ยงให้สามารถปฏิบัติตามหน้าที่อย่างมีประสิทธิภาพและสมบูรณ์ ได้รับการจัดสรรทรัพยากรให้อย่างเพียงพอ

ฉ. การใช้เทคโนโลยีสารสนเทศโดยสอดรับกับกลยุทธ์ในการดำเนินธุรกิจซึ่งมีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศ และคำนึงถึงการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต รวมทั้งความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

ช. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์

ซ. การกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ฌ. การนำนโยบายที่กำหนดมาจัดทำแนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม โดยมีการทบทวนอย่างน้อยปีละหนึ่งครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

ญ. การรายงานผลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาพรวมของบริษัท และรายงาน

ข้อมูลเกี่ยวกับปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศที่สำคัญ หรือที่อาจส่งผลกระทบในวงกว้าง หรือส่งผลกระทบต่อชื่อเสียงของบริษัท หรือต่อการดำเนินงานและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ตลอดจนผลการทดสอบและการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

2.2 **คณะกรรมการตรวจสอบ** มีหน้าที่รับผิดชอบ ดังนี้

1) สอบทานให้บริษัทมีการรายงานทางการเงินที่มีความสมบูรณ์ ถูกต้อง เชื่อถือได้ มีการเปิดเผยข้อมูลที่สำคัญโดยครบถ้วนและเป็นไปตามมาตรฐานบัญชีที่รับรองโดยทั่วไป
2) สอบทานและประเมินผลให้บริษัทมีระบบการควบคุมภายใน ระบบการตรวจสอบภายในและระบบการบริหารความเสี่ยงที่เหมาะสม มีประสิทธิผล และรัดกุม ตามกรอบที่ได้รับการยอมรับเป็นมาตรฐานสากล รวมถึงกำหนดอำนาจหน้าที่ ความรับผิดชอบของหน่วยงานตรวจสอบภายใน รวมถึงให้ความเห็นชอบแผนงานและขอบเขตการตรวจสอบด้านเทคโนโลยีสารสนเทศโดยมีการทบทวนแผนงานดังกล่าวอย่างน้อยปีละหนึ่งครั้งหรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
3) สอบทานให้บริษัทปฏิบัติตามกฎหมายว่าด้วยการประกันวินาศภัย ข้อกำหนดของสำนักงานและกฎหมายอื่นที่เกี่ยวข้องกับธุรกิจของบริษัท
4) พิจารณาคัดเลือก เสนอแต่งตั้งบุคคลซึ่งมีความเป็นอิสระเพื่อทำหน้าที่เป็นผู้สอบบัญชีของบริษัท และเสนอค่าตอบแทนบุคคลดังกล่าว รวมทั้งเข้าประชุมร่วมกับผู้สอบบัญชี โดยไม่มีผู้บริหารร่วมประชุมด้วย อย่างน้อยปีละหนึ่งครั้ง
5) ให้ข้อเสนอแนะแก่ฝ่ายบริหารเพื่อการกำกับดูแลการปฏิบัติงานให้เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล และรายงานต่อคณะกรรมการบริษัทเพื่อดำเนินการปรับปรุงแก้ไขภายในเวลาที่คณะกรรมการตรวจสอบเห็นสมควร ในกรณีที่คณะกรรมการตรวจสอบพบหรือมีข้อสงสัยว่ามีรายการหรือการกระทำ ดังต่อไปนี้
    ก. รายการที่เกิดความขัดแย้งทางผลประโยชน์
    ข. การทุจริต มีสิ่งปกติ หรือมีความบกพร่องที่สำคัญในระบบควบคุมภายใน
    ค. การฝ่าฝืนกฎหมายว่าด้วยการประกันวินาศภัย หรือกฎหมายอื่นที่เกี่ยวข้องกับธุรกิจของบริษัท

    หากคณะกรรมการบริษัทหรือผู้บริหารไม่ดำเนินการให้มีการปรับปรุงแก้ไขภายในเวลาตามที่คณะกรรมการตรวจสอบกำหนด คณะกรรมการตรวจสอบจะต้องรายงานต่อสำนักงาน (คปภ.) โดยทันที
6) แสดงความเห็นประกอบรายงานผลการประเมินการควบคุมภายในของบริษัทโดยรวมต่อคณะกรรมการบริษัท

2.3 **คณะกรรมการบริหารความเสี่ยง** มีหน้าที่รับผิดชอบ ดังนี้

1) กำหนดกรอบและนโยบายการบริหารความเสี่ยงเสนอต่อคณะกรรมการบริษัท เพื่อพิจารณาอนุมัติ โดยต้องครอบคลุมความเสี่ยงที่สำคัญที่ส่งผลกระทบต่อบริษัท ทั้งทางการเงินและที่มิใช่ทางการเงิน และกำกับดูแลการใช้เทคโนโลยีสารสนเทศให้สอดรับกับกลยุทธ์ในการดำเนินธุรกิจ รวมทั้งกำกับดูแลให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตลอดจนกำหนดกรอบและนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยมีการรายงานผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศให้คณะกรรมการบริษัททราบเป็นระยะ หรือเมื่อมีปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศที่สำคัญ หรือที่อาจส่งผลกระทบในวงกว้าง หรือส่งผลกระทบต่อชื่อเสียง หรือต่อการดำเนินงานและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทเกิดขึ้น
2) ประเมินความเพียงพอของกลยุทธ์การบริหารความเสี่ยงรวมถึงประสิทธิภาพในการบริหารความเสี่ยงของบริษัท
3) ติดตามสถานะความเสี่ยง รวมถึงความคืบหน้าในการบริหารความเสี่ยงและ ให้ข้อเสนอแนะในสิ่งที่ต้องดำเนินการปรับปรุงแก้ไข เพื่อให้สอดคล้องกับกรอบการบริหารความเสี่ยงและนโยบายการบริหารความเสี่ยงและกลยุทธ์ที่กำหนดตามความเหมาะสมและรายงานให้คณะกรรมการบริษัททราบอย่างน้อยไตรมาสละ 1 ครั้ง
4) กำกับดูแลกิจกรรมโดยรวมของบริษัทที่เกี่ยวข้องกับความเสี่ยง
5) ทำให้มั่นใจว่าบริษัทดำเนินกิจการภายใต้นโยบายการบริหารความเสี่ยง
6) จัดเตรียมแผนบรรเทาความเสี่ยงเพื่อรับมือกับความเสี่ยงกรณีฉุกเฉิน

2.4 **กรรมการผู้จัดการ** มีหน้าที่รับผิดชอบ ดังนี้

1) ปฏิบัติตามกฎหมายว่าด้วยประกันวินาศภัย และกฎหมายอื่นที่เกี่ยวข้อง
2) ปฏิบัติหน้าที่ด้วยความรับผิดชอบ ซื่อสัตย์สุจริต และระมัดระวัง คำนึงถึงผลประโยชน์ของบริษัท และผู้เอาประกันภัยเป็นสำคัญ ต้องไม่ใช้ตำแหน่งหน้าที่แสวงหาผลประโยชน์ส่วนตนหรือกระทำการที่ก่อให้เกิดความเสียหายต่อบริษัท รวมทั้งปฏิบัติตามวัตถุประสงค์ ข้อบังคับของบริษัท มติคณะกรรมการ ตลอดจนมติที่ประชุมผู้ถือหุ้น
3) ให้ข้อเสนอแนะที่เป็นประโยชน์ในการประชุม ปฏิบัติหน้าที่ได้อย่างเต็มความสามารถ รวมถึงเข้าร่วมประชุมคณะกรรมการบริษัททุกครั้ง เว้นแต่มีเหตุจำเป็น
4) ตัดสินใจอย่างเป็นอิสระ สมเหตุสมผล อยู่บนพื้นฐานของการมีข้อมูลที่เพียงพอ สำหรับการตัดสินใจ ทั้งนี้เพื่อไม่ให้เกิดปัญหาความขัดแย้งทางผลประโยชน์

2.5 **ผู้บริหาร** มีหน้าที่รับผิดชอบ ดังนี้

1) นำกลยุทธ์และนโยบายในการดำเนินธุรกิจที่คณะกรรมการบริษัทกำหนดไปปฏิบัติอย่างมีประสิทธิภาพ โดยคำนึงถึงการสร้างมูลค่าในระยะยาวและการดำเนินธุรกิจอย่างยั่งยืนของบริษัท
2) ส่งเสริม สนับสนุน และดำเนินการให้บริษัทมีการบริหารจัดการความเสี่ยงรวมทั้งการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์ มีระบบการควบคุมภายในอย่างมีประสิทธิภาพ มีการปฏิบัติตามกฎหมายที่เกี่ยวข้องได้อย่างถูกต้อง และมีการปฏิบัติต่อผู้เอาประกันภัยอย่างเป็นธรรม
3) มีการรายงานข้อมูลที่สำคัญเกี่ยวกับผลการดำเนินงานของบริษัท ระดับความเสี่ยงของบริษัท และผลการปฏิบัติงานของผู้บริหารต่อคณะกรรมการบริษัทอย่างถูกต้อง เพียงพอ และทันเวลา เพื่อให้คณะกรรมการบริษัทสามารถกำกับดูแลและติดตามผลการดำเนินงานได้อย่างมีประสิทธิภาพ
4) กำหนดโครงสร้างสายการบังคับบัญชาหรือสายการรายงานที่เหมาะสม รวมถึงการกำหนดหน้าที่ความรับผิดชอบของแต่ละหน่วยงานภายใต้สายการบังคับบัญชานั้นอย่างชัดเจน ให้เอื้อต่อการบริหารจัดการความเสี่ยง และการกำกับ ควบคุม ตรวจสอบ อย่างมีประสิทธิภาพ
5) ส่งเสริมให้บริษัทมีวัฒนธรรมการบริหารความเสี่ยง ดูแลและควบคุมความเสี่ยงของบริษัทให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ (risk appetite) ตามที่คณะกรรมการบริษัทกำหนด รวมทั้งสื่อสารให้พนักงานทุกคนในบริษัทเข้าใจและตระหนักถึงความสำคัญของนโยบายการบริหารความเสี่ยงของบริษัท
6) จัดให้มีการประเมินผลการปฏิบัติงานของผู้บริหารเป็นประจำทุกปีโดยเปรียบเทียบกับเป้าหมายที่คณะกรรมการบริษัทกำหนดไว้และรายงานผลการประเมินต่อคณะกรรมการบริษัท

2.6 **หน่วยงานบริหารความเสี่ยง** มีหน้าที่รับผิดชอบ ดังนี้

1) สนับสนุนการทำงานของคณะกรรมการบริษัท คณะกรรมการบริหารความเสี่ยง และผู้บริหาร ในประเด็นที่เกี่ยวข้องกับการบริหารความเสี่ยงของบริษัท รวมทั้งการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์
2) ระบุความเสี่ยงที่สำคัญที่บริษัทเผชิญอยู่ในปัจจุบัน และที่คาดว่าจะเกิดขึ้นในอนาคต
3) ประเมิน รวบรวม และติดตาม รวมถึงช่วยให้หน่วยงานภายในบริษัทสามารถระบุ ประเมินและบริหารความเสี่ยงของบริษัทให้อยู่ในระดับความเสี่ยงที่ยอมรับได้

4) สร้างแนวทางการประเมิน ลักษณะความเสี่ยงของบริษัท ที่เป็นการคาดการไปข้างหน้าโดยการประเมินสภาพแวดล้อม ความเสี่ยง ทั้งภายในและภายนอกอย่างต่อเนื่อง เพื่อระบุ และประเมินความเสี่ยงที่มีโอกาสจะเกิดขึ้นได้ทันท่วงที

5) พิจารณาความเสี่ยงที่เกิดจากนโยบายการจ่ายค่าตอบแทน ที่อนุมัติจากคณะกรรมบริษัท โดยครอบคลุมถึงกรรมการ ผู้บริหาร บุคคลากรหลักในหน่วยงานบริหารความเสี่ยง การดูแลการปฏิบัติตามกฎหมาย (compliance) งานด้านคณิตศาสตร์ประกันภัย (actuarial) งานด้านการตรวจสอบภายใน (internal audit) และพนักงานในหน่วยงานที่ก่อให้เกิดความเสี่ยงทีสำคัญ (major risk-taking staff)

6) จัดทำการวิเคราะห์สถานการณ์และการทดสอบภาวะวิกฤตภายใต้กรอบการบริหารความเสี่ยงและนโยบายการบริหารความเสี่ยง

7) จัดทำรายงานสถานะความเสี่ยงที่ระบุถึงความเสี่ยงที่บริษัทเผชิญ และรายงานการปฏิบัติตามมาตรการบริหารความเสี่ยงเป็นลายลักษณ์อักษร และนำเสนอต่อคณะกรรมการบริษัท และผู้บริหาร รวมถึงหน่วยงานอื่นที่เกี่ยวกับการควบคุมการดำเนินงานของบริษัท

8) จัดทำเอกสารและรายงานการเปลี่ยนแปลงสำคัญที่ส่งผลกระทบต่อกรอบการบริหารความเสี่ยงและนโยบายการบริหารความเสี่ยงต่อคณะกรรมการบริหารความเสี่ยงเพื่อให้มั่นใจว่ามีการนำไปใช้จริง และมีการปรับปรุงอยู่เสมอ

9) จัดทำรายงานการบริหารความเสี่ยงแบบองค์รวมและการประเมินความเสี่ยงและความมั่นคงทางการเงินของบริษัท

10) ดำเนินการอื่นใดเพื่อให้บริษัทสามารถดำรงภาพรวมของลักษณะความเสี่ยงที่ยอมรับได้ ทั้งระดับบริษัทและระดับกลุ่มธุรกิจ

11) ประเมินตนเองในเรื่องของคุณภาพการทำงานและติดตามการปรับปรุงใดๆ ที่จำเป็นเพื่อเพิ่มประสิทธิภาพของหน่วยงานบริหารความเสี่ยง

3. ขอบเขตการบริหารความเสี่ยง

บริษัทฯ ได้มีการกำหนดขอบเขตการบริหารความเสี่ยงให้สอดคล้องกับกรอบการบริหารความเสี่ยงและนโยบายการบริหารความเสี่ยงของบริษัทฯ และครอบคลุมประเภทความเสี่ยงที่อาจส่งผลกระทบต่อรายได้ เงินกองทุน ชื่อเสียง หรือการดำรงอยู่ของบริษัทฯ ดังนี้

(1) **ความเสี่ยงด้านกลยุทธ์** (strategic risk) หมายความรวมถึง ความเสี่ยงที่เกิดจากการกำหนดนโยบายแผนกลยุทธ์ แผนการดำเนินงาน และการนำไปปฏิบัติอย่างไม่เหมาะสม หรือไม่สอดคล้องกับปัจจัยภายในและสภาพแวดล้อมภายนอกซึ่งรวมถึงการเปลี่ยนแปลงทางสังคม เทคโนโลยี และความคาดหวังของสาธารณชน

(2) **ความเสี่ยงด้านประกันภัย** (insurance risk) หมายความรวมถึง ความเสี่ยงที่เกิดจากความผันผวนของความถี่ ความรุนแรง และเวลาที่เกิดความเสียหายที่เบี่ยงเบนจากสมมติฐานที่ใช้ในการกำหนดเบี้ยประกันภัย การคำนวณสำรองประกันภัย และการพิจารณารับประกันภัย

(3) **ความเสี่ยงด้านตลาด** (market risk) หมายความรวมถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของอัตราดอกเบี้ย อัตราแลกเปลี่ยนเงินตราต่างประเทศ ราคาของสินทรัพย์ที่ลงทุนราคาตราสารในตลาดเงินตลาดทุนและราคาสินค้าโภคภัณฑ์

(4) **ความเสี่ยงด้านเครดิต** (credit risk) หมายความรวมถึง ความเสี่ยงที่เกิดจากคู่สัญญาไม่สามารถปฏิบัติตามภาระที่ได้ตกลงไว้กับบริษัท รวมถึงโอกาสที่คู่สัญญาจะถูกปรับลดอันดับความเสี่ยงด้านเครดิต

(5) **ความเสี่ยงด้านสภาพคล่อง** (liquidity risk) หมายความรวมถึง ความเสี่ยงที่เกิดจากการที่บริษัทไม่สามารถชำระหนี้สินและภาระผูกพันเมื่อถึงกำหนด เนื่องจากไม่สามารถเปลี่ยนสินทรัพย์เป็นเงินสดได้ หรือไม่สามารถจัดหาเงินทุนได้เพียงพอ หรือสามารถจัดหาเงินมาชำระได้แต่ด้วยต้นทุนที่สูงเกินกว่าที่จะยอมรับได้

(6) **ความเสี่ยงด้านปฏิบัติการ** (operational risk) หมายความรวมถึง ความเสี่ยงที่จะเกิดความเสียหายอันเนื่องมาจากการขาดการกำกับดูแลกิจการที่ดี ขาดธรรมาภิบาลในองค์กร หรือขาดการควบคุมที่ดีที่เกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน บุคลากร ระบบงาน ระบบเทคโนโลยีสารสนเทศ ความปลอดภัยของข้อมูล หรือเหตุการณ์ภายนอก

(7) **ความเสี่ยงด้านชื่อเสียง** (reputation risk) หมายความรวมถึง ความเสี่ยงที่เกิดจากความเสียหายต่อบริษัทอันเนื่องมาจากการเสื่อมเสียชื่อเสียงเนื่องจากลูกค้า คู่ค้า ผู้ถือหุ้น และ/หรือหน่วยงานกำกับดูแล ที่มีมุมมองภาพลักษณ์ต่อบริษัทในแง่ลบ

(8) **ความเสี่ยงด้านเทคโนโลยีสารสนเทศ** (information technology risk) หมายความรวมถึง ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินธุรกิจ ซึ่งจะมีผลกระทบต่อระบบหรือการปฏิบัติงานของบริษัท รวมถึงความเสี่ยงเกิดจากภัยคุกคามทางไซเบอร์ (cyber threat)

(9) **ความเสี่ยงด้านมหันตภัย** (catastrophe risk) หมายความรวมถึง ความเสี่ยงที่เหตุการณ์หนึ่ง หรือเหตุการณ์ต่อเนื่องที่มีขนาดใหญ่ซึ่งก่อให้เกิดการจ่ายค่าสินไหมทดแทนจริงเบี่ยงเบนไปจากค่าสินไหมทดแทนที่ได้มีการคาดการณ์ไว้อย่างมาก

(10) **ความเสี่ยงภายในกลุ่มธุรกิจ** (group risk) หมายความรวมถึง ความเสี่ยงที่บริษัทอาจได้รับผลกระทบเชิงลบจากเหตุการณ์ (ทั้งที่เป็นทางการเงินและที่มิใช่ทางการเงิน) จากธุรกิจในกลุ่มเดียวกัน นอกจากนี้ยังรวมถึงความเสี่ยงที่เกิดจากความมั่นคงทางการเงินของกลุ่มธุรกิจทั้งหมดหรือบริษัทภายในกลุ่มธุรกิจซึ่งได้รับผลกระทบจากเหตุการณ์ของธุรกิจใดธุรกิจหนึ่ง ซึ่งเป็นทั้งเหตุการณ์ที่เกิดขึ้นภายในกลุ่มธุรกิจเองหรือ เหตุการณ์ภายนอกที่กระทบต่อกลุ่มธุรกิจ

(11) **ความเสี่ยงที่เกิดขึ้นใหม่** (emerging risk) หมายความรวมถึง ความเสี่ยงที่อาจเกิดใหม่เป็นความสูญเสียที่อาจไม่เคยปรากฏขึ้นหรือไม่เคยมีประสบการณ์มาก่อน และเป็นความเสี่ยงที่ยากต่อการประมาณการทั้งในเชิงโอกาสการเกิดและความรุนแรงในการเกิด เนื่องจากความไม่แน่นอนและการเปลี่ยนแปลงของปัจจัยแวดล้อม อาทิ การเมือง กฎหมาย สังคม เทคโนโลยี สภาพแวดล้อมทางกายภาพ รวมถึงการเปลี่ยนแปลงทางธรรมชาติ

4. กระบวนการบริหารความเสี่ยง

บริษัทฯ ได้จัดให้มีกระบวนการบริหารความเสี่ยง เพื่อให้ขั้นตอนและวิธีการในการบริหารความเสี่ยงเป็นไปอย่างมีระบบและดำเนินไปในทิศทางเดียวกันทั่วทั้งองค์กร มีการระบุเหตุการณ์ความเสี่ยง แหล่งที่มาของความเสี่ยงที่ส่งผลกระทบต่อบริษัทฯ ทั้งในทางการเงินและที่มิใช่ทางการเงิน และได้จัดทำเป็นทะเบียนความเสี่ยง ได้คำนึงถึงทิศทางการขยายงานและแผนรองรับการขยายงานตามที่ระบุไว้ในแผนธุรกิจ อีกทั้งยังได้ทบทวนเหตุการณ์ความเสี่ยงอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญของเหตุการณ์ความเสี่ยง

ทั้งนี้ กระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้เป็นไปตามนโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) และนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ที่บริษัทกำหนดขึ้นประกอบกัน

โดยขั้นตอนสำคัญของกระบวนการบริหารความเสี่ยงองค์กรประกอบด้วย 8 ขั้นตอน ดังนี้

4.1 สภาพแวดล้อมภายในองค์กร

สภาพแวดล้อมภายในองค์กร เป็นพื้นฐานที่สำคัญสำหรับกรอบการบริหารความเสี่ยง ซึ่งมีอิทธิพลต่อการกำหนดกลยุทธ์และเป้าหมายขององค์กร การกำหนดกิจกรรม การบ่งชี้ประเมิน และจัดการความเสี่ยง

สภาพแวดล้อมภายในองค์กร หมายถึง ปัจจัยต่างๆ เช่น จริยธรรม วิธีการทำงานของผู้บริหารและบุคลากร รูปแบบการจัดการของฝ่ายบริหารและวิธีการมอบหมายอำนาจหน้าที่และความรับผิดชอบ ซึ่งผู้บริหารต้องมีการกำหนดร่วมกันกับพนักงานในองค์กร ส่งผลให้มีการสร้างจิตสำนึก การตระหนักและรับรู้เรื่องความเสี่ยง และการควบคุมแก่พนักงานทุกคน

4.2 การกำหนดวัตถุประสงค์

บริษัทฯ ได้กำหนดให้มีกรอบการบริหารความเสี่ยง เพื่อให้หน่วยงานสามารถนำไปใช้ในการปฏิบัติงานได้อย่างมีประสิทธิผล และก่อให้เกิดความมั่นใจอย่างสมเหตุสมผลว่าผลสำเร็จของงานจะสามารถบรรลุวัตถุประสงค์ของบริษัทฯ และสามารถลดมูลเหตุของโอกาสที่จะเกิดความเสียหายในอนาคตให้อยู่ในระดับความเสี่ยงที่ยอมรับได้

อีกทั้ง ยังได้กำหนดวัตถุประสงค์ทางธุรกิจที่ชัดเจน เพื่อให้มั่นใจว่าวัตถุประสงค์ที่กำหนดนั้นมีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่ยอมรับได้โดยการบริหารจัดการให้อยู่ในกรอบของ Risk Appetite และ Risk Tolerance

4.3 การระบุความเสี่ยง

ในกระบวนการระบุความเสี่ยง บริษัทฯ ได้พิจารณาปัจจัยความเสี่ยงทุกด้านที่อาจเกิดขึ้น เช่น ความเสี่ยงด้านกลยุทธ์ การเงิน บุคลากร การปฏิบัติงาน กฎหมาย ภาษีอากร ระบบงาน สิ่งแวดล้อม ความสัมพันธ์ระหว่างเหตุการณ์ที่อาจเกิดขึ้น แหล่งความเสี่ยงทั้งจากสภาพแวดล้อมภายในและภายนอก

สภาพแวดล้อมภายนอกองค์กร เป็นองค์ประกอบต่างๆ ที่อยู่ภายนอกองค์กร ซึ่งมีอิทธิพลต่อวัตถุประสงค์/เป้าหมายขององค์กร เช่น

- วัฒนธรรม การเมือง กฎหมาย ข้อบังคับ การเงิน เทคโนโลยี เศรษฐกิจ สภาพแวดล้อมในการแข่งขันการแข่งขันทั้งภายในประเทศและต่างประเทศ
- ตัวขับเคลื่อนหลักและแนวโน้มที่ส่งผลกระทบต่อวัตถุประสงค์ขององค์กร
- การยอมรับและคุณค่าของผู้มีส่วนได้เสียภายนอกองค์กร

สภาพแวดล้อมภายในองค์กร เป็นสิ่งต่างๆ ที่อยู่ภายในองค์กรและมีอิทธิพลต่อเป้าหมายขององค์กร เช่น

- ขีดความสามารถขององค์กร ในแง่ของทรัพยากรและความรู้ เช่น เงินทุน เวลา บุคลากร กระบวนการ ระบบ และเทคโนโลยี
- ระบบสารสนเทศ การ Flow ของข้อมูล และกระบวนการตัดสินใจทั้งที่เป็นทางการและไม่เป็นทางการ
- ผู้มีส่วนได้เสียภายในองค์กร
- นโยบาย วัตถุประสงค์และกลยุทธ์องค์กร
- การรับรู้ คุณค่าและวัฒนธรรมองค์กร
- โครงสร้าง เช่น ระบบการจัดการ บทบาทหน้าที่และความรับผิดชอบ

การระบุความเสี่ยงอาจดำเนินการโดยการเรียกประชุม หรือสัมภาษณ์ผู้บริหารระดับสูงหรือฝ่ายจัดการที่รับผิดชอบในแผนงานหรือการดำเนินการนั้น และรวบรวมประเด็นความเสี่ยงสำคัญที่ได้รับความสนใจหรือเป็นประเด็นที่กังวล เพื่อนำมาจัดทำภาพรวมความเสี่ยงขององค์กร ซึ่งที่ผ่านมา บริษัทฯ จะมีการระบุความเสี่ยงด้วยวิธีการจาก การสัมภาษณ์ (Interviews) การ

จัดประชุมเชิงปฏิบัติการ (Facilitated Workshops) การระดมสมอง (Brainstorming) และการใช้ Check Lists หรือการประเมินการควบคุมภายในด้วยตนเอง (Control Self-Assessment – CSA)

4.4 การประเมินความเสี่ยง

สำหรับการประเมินความเสี่ยงเป็นขั้นตอนที่จะต้องดำเนินการต่อจากการระบุความเสี่ยง โดยการประเมินความเสี่ยงประกอบด้วย 2 กระบวนการหลัก ได้แก่

1. **การวิเคราะห์ความเสี่ยง** จะพิจารณาสาเหตุและแหล่งที่มาของความเสี่ยง ผลกระทบที่ตามมาทั้งในทางบวกและทางลบ รวมทั้งโอกาสที่อาจเกิดขึ้นของผลกระทบที่อาจตามมา โดยจะต้องมีการระบุถึงปัจจัยที่มีผลต่อผลกระทบและโอกาสที่จะเกิดขึ้น ทั้งนี้เหตุการณ์หรือสถานการณ์หนึ่งๆ อาจจะเกิดผลที่ตามมาและกระทบต่อวัตถุประสงค์/เป้าหมายหลายด้าน นอกจากนั้นในการวิเคราะห์ควรพิจารณาถึงมาตรการจัดการความเสี่ยงที่ดำเนินการอยู่ ณ ปัจจุบัน รวมถึงประสิทธิผลของมาตรการดังกล่าวด้วย

2. **การประเมินระดับความเสี่ยง** จะเปรียบเทียบระหว่างระดับของความเสี่ยงที่ได้จากการวิเคราะห์ความเสี่ยงเทียบกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ในกรณีที่ระดับของความเสี่ยงไม่อยู่ในระดับที่ยอมรับได้ของเกณฑ์การยอมรับความเสี่ยง ความเสี่ยงดังกล่าวจะได้รับการบริหารจัดการทันที ซึ่งหลักการประเมินความเสี่ยง จะพิจารณาจาก 2 มิติ ได้แก่

   (1) **โอกาสที่จะเกิดความเสี่ยง** (Likelihood) หมายถึง ความเป็นไปได้ที่ความเสี่ยงหรือเหตุการณ์นั้นจะเกิดขึ้น ซึ่งในการพิจารณาระดับของโอกาสที่จะเกิดขึ้น มักจะใช้ข้อมูลที่ผ่านมา อย่างไรก็ตามในกรณีที่เป็นเหตุการณ์ที่ไม่เคยมีมาก่อน อาจจะใช้ข้อมูลของเหตุการณ์ในลักษณะเดียวกันที่ได้เคยเกิดขึ้นในหน่วยงานอื่น ข้อมูลที่ได้จากการค้นคว้า หรือประสบการณ์ของผู้ประเมิน ในการประเมินโอกาสที่จะเกิดความเสี่ยง

(2) **ผลกระทบที่เกิดขึ้น** (Impact) หมายถึง ผลกระทบหรือความเสียหายจากความเสี่ยงที่จะเกิดขึ้น ซึ่งอาจเป็นมูลค่าความเสียหาย ความมีนัยสำคัญต่อเป้าหมายของบริษัท ทั้งในแง่ที่สามารถวัดออกมาเป็นมูลค่า (ทางการเงิน) และมีผลกระทบต่อภาพลักษณ์และชื่อเสียงองค์กร

การวัดระดับโอกาสและผลกระทบ บริษัทฯ เลือกใช้เทคนิคการวิเคราะห์แบบต่างๆ ประกอบกันตามความเหมาะสมของแต่ละความเสี่ยง ได้แก่ การวิเคราะห์เชิงคุณภาพ การวิเคราะห์กึ่งคุณภาพกึ่งปริมาณ และการวิเคราะห์เชิงปริมาณ (เป็นการใช้ตัววัดที่เป็นตัวเลข เช่น จำนวนเงินที่สูญเสีย จำนวนข้อร้องเรียน ร้อยละความล่าช้าเทียบกับแผนงาน เป็นต้น) โดยมีการวิเคราะห์เชิงปริมาณและอาศัยการเก็บรวบรวมสถิติและข้อมูลที่เกี่ยวข้อง รวมถึงการใช้แบบจำลองหรือวิธีการทางคณิตศาสตร์ช่วยในการกำหนดค่าตัวเลข โดยมีการกำหนดตัวชี้วัดความเสี่ยง (Key Risk Indicator : KRI) ซึ่งเป็นการระบุว่าความเสี่ยงนั้นมีตัวชี้วัดอะไรบ้าง

บริษัทฯ ได้กำหนดหลักเกณฑ์การประเมินระดับโอกาสและผลกระทบไว้ 5 ระดับ ซึ่งในการประเมินความเสี่ยงนั้นๆ คณะกรรมการบริหารความเสี่ยง จะเป็นผู้พิจารณากำหนดเกณฑ์ประเมินระดับโอกาสและผลกระทบสำหรับความเสี่ยงนั้น ๆ โดยเฉพาะต่อไป

3. **ระดับความเสี่ยง** คือ ตัวชี้วัดที่ใช้ในการกำหนดความสำคัญของความเสี่ยง โดยค่าระดับความเสี่ยงได้จาก การนำโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงมาพิจารณาร่วมกัน ดังนี้

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

ระดับความเสี่ยงที่ได้จากการคำนวณตามสูตรข้างต้น หากมีค่าต่ำ หมายถึงความเสี่ยงอยู่ในระดับต่ำ และหากมีค่าสูงขึ้น ความเสี่ยงจะมีระดับสูงขึ้น โดยความหมายของแต่ละระดับความเสี่ยงแสดงดังตารางดังนี้

ระดับความเสี่ยง	คำอธิบาย	
1 - 3		ต่ำ
4 - 8		ปานกลาง
9 - 16		สูง
มากกว่า 16		สูงมาก

โอกาสที่จะเกิดความเสี่ยง	ความรุนแรงของผลกระทบจากความเสี่ยง				
	1 = น้อยมาก	2 = น้อย	3 = ปานกลาง	4 = สูง	5 = สูงมาก
5 = เกือบแน่นอน	5	10	15	20	25
4 = น่าจะเกิดขึ้น	4	8	12	16	20
3 = เป็นไปได้	3	6	9	12	15
2 = ไม่น่าจะเกิด	2	4	6	8	10
1 = เกิดขึ้นยาก	1	2	3	4	5

โซนสีเขียว
ระดับต่ำ
(Low = L)

โอกาส:ผลกระทบ
1 = 1:1
2 = 1:2
2 = 2:1
3 = 1:3
3 = 3:1

โซนสีเหลือง
ระดับปานกลาง
(Medium = M)

โอกาส:ผลกระทบ
4 = 1:4
4 = 2:2
4 = 4:1
5 = 1:5
5 = 5:1
6 = 2:3
6 = 3:2
8 = 2:4
8 = 4:2

โซนสีส้ม
ระดับสูง
(High = H)

โอกาส:ผลกระทบ
9 = 3:3
10 = 2:5
10 = 5:2
12 = 3:4
12 = 4:3
15 = 3:5
15 = 5:3
16 = 4:4

โซนสีแดง
ระดับสูงมาก
(Extreme = E)

โอกาส:ผลกระทบ
20 = 4:5
20 = 5:4
25 = 5:5

หลังจากได้รับผลการประเมินแล้ว หน่วยงานบริหารความเสี่ยง/ฝ่ายจัดการจะดำเนินการ ดังนี้

- วิเคราะห์และสรุปผลการประเมิน โดยใช้ Risk Map ข้างต้น และจัดลำดับความสำคัญของประเด็นความเสี่ยง

- นำเสนอผลการประเมินต่อที่กรรมการผู้จัดการ เพื่อดำเนินการคัดเลือกความเสี่ยงที่สำคัญที่ต้องจัดการดูแล รวมถึงการกำหนดฝ่ายจัดการที่รับผิดชอบ(Risk Champion) เพื่อดำเนินการจัดหามาตรการจัดการความเสี่ยงเพิ่มเติมจากที่มีอยู่ ณ ปัจจุบัน
- นำเสนอประเด็นความเสี่ยงและมาตรการต่างๆ ที่กำหนดให้ต้องจัดการดูแล ต่อคณะกรรมการบริหารความเสี่ยง เพื่อทราบ

การกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้ (Risk Appetite)

บริษัทฯ ได้มีการกำหนดระดับความเสี่ยงที่ยอมรับได้เพื่อให้บรรลุวัตถุประสงค์หรือเป้าหมายของบริษัทฯ ซึ่งกำหนดทั้งในเชิงปริมาณและ/หรือเชิงคุณภาพ ทั้ง 2 ด้าน โดยกำหนดให้ระดับความเสี่ยงที่ยอมรับได้อยู่ในระดับน้อยมาก – ปานกลาง (ระดับคะแนน 1-8) และไม่ทำให้อัตราส่วนความเพียงพอของเงินกองทุน (CAR) ของบริษัทต่ำกว่า 180%

4.5 การตอบสนองความเสี่ยง

การกำหนดแผนจัดการความเสี่ยงจะมีการนำเสนอแผนจัดการความเสี่ยงที่จะดำเนินการต่อที่ประชุมคณะกรรมการบริษัทเพื่อพิจารณา และขออนุมัติการจัดการกับความเสี่ยงนั้นจากคณะกรรมการบริษัท โดยในการคัดเลือกแนวทางในการจัดการความเสี่ยงที่เหมาะสมที่สุดจะคำนึงถึงความเสี่ยงที่ยอมรับได้ (Risk Appetite) กับต้นทุนที่เกิดขึ้นเปรียบเทียบกับประโยชน์ที่จะได้รับ รวมถึงข้อกฎหมายและข้อกำหนดอื่นๆ ที่เกี่ยวข้อง

ระดับความเสี่ยงที่ยอมรับได้ คือ ระดับความเสี่ยงที่บริษัทฯ ยอมรับได้ โดยยังคงให้องค์กรสามารถดำเนินธุรกิจและบรรลุเป้าหมายหรือวัตถุประสงค์ที่วางไว้

ทั้งนี้ในการตัดสินใจเลือกแนวทางในการจัดการความเสี่ยง บริษัทฯ ได้คำนึงถึงความเสี่ยงที่อาจเกิดขึ้นหากไม่มีการจัดการความเสี่ยง หรือความเสี่ยงที่ส่งผลกระทบในทางลบอย่างมีนัยสำคัญ แต่โอกาสที่จะเกิดขึ้นน้อยมาก ซึ่งแนวทางในการจัดการความเสี่ยงก็จะพิจารณาดำเนินการเป็นกรณีๆ ไป หรือดำเนินการไปพร้อมกับความเสี่ยงอื่นๆ

<u>แนวทางในการจัดการความเสี่ยง</u>

- การหลีกเลี่ยง (Avoid) เป็นการดำเนินการเพื่อหลีกเลี่ยงเหตุการณ์ที่ก่อให้เกิดความเสี่ยง มักใช้ในกรณีที่ความเสี่ยงมีความรุนแรงสูง ไม่สามารถหาวิธีลด/จัดการให้อยู่ในระดับที่ยอมรับได้

- การร่วมจัดการ (Share) เป็นการร่วมหรือถ่ายโอนความเสี่ยงทั้งหมดหรือบางส่วนไปยังบุคคล/หน่วยงานภายนอกองค์กร ให้ช่วยแบกรับภาระความเสี่ยงแทน เช่น การทำประกันภัยต่อ

- การลด (Reduce) เป็นการจัดหามาตรการจัดการ เพื่อลดโอกาสการเกิดเหตุการณ์ความเสี่ยง หรือลดผลกระทบที่อาจเกิดขึ้น ให้อยู่ในระดับที่ยอมรับได้ เช่น การเตรียมแผนฉุกเฉิน (Contingency Plan)

- การยอมรับ (Accept) ในกรณีที่ความเสี่ยงที่เหลือในปัจจุบันอยู่ในระดับที่ยอมรับได้ และไม่ต้องดำเนินการใดๆ เพื่อลดโอกาสหรือผลกระทบที่อาจเกิดขึ้นอีก มักใช้กับความเสี่ยงที่ต้นทุนของมาตรการจัดการสูงไม่คุ้มกับประโยชน์ที่ได้รับ

4.6 กิจกรรมการควบคุม

กิจกรรมการควบคุม คือ กระบวนการปฏิบัติงาน เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยงให้อยู่ในระดับที่สามารถยอมรับได้ เพื่อป้องกันไม่ให้เกิดผลกระทบต่อเป้าหมายขององค์กร ซึ่งอาจแบ่งได้เป็น 4 ประเภท คือ

1. การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก
2. การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมเพื่อให้ค้นพบข้อผิดพลาดที่ได้เกิดขึ้นแล้ว
3. การควบคุมโดยการชี้แนะ (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้น ให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ
4. การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้น เพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้น และป้องกันไม่ให้เกิดซ้ำอีกในอนาคต

ทั้งนี้ ในการดำเนินกิจกรรมการควบคุมควรต้องคำนึงถึงความคุ้มค่าในด้านค่าใช้จ่ายและต้นทุน กับ

ผลประโยชน์ที่คาดว่าจะได้รับด้วย โดยกิจกรรมการควบคุมควรมีองค์ประกอบดังนี้

- วิธีการดำเนินงาน (ขั้นตอน, กระบวนการ)

- การกำหนดบุคลากรภายในองค์กรเพื่อรับผิดชอบการควบคุมนั้น ซึ่งควรมีความรับผิดชอบดังนี้

(1) พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

(2) พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยง

- กำหนดระยะเวลาแล้วเสร็จของงาน

4.7 ข้อมูลและการติดต่อสื่อสาร

สารสนเทศเป็นสิ่งจำเป็นสำหรับบริษัทฯ ในการบ่งชี้ ประเมิน และจัดการความเสี่ยง ข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กรทั้งจากแหล่งข้อมูลภายในและภายนอกองค์กรควรได้รับการบันทึกและสื่อสารไปยังบุคลากรในองค์กรอย่างเหมาะสมทั้งในด้านรูปแบบและเวลา เพื่อให้สามารถปฏิบัติงานตามหน้าที่และความรับผิดชอบได้รวมถึงเป็นการรายงานการบริหารจัดการความเสี่ยง เพื่อให้ทุกคนได้รับทราบถึงความเสี่ยงที่เกิดขึ้น และผลของการบริหารจัดการความเสี่ยงเหล่านั้น

การสื่อสารที่มีประสิทธิภาพยังคลอบคลุมถึงการสื่อสารจากระดับบนลงล่าง ระดับล่างไปสู่บน และการสื่อสารระหว่างหน่วยงาน

การบริหารความเสี่ยงควรใช้ทั้งข้อมูลในอดีตและปัจจุบัน โดยข้อมูลในอดีตจะแสดงแนวโน้มของเหตุการณ์และช่วยคาดการณ์การปฏิบัติงานในอนาคต ส่วนข้อมูลปัจจุบันมีประโยชน์ต่อผู้บริหารในการพิจารณาความเสี่ยงที่เกิดขึ้นในกระบวนการ สายงาน หรือหน่วยงานซึ่งช่วยให้สามารถปรับเปลี่ยนกิจกรรมการควบคุมตามความจำเป็น เพื่อให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้

4.8 การติดตามประเมินผลและการรายงาน

กระบวนการบริหารความเสี่ยงที่ดำเนินการภายในบริษัทฯ มีความจำเป็นต้องได้รับการสื่อสารถึงการประเมินความเสี่ยงและการควบคุม ความคืบหน้าในการบริหารความเสี่ยง การดูแลติดตามแนวโน้มของความเสี่ยงหลัก รวมถึงการเกิดเหตุการณ์ผิดปกติอย่างต่อเนื่อง เพื่อให้มั่นใจว่า

- เจ้าของความเสี่ยง (Risk Owner) มีการติดตาม ประเมินสถานการณ์ วิเคราะห์ และบริหารความเสี่ยงที่อยู่ภายใต้ความรับผิดชอบของตนอย่างสม่ำเสมอ และเหมาะสม

- ความเสี่ยงที่มีผลกระทบสำคัญต่อการบรรลุวัตถุประสงค์ขององค์กร ได้รับการรายงานถึงความคืบหน้าในการบริหารความเสี่ยง และแนวโน้มของความเสี่ยงต่อผู้บริหารที่รับผิดชอบและคณะกรรมการบริหารความเสี่ยง
- ระบบการควบคุมภายในที่วางไว้มีความเพียงพอ เหมาะสม มีประสิทธิผล และมีการนำมาปฏิบัติใช้จริงเพื่อป้องกันหรือลดความเสี่ยงที่อาจเกิดขึ้น รวมทั้งมีการปรับปรุงแก้ไขการควบคุมภายในอยู่เสมอเพื่อให้สอดคล้องกับสถานการณ์หรือความเสี่ยงที่เปลี่ยนไป

ทั้งนี้ บริษัทฯ ได้กำหนดวิธีการที่เหมาะสมในการติดตามการบริหารความเสี่ยง โดยให้มีการรายงานและการสอบทานตามกระบวนการบริหารความเสี่ยงอย่างสม่ำเสมอ โดยกระบวนการบริหารความเสี่ยง ภายใต้กรอบและนโยบายบริหารความเสี่ยงที่บริษัทฯ กำหนด เป็นไปตามแนวทาง 3 Lines of Defense Model โดยได้แบ่งหน้าที่ความรับผิดชอบในการบริหารความเสี่ยงเป็น 3 ส่วน ดังนี้

1) **ปราการด่านที่** 1 (1st Line of Defense) : **การบริหารความเสี่ยงในการปฏิบัติงาน**

พนักงานทุกฝ่ายงาน มีหน้าที่ในการบริหารความเสี่ยงในการปฏิบัติงานของฝ่ายงานที่ตนเองมีส่วนเกี่ยวข้อง ผ่านกิจกรรมควบคุมการปฏิบัติงานต่างๆ ซึ่งควบคุม ติดตาม และรายงานผ่านผู้บริหาร เพื่อเสนอต่อคณะกรรมการบริษัท

2) **ปราการด่านที่** 2 (2nd Line of Defense) : **การกำกับดูแลการบริหารความเสี่ยง**

หน่วยงานบริหารความเสี่ยง ซึ่งหมายรวมถึงคณะกรรมการบริหารความเสี่ยง หน่วยงานคณิตศาสตร์ประกันภัย และหน่วยงาน Compliance มีหน้าที่ในการติดตามความเพียงพอหรือความเหมาะสมถึงแนวทางการบริหารความเสี่ยงในการปฏิบัติงานจากฝ่ายงาน รวมทั้งมีหน้าที่ติดตามรวบรวมข้อมูลที่เกี่ยวข้องกับการบริหารความเสี่ยงของฝ่ายงาน รายงานผ่านสายงานกำกับของตนเอง

3) **ปราการด่านที่** 3 (3rd Line of Defense) : **การสร้างความเชื่อมั่นในการบริหารความเสี่ยง**

ฝ่ายตรวจสอบภายใน รวมถึงผู้ตรวจสอบภายนอก มีหน้าที่ในการตรวจสอบกระบวนการบริหารความเสี่ยง รวมถึงการปฏิบัติตามกระบวนการบริหารความเสี่ยงทั้งในส่วนของหน่วยงานบริหารความเสี่ยง และฝ่ายงานต่างๆ และรายงานต่อคณะกรรมการตรวจสอบ และคณะกรรมการบริษัทฯ เพื่อเป็นการสร้างความเชื่อมั่นในการบริหารความเสี่ยงของบริษัทโดยรวม

นอกจากนี้ ในปัจจุบัน บริษัทฯ ได้มีการว่าจ้างหน่วยงานภายนอกเข้ามาทำหน้าที่ตรวจสอบภายในเพื่อติดตามและประเมินผลการบริหารความเสี่ยงของหน่วยงานภายในว่าเป็นไปตามกรอบการบริหารความเสี่ยง และนโยบายการบริหารความเสี่ยง และรายงานต่อคณะกรรมการตรวจสอบหรือคณะกรรมการบริษัท อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินผลการบริหารความเสี่ยงของบริษัทฯ และให้ข้อเสนอแนะแก่ฝ่ายบริหารเพื่อกำกับดูแลการปฏิบัติงานให้เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล อีกทั้งได้จัดให้มีการทบทวนประสิทธิผลของกรอบการบริหารความเสี่ยงและนโยบายการบริหารความเสี่ยงอย่างน้อยปีละ 1 ครั้งหรือทุกครั้งที่เกิดเหตุการณ์สำคัญที่อาจส่งผลกระทบต่อความมั่นคงทางการเงินของบริษัทฯ อย่างมีนัยสำคัญ

5. ระบบสารสนเทศเพื่อรองรับการบริหารความเสี่ยง

บริษัทฯ จัดให้มีระบบสารสนเทศที่เป็นปัจจุบัน เชื่อถือได้ รวดเร็ว และมีรูปแบบที่เหมาะสมและสอดคล้องกับขนาดลักษณะและความซับซ้อนของธุรกิจ โดยสามารถสนับสนุน ติดตามดูแล และควบคุมการบริหารความเสี่ยง รวมถึงการนำข้อมูลไปใช้ได้อย่างถูกต้องและมีประสิทธิภาพ อีกทั้ง ยังจัดให้มีระบบการจัดเก็บข้อมูลที่ปลอดภัย มีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลของบุคลากรเฉพาะที่เกี่ยวข้อง และจัดให้มีระบบสำรองข้อมูลรวมทั้งระบบการกู้คืนข้อมูลในกรณีที่เกิดเหตุฉุกเฉินขึ้น

6. วัฒนธรรมการบริหารความเสี่ยง

บริษัทฯ ได้ให้ความสำคัญกับการสร้างวัฒนธรรมการบริหารความเสี่ยงภายในองค์กร และดำเนินการเพื่อให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการทำงานของพนักงานทุกคน โดยได้ดำเนินการดังนี้

1) คณะกรรมการ และผู้บริหารของบริษัทฯ กำหนดทิศทาง นโยบาย และแนวปฏิบัติในการบริหารความเสี่ยง และสื่อสารวัตถุประสงค์และประโยชน์ที่จะได้รับจากการบริหารความเสี่ยงขององค์กรไปยังพนักงานทุกคนเพื่อให้เกิดความตระหนักและเห็นคุณค่าของการบริหารความเสี่ยง

2) จัดให้มีการฝึกอบรมพัฒนาบุคลากร ให้มีความรู้ ความเข้าใจ ความระมัดระวัง กรอบการบริหารความเสี่ยงและความรับผิดชอบของแต่ละบุคคลในการจัดการความเสี่ยง และสื่อสารข้อมูลเกี่ยวกับความเสี่ยง เพื่อให้ร่วมกันตระหนักถึงความเสี่ยงที่อาจจะเกิดขึ้นและมีผลกระทบต่อฝ่ายงาน องค์กร และผู้ที่เกี่ยวข้อง รวมทั้งยังได้ส่งเสริมให้มีการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานต่างๆ ภายในองค์กร

3) จัดให้มีการบูรณาการการบริหารความเสี่ยงเข้ากับการตัดสินใจทางธุรกิจ การกำกับดูแลกิจการ และควบคุมภายในของบริษัทฯ