นโยบายการบริหารความเสี่ยง

บริษัท โคแมนชี่ อินเตอร์เนชั่นแนล จำกัด (มหาชน)

นโยบายการบริหารความเสี่ยง

นโยบายการบริหารความเสี่ยงฉบับนี้ จัดทำขึ้นเพื่อ เป็นเครื่องมือในการสื่อสาร และสร้างความเข้าใจในกระบวนการบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management) แก่ผู้บริหาร พนักงาน และผู้เกี่ยวข้องของบริษัท โคแมนชี่ อินเตอร์เนชั่นแนล จำกัด (มหาชน) (“บริษัทฯ”) และบริษัทย่อย (“กลุ่มบริษัท”) เพื่อให้การดำเนินงานบริหารความเสี่ยงของบริษัทฯ เป็นไปตาม นโยบายที่คณะกรรมการบริษัทกำหนด โดยได้นำกระบวนการบริหารความเสี่ยงมาบูรณาการกับกระบวนการบริหาร จัดการภายในเพื่อขับเคลื่อนการบริหารความเสี่ยงให้เป็นส่วนหนึ่งของการบริหารงาน

บริษัทฯ ตระหนักถึงความสำคัญของการบริหารความเสี่ยงอย่างยั่งยืนซึ่งครอบคลุมความเสี่ยงหลัก ๆ ที่อาจมีผลต่อธุรกิจของบริษัท โดยหน้าที่และความรับผิดชอบของคณะกรรมการบริหารความเสี่ยง คือ วิเคราะห์และประเมินความเสี่ยงที่เกิดขึ้นหรือมีความเป็นไปได้ที่จะเกิดขึ้นอย่างต่อเนื่องในแต่ละปี และบริษัทฯ ได้นำกรอบแนวทางการปฏิบัติด้านการควบคุมภายในตามมาตรฐานสากลของ The Committee of Sponsoring Organizations of the Treadway Commission (COSO) มาประยุกต์ใช้ เพื่อให้องค์กรสามารถบรรลุเป้าหมายที่กำหนด พัฒนา และทบทวนนโยบายการบริหารความเสี่ยงเพื่อลดโอกาสหรือความเสียหายที่อาจเกิดจากความเสี่ยงที่จะส่งผลกระทบ โดยทำให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้

คำนิยาม

- ความเสี่ยง (Risks) หมายถึง โอกาส/เหตุการณ์ที่มีความไม่แน่นอน หรือสิ่งที่ทำให้แผนงานหรือการดำเนินการอยู่ ณ ปัจจุบันไม่บรรลุวัตถุประสงค์/เป้าหมายที่กำหนดไว้ โดยก่อให้เกิดผลกระทบหรือความเสียหายต่อองค์กร
- การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ปฏิบัติโดยคณะกรรมการผู้บริหารและบุคลากรทุกคนในองค์กร เพื่อช่วยในการกำหนดกลยุทธ์และดำเนินงาน โดยกระบวนการบริหารความเสี่ยงได้รับการออกแบบให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อองค์กร เพื่อให้องค์กรสามารถจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ทั้งนี้เพื่อให้ได้ความมั่นใจอย่างสมเหตุสมผล ในการบรรลุวัตถุประสงค์ที่องค์กรกำหนดไว้
- ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) หมายถึง ขนาด ปริมาณ หรือระดับของความเสี่ยงที่องค์กรสามารถยอมรับได้ อาจเป็นค่าเดียวหรือ เป็นช่วงขึ้นอยู่กับความเหมาะสมของแต่ละปัจจัย ระดับความเสี่ยงที่ยอมรับได้กำหนดขึ้นเพื่อให้ทุกหน่วยงานในบริษัทฯ ใช้เป็นกรอบในการดำเนินงานและการตัดสินใจหรือพิจารณาอนุมัติเรื่องต่าง ๆ ของบริษัทฯ เพื่อช่วยให้บรรลุเป้าหมายขององค์กร

วัตถุประสงค์ของการบริหารความเสี่ยง

1. เพื่อให้สามารถระบุความเสี่ยงหรือวิกฤตการณ์ที่ไม่คาดคิด และสามารถตอบสนองการลดความสูญเสียหรือ ความเสียหายต่อองค์กรได้อย่างเหมาะสมและทันการณ์ มีการกำหนดมาตรการและแนวทางบริหารจัดการความเสี่ยงที่เหลืออยู่ให้อยู่ในระดับที่ยอมรับได้ขององค์กร โดยพิจารณามาตรการที่จะลดโอกาสและ/หรือ ผลกระทบจากความเสี่ยงที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ เพื่อผลักดันให้สามารถบรรลุวัตถุประสงค์ที่ องค์กรกำหนดไว้
2. เพื่อให้คณะกรรมการบริหารความเสี่ยง คณะกรรมการตรวจสอบ คณะกรรมการบริษัทรับทราบและกำกับดูแล การบริหารความเสี่ยงที่สำคัญของบริษัท ได้อย่างมีประสิทธิภาพ มีการบริหารความเสี่ยงอย่างเป็นระบบโดยต่อเนื่อง
3. เพื่อให้มีการสื่อสารและสร้างความรู้ความเข้าใจในเรื่องการบริหารความเสี่ยง รวมทั้งมีความตระหนักถึงการ เป็นเจ้าของความเสี่ยง ตลอดจนมีการบริหารความเสี่ยงร่วมกันภายใต้งานที่รับผิดชอบ และพัฒนาการสร้างเป็นวัฒนธรรมขององค์กร

ขอบเขต

นโยบายฉบับนี้มีผลบังคับใช้กับคณะกรรมการบริหาร ผู้บริหาร ตลอดจนพนักงานในทุกระดับของบริษัทฯ โดยนโยบายฉบับนี้จัดทำขึ้นโดยคำนึงถึงความสอดคล้องกับแผนยุทธศาสตร์ แผนปฏิบัติงาน แผนงานโครงการ กฎหมายและกฎระเบียบต่าง ๆ ที่เกี่ยวข้องกับการดำเนินงานของบริษัทฯ บริษัทจึงกำหนดนโยบายการบริหารความเสี่ยง ดังต่อไปนี้

1. คณะกรรมการบริษัททำหน้าที่กำกับดูแลให้การบริหารความเสี่ยงเป็นไปตามนโยบายที่กำหนด มีการกลั่นกรองให้ข้อเสนอแนะ และติดตามการดำเนินการ เพื่อให้การบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิภาพ รวมถึงทบทวนและประเมินระบบจัดการบริหารความเสี่ยงอย่างสม่ำเสมอ
2. คณะกรรมการตรวจสอบทำหน้าที่สอบทานความเหมาะสม และประสิทธิภาพของการบริหารความเสี่ยง และกระบวนการจัดการความเสี่ยงของบริษัท เพื่อทำให้มั่นใจว่าการควบคุมภายใน และการบริหารความเสี่ยงที่จัดตั้งขึ้นนั้นมีประสิทธิภาพอย่างเพียงพอ และรายงานต่อคณะกรรมการบริษัทเกี่ยวกับผลการทบทวนความเสี่ยงดังกล่าว
3. คณะกรรมการบริหารมีหน้าที่กำหนดทิศทางในการบริหารจัดการและอนุมัติกลยุทธ์ ตลอดจนนโยบายขององค์กรที่เป็นส่วนสำคัญของบริษัทอย่างมีนัยสำคัญ และให้คำแนะนำเกี่ยวกับการจัดการความเสี่ยงในเรื่องที่เกี่ยวข้องกับนโยบาย การกำกับดูแล และแผนงานในการดำเนินธุรกิจของบริษัท
4. ประธานเจ้าหน้าที่บริหารมีหน้าที่ความรับผิดชอบในการดำเนินการตามนโยบายฉบับนี้ และกำกับดูแลให้มีการปฏิบัติตามอย่างต่อเนื่อง ผ่านคณะกรรมการบริหารความเสี่ยง และ/หรือ คณะทำงานบริหารความเสี่ยง ซึ่งประกอบด้วยผู้บริหารจากหน่วยงานหลักของบริษัท
5. บริษัทกำหนดให้มีการบริหารความเสี่ยงขององค์กรเป็นไปตามมาตรฐานสากลอย่างมีประสิทธิภาพและประสิทธิผล พร้อมจัดทำความเสี่ยงที่ยอมรับได้ (Risk Appetite) เพื่อใช้เป็นเกณฑ์ในการกำหนดกลยุทธ์หรือมาตรการที่เหมาะสมในการจัดการความเสี่ยง และเป็นกรอบการปฏิบัติงานบริหารความเสี่ยงของพนักงานทุกคนในบริษัทให้เป็นไปในทิศทางเดียวกัน
6. บริษัทกำหนดให้มีการแต่งตั้งคณะทำงานบริหารความเสี่ยงเป็นผู้รับผิดชอบในการกำหนดและปฏิบัติงานตามแผนการจัดการการบริหารความเสี่ยง ตลอดจนรายงานผลต่อคณะกรรมการบริษัทและ/หรือ คณะกรรมการตรวจสอบ และ/หรือ คณะกรรมการบริหาร
7. บริษัทกำหนดให้มีการระบุและประเมินความเสี่ยงซึ่งจะพิจารณาจากทั้งปัจจัยภายนอก และปัจจัยภายในองค์กรที่อาจส่งผลให้บริษัทไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้
8. บริษัทกำหนดให้มีเกณฑ์ในการประเมินความเสี่ยง การจัดระดับความเสี่ยงที่ได้ระบุไว้ และแนวทางในการตอบสนองต่อความเสี่ยงเพื่อให้สามารถจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้โดยคำนึงถึงต้นทุน และผลประโยชน์ที่จะได้รับจากการดำเนินการตามแนวทางต่าง ๆ
9. ผู้บริหารและพนักงานทุกคนของบริษัท มีหน้าที่ความรับผิดชอบในการระบุ วิเคราะห์ ประเมินและจัดลำดับความเสี่ยงของหน่วยงานที่ตนเองรับผิดชอบ รวมทั้งกำหนดแนวทาง และ/หรือมาตรการที่เหมาะสมเพื่อจัดการความเสี่ยงตามลำดับความสำคัญ

กระบวนการบริหารความเสี่ยง

การบริหารความเสี่ยงตามมาตรฐานจะระบุขั้นตอนในการบริหารความเสี่ยง ประกอบด้วย 8 ขั้นตอน ซึ่งครอบคลุมแนวทางการกำหนดนโยบายการบริหารงาน การดำเนินงาน และการบริหารความเสี่ยง ดังนี้

1. **สภาพแวดล้อมภายในองค์กร (Internal Environment)**

สภาพแวดล้อมขององค์กรเป็นองค์ประกอบที่สำคัญ ในการกำหนดกรอบบริหารความเสี่ยง ประกอบด้วย ปัจจัยหลายประการ เช่น จริยธรรม วัฒนธรรมองค์กร นโยบายของผู้บริหาร แนวทางการปฏิบัติงานบุคลากร กระบวนการทำงาน ระบบสารสนเทศ ระเบียบ เป็นต้น สภาพแวดล้อมภายในองค์กรประกอบเป็นพื้นฐานสำคัญในการกำหนดทิศทางของกรอบการบริหารความเสี่ยงขององค์กร

2. **การกำหนดวัตถุประสงค์ (Objective Setting)**

องค์กรต้องพิจารณากำหนดวัตถุประสงค์ในการบริหารความเสี่ยง ให้มีความสอดคล้องกับกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ เพื่อวางเป้าหมายในการบริหารความเสี่ยงขององค์กรได้อย่างชัดเจน และเหมาะสม

3. **การบ่งชี้เหตุการณ์ (Event Identification)**

เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงาน ทั้งในส่วนของปัจจัยเสี่ยงที่เกิดจากภายในและภายนอกองค์กร เช่น นโยบายบริหารงาน บุคลากร การปฏิบัติงาน การเงิน ระบบสารสนเทศ ระเบียบ กฎหมาย ระบบบัญชี ภาษีอากร ทั้งนี้เพื่อทำความเข้าใจต่อเหตุการณ์และสถานการณ์นั้น เพื่อให้ผู้บริหารสามารถพิจารณากำหนดแนวทางและนโยบายในการจัดการกับความเสี่ยงที่อาจจะเกิดขึ้นได้เป็นอย่างดี โดยครอบคลุมความเสี่ยงใน 5 ด้าน ได้แก่

1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) ความเสี่ยงที่เกี่ยวข้องกับการกำหนดแผนกลยุทธ์ แผนการดำเนินงาน และการนำแผนดังกล่าวไปปฏิบัติอย่างไม่เหมาะสม นอกจากนี้ ยังรวมถึงการเปลี่ยนแปลงจากปัจจัยภายนอกและปัจจัยภายใน อันส่งผลกระทบต่อการทำหนดกลยุทธ์ หรือการดำเนินงานเพื่อให้บรรลุวัตถุประสงค์หลัก เป้าหมาย และแนวทางการดำเนินงานขององค์กร
2) ความเสี่ยงด้านการเงิน (Financial Risk) ความเสี่ยงที่เกี่ยวข้องกับการบริหารจัดการทางการเงิน โดยอาจเป็นความเสี่ยงที่เกิดจากปัจจัยภายใน เช่น การบริหารจัดการด้านสภาพคล่อง ด้านเครดิต ด้านเงินลงทุน หรือจากปัจจัยภายนอก เช่น การเปลี่ยนแปลงของอัตราดอกเบี้ย อัตราแลกเปลี่ยน หรือความเสี่ยงที่คู่สัญญาไม่สามารถปฏิบัติตามภาระผูกพันที่ตกลงไว้ อันส่งผลกระทบต่อการดำรงอยู่ รวมถึงส่งผลให้เกิดความเสียหายต่อองค์กร
3) ความเสี่ยงด้านปฏิบัติการ (Operational Risk) ความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติงานของแต่ละกระบวนการ หรือกิจกรรมภายในองค์กร รวมทั้งความเสี่ยงที่เกี่ยวข้องกับการบริหารจัดการข้อมูลด้านเทคโนโลยีสารสนเทศ และข้อมูลความรู้ต่าง ๆ เพื่อให้การปฏิบัติงานบรรลุเป้าหมายที่กำหนด ซึ่งความเสี่ยงด้านปฏิบัติการจะส่งผลกระทบต่อประสิทธิภาพของกระบวนการทำงาน และการบรรลุวัตถุประสงค์หลักขององค์กรในภาพรวม
4) ความเสี่ยงด้านการดำเนินการให้เป็นไปตามกฎหมาย และกฎเกณฑ์ต่าง ๆ (Compliance Risk) ความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติตามกฎหมาย กฎระเบียบ ข้อบังคับของหน่วยงานต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจของกลุ่มบริษัท ซึ่งเมื่อมีความเสี่ยงด้านนี้เกิดขึ้น จะส่งผลกระทบต่อชื่อเสียงและภาพลักษณ์ขององค์กรโดยรวม
5) ความเสี่ยงด้านการทุจริต (Fraud Risk) ความเสี่ยงที่เกี่ยวข้องกับการทุจริตที่อาจเกิดขึ้นจากกิจกรรม กระบวนการหรือขั้นตอนการปฏิบัติงานของหน่วยงานนั้น ๆ ซึ่งเกี่ยวข้องกับผู้มีส่วนได้เสีย (stakeholders) ทุกฝ่ายทั้งภายในและภายนอกองค์กรที่อาจทำให้เกิดการทุจริต ซึ่งสามารถแบ่งเป็น 3 ด้าน ได้แก่
   - ความเสี่ยงการทุจริตที่เกี่ยวข้องกับการพิจารณาอนุมัติ และ/หรือ อนุญาต

- ความเสี่ยงการทุจริตในความโปร่งใสของการใช้อำนาจ และตำแหน่งหน้าที่
- ความเสี่ยงการทุจริตเรื่องการขอ และ/หรือ ใช้จ่ายงบประมาณ

4. การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงเป็นการจำแนกและพิจารณาจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่ โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) โดยสามารถประเมินความเสี่ยงได้ทั้งจากปัจจัยความเสี่ยงภายนอกและปัจจัยความเสี่ยงภายในองค์กร

5. การตอบสนองความเสี่ยง (Risk Response)

เป็นการดำเนินการหลังจากที่องค์กรสามารถบ่งชี้ความเสี่ยงขององค์กร และประเมินความสำคัญของความเสี่ยงแล้ว โดยจะต้องนำความเสี่ยงไปดำเนินการตอบสนองด้วยวิธีการที่เหมาะสม เพื่อลดความสูญเสียหรือโอกาสที่จะเกิดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้

<u>แนวทางในการจัดการความเสี่ยง</u>

- การหลีกเลี่ยง (Avoid) เป็นการดำเนินการเพื่อหลีกเลี่ยงเหตุการณ์ที่ก่อให้เกิดความเสี่ยง มักใช้ในกรณีที่ความเสี่ยงมีความรุนแรงสูง ไม่สามารถหาวิธีลด/จัดการให้อยู่ในระดับที่ยอมรับได้
- การร่วมจัดการ (Share) เป็นการร่วมหรือถ่ายโอนความเสี่ยงทั้งหมดหรือบางส่วนไปยังบุคคล/หน่วยงานภายนอกองค์กร ให้ช่วยแบกรับภาระความเสี่ยงแทน เช่น การซื้อกรมธรรม์ประกันภัย
- การลด (Reduce) เป็นการจัดหามาตรการจัดการ เพื่อลดโอกาสการเกิดเหตุการณ์ความเสี่ยง หรือลดผลกระทบที่อาจเกิดขึ้น ให้อยู่ในระดับที่ยอมรับได้เช่น การเตรียมแผนฉุกเฉิน (Contingency plan)
- การยอมรับ (Accept) ความเสี่ยงที่เหลือในปัจจุบันอยู่ในระดับที่ยอมรับได้โดยไม่ต้องดำเนินการใด ๆ เพื่อลดโอกาสหรือผลกระทบที่อาจเกิดขึ้นอีก มักใช้กับความเสี่ยงที่ต้นทุนของมาตรการจัดการสูงไม่คุ้มกับประโยชน์ที่ได้รับ

6. กิจกรรมการควบคุม (Control Activities)

การกำหนดกิจกรรมและการปฏิบัติต่าง ๆ ที่กระทำเพื่อลดความเสี่ยง และทำให้การดำเนินงานบรรลุตามวัตถุประสงค์และเป้าหมายขององค์กร เช่น การกำหนดกระบวนการปฏิบัติงานที่เกี่ยวข้องกับการจัดการความเสี่ยงให้กับบุคลากรภายในองค์กร เพื่อเป็นการสร้างความมั่นใจว่าจะสามารถจัดการกับความเสี่ยงนั้นได้อย่างถูกต้องและเป็นไปตามเป้าหมายที่กำหนด

7. สารสนเทศและการสื่อสาร (Information and Communication)

องค์กรจะต้องมีระบบสารสนเทศและการติดต่อสื่อสารที่มีประสิทธิภาพ เพราะเป็นพื้นฐานสำคัญที่จะนำไปพิจารณาดำเนินการบริหารความเสี่ยงให้เป็นไปตามกรอบ และขั้นตอนการปฏิบัติที่องค์กรกำหนด

8. การติดตามประเมินผล (Monitoring)

องค์กรจะต้องมีการติดตามผล เพื่อให้ทราบถึงผลการดำเนินการว่ามีความเหมาะสมและสามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพหรือไม่ เพื่อให้มั่นใจว่า

- เจ้าของความเสี่ยง (Risk Owner) มีการติดตาม ประเมินสถานการณ์ วิเคราะห์และบริหารความเสี่ยงที่อยู่ภายใต้ความรับผิดชอบของตนอย่างสม่ำเสมอ และเหมาะสม
- ระบบการควบคุมภายในที่วางไว้มีความเพียงพอ เหมาะสม มีประสิทธิผล และมีการนำมาปฏิบัติใช้จริงเพื่อป้องกันหรือลดความเสี่ยงที่อาจเกิดขึ้น รวมทั้งมีการปรับปรุงแก้ไขการควบคุมภายในอยู่เสมอเพื่อให้สอดคล้องกับสถานการณ์หรือความเสี่ยงที่เปลี่ยนไป