บริษัท โรงแรมเซ็นทรัลพลาซา จำกัด (มหาชน)

กรอบการบริหารความเสี่ยง

(ฉบับทบทวน ปี 2569)

ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 7/2568
เมื่อวันที่ 14 พฤศจิกายน 2568

จัดทำโดย ฝ่ายบริหารความเสี่ยง

PUBLIC

กรอบการบริหารความเสี่ยง (ฉบับทบทวน ปี 2569)
บริษัท โรงแรมเซ็นทรัลพลาซา จำกัด (มหาชน)

วัตถุประสงค์หลักในการดำเนินธุรกิจของบริษัท คือการเพิ่มคุณค่าให้กับผู้มีส่วนได้เสียทุกฝ่าย ซึ่งรวมถึงผู้ถือหุ้น ลูกค้า คู่ค้า พนักงานทั้งหมด รัฐบาล และประชาชนทั่วไป อย่างไรก็ตาม ในการดำเนินธุรกิจ บริษัทต้องเผชิญหน้ากับความเสี่ยงซึ่งอาจเพิ่มหรือลดคุณค่าของบริษัทได้ จึงจำเป็นต้องบริหารความเสี่ยง โดยบริษัทมีการบริหารความเสี่ยงอย่างเป็นระบบตามมาตรฐานสากล (COSO Enterprise Risk Management Framework : COSO ERM) และบูรณาการการบริหารความเสี่ยงเข้ากับการวางแผนเชิงกลยุทธ์และการดำเนินธุรกิจเพื่อสร้างคุณค่า รักษาคุณค่า และทำให้คุณค่าเกิดขึ้นจริงต่อองค์กร ที่ปฏิบัติโดยคณะกรรมการบริษัท ผู้บริหาร และบุคลากรอื่นๆ เพื่อช่วยในการกำหนดกลยุทธ์ และปฏิบัติงานทั่วทั้งองค์กร กรอบการบริหารความเสี่ยงจึงได้รับการออกแบบให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อองค์กร และสามารถจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ เพื่อเป็นการรับประกันอย่างสมเหตุสมผลในการบรรลุวัตถุประสงค์ขององค์กร

1. คำนิยาม

- **ความเสี่ยง (Risk)** คือ ความเป็นไปได้ของเหตุการณ์ที่อาจเกิดขึ้น และส่งผลกระทบต่อการบรรลุกลยุทธ์และวัตถุประสงค์ทางธุรกิจ
- **การบริหารความเสี่ยงขององค์กร (Enterprise Risk Management)** คือ วัฒนธรรมองค์กร ความรู้ความสามารถ และแนวปฏิบัติที่บูรณาการร่วมกับการกำหนดกลยุทธ์และผลการปฏิบัติงาน ซึ่งองค์กรใช้ในการบริหารความเสี่ยงเกี่ยวกับการสร้างคุณค่า การรักษาคุณค่า และการทำให้คุณค่าเกิดขึ้นจริง
- **ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)** คือ ขนาด ปริมาณ หรือระดับความเสี่ยงที่องค์กรสามารถยอมรับได้เพื่อการสร้างคุณค่าโดยยังคงให้องค์กรสามารถบรรลุเป้าหมายได้ อาจเป็นค่าเดียว หรือเป็นช่วงขึ้นอยู่กับความเหมาะสมของแต่ละปัจจัย และได้รับอนุมัติจากคณะกรรมการบริษัท เพื่อใช้ในการประเมินและบริหารความเสี่ยง โดยความเสี่ยงใดที่ได้รับการวิเคราะห์และประเมินแล้วพบว่าอาจมีผลกระทบต่อบริษัท เกินกว่าระดับความเสี่ยงที่ยอมรับได้ ให้หน่วยงานเจ้าของความเสี่ยงนั้นๆ จัดทำแผนบริหารความเสี่ยง (Action Plan) และรายงานต่อคณะกรรมการบริหารความเสี่ยง การกำกับดูแล และความยั่งยืนเพื่อพิจารณาและนำเสนอต่อคณะกรรมการบริษัท
- **ทะเบียนความเสี่ยง (Risk Inventory)** คือ รายการความเสี่ยงทั้งหมดที่สามารถมีผลกระทบต่อองค์กร

- **ภาพความเสี่ยง (Risk Profile)** คือ ภาพรวมของความเสี่ยง ณ ระดับใดระดับหนึ่งของกิจการ หรือแง่มุมของธุรกิจ ซึ่งทำให้ผู้บริหารสามารถพิจารณาประเภท ความรุนแรง และความเกี่ยวข้องกันของความเสี่ยงต่างๆ รวมทั้งทำให้สามารถพิจารณาได้ว่า อาจกระทบต่อผลการปฏิบัติงานในส่วนที่เกี่ยวกับกลยุทธ์และวัตถุประสงค์ทางธุรกิจของกิจการ
- **ปัจจัยเสี่ยง (Risk Factor)** คือ ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงและเหตุการณ์ที่จะทำให้ไม่บรรลุวัตถุประสงค์ หรือเป้าหมายที่กำหนดไว้ ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง ที่สามารถอธิบายได้ว่าสาเหตุปัจจัยเสี่ยงดังกล่าวส่งผลให้เกิดความเสี่ยงใด และสามารถหามาตรการจัดการเพื่อลดความเสี่ยงที่จะเกิดขึ้นได้อย่างถูกต้อง
- **การประเมินความเสี่ยง (Risk Assessment)** คือ กระบวนการในการระบุระดับความรุนแรง และการจัดลำดับความสำคัญของความเสี่ยง โดยประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) ที่จะเกิดขึ้น

2. บทบาทและความรับผิดชอบในการบริหารความเสี่ยง

- **คณะกรรมการบริษัท**
  มีหน้าที่ความรับผิดชอบในการกำหนดนโยบาย ทิศทางกลยุทธ์ของบริษัท และกำกับดูแลให้บริษัทมีระบบการบริหารความเสี่ยง อย่างมีประสิทธิภาพ และประสิทธิผล เพื่อให้มั่นใจว่าฝ่ายบริหารให้ความสำคัญต่อการบริหารความเสี่ยง และปลูกฝังจนเป็นวัฒนธรรมองค์กร
- **คณะกรรมการบริหารความเสี่ยง การกำกับดูแล และความยั่งยืน**
  มีหน้าที่ความรับผิดชอบในการกำหนดแนวทางในการบริหารความเสี่ยง พิจารณาให้ความเห็นชอบกรอบบริหารความเสี่ยงเพื่อใช้เป็นแนวปฏิบัติของบริษัท ติดตามผลการบริหารความเสี่ยง สนับสนุนให้มีการเผยแพร่ สร้างความเข้าใจในเรื่องการบริหารความเสี่ยงให้กับพนักงานทุกระดับและให้มีผลในทางปฏิบัติทั่วทั้งองค์กร รวมทั้งให้ความเห็น/ข้อแนะนำ ให้คำปรึกษาแก่ฝ่ายบริหาร และรายงานต่อคณะกรรมการบริษัท
- **ประธานเจ้าหน้าที่บริหาร และผู้บริหาร**
  มีหน้าที่ความรับผิดชอบในการจัดให้มีระบบบริหารความเสี่ยงตามนโยบายและแนวทางที่คณะกรรมการกำหนด พิจารณาและกำหนดกลยุทธ์ และกำหนดให้มีการจัดทำและติดตามแผนบริหารความเสี่ยงทั่วทั้งองค์กร กำหนดและมอบหมายความรับผิดชอบความเสี่ยง (Risk Owner) พิจารณาและกำหนดระดับความเสี่ยงที่ยอมรับได้ เพื่อนำเสนอขออนุมัติต่อคณะกรรมการบริษัท สื่อสารและพัฒนาวัฒนธรรมองค์กรที่ตระหนักรู้ความเสี่ยง รวมทั้งทบทวนความเหมาะสมของระบบและมาตรการต่างๆ

- **ผู้รับผิดชอบความเสี่ยง (Risk Owner)**
  มีหน้าที่ความรับผิดชอบในการประเมินและวิเคราะห์ความเสี่ยง กำหนดมาตรการ/กิจกรรมที่ใช้ในการจัดการความเสี่ยง วิเคราะห์ต้นทุน-ผลประโยชน์ (Cost – Benefit) ของแต่ละทางเลือก ติดตามผลการประเมินความเสี่ยง และนำเสนอต่อประธานเจ้าหน้าที่บริหาร และคณะกรรมการบริหารความเสี่ยง การกำกับดูแล และความยั่งยืน
- **หน่วยงานบริหารความเสี่ยง**
  มีหน้าที่ความรับผิดชอบในการพัฒนาระบบบริหารความเสี่ยงให้มีประสิทธิภาพ ประสิทธิผล ให้คำแนะนำ ปรึกษา และจัดอบรมสร้างความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยง เพื่อนำไปสู่การสร้างวัฒนธรรมองค์กร ประสานงาน และติดตามผลการบริหารความเสี่ยงจาก Risk Owner และผู้ที่เกี่ยวข้องเพื่อจัดทำรายงานความเสี่ยงเสนอฝ่ายบริหาร และคณะกรรมการบริหารความเสี่ยง การกำกับดูแล และความยั่งยืน และ/หรือคณะกรรมการบริษัท ตามที่ได้รับมอบหมาย
- **พนักงานทุกคน**
  มีหน้าที่ในการปฏิบัติตามนโยบายและกระบวนการบริหารความเสี่ยงของบริษัท รวมถึงแนวทางหรือคำสั่งอื่นๆ ที่ออกโดยคณะกรรมการบริษัท หรือคณะกรรมการบริหารความเสี่ยง การกำกับดูแล และความยั่งยืน

3. กรอบโครงสร้างการบริหารความเสี่ยง

บริษัทมีการกำหนดกรอบโครงสร้างการบริหารความเสี่ยง โดยอ้างอิงตามมาตรฐานสากล (COSO Enterprise Risk Management Framework : COSO ERM) ซึ่งเป็นการบริหารความเสี่ยงขององค์กร โดยการบูรณาการร่วมกับกลยุทธ์และผลการปฏิบัติงาน สร้างความชัดเจนเกี่ยวกับความสำคัญของการบริหารความเสี่ยงขององค์กรในการวางแผนกลยุทธ์ และความสำคัญในการนำการบริหารความเสี่ยงขององค์กรไปใช้ร่วมกับการดำเนินงานทั่วทั้งองค์กร ซึ่งแบ่งได้เป็น 5 องค์ประกอบที่สัมพันธ์กัน ดังนี้

1) การกำกับดูและวัฒนธรรม (Governance & Culture)

บริษัทมีการจัดโครงสร้างและกำหนดหน้าที่ความรับผิดชอบในการบริหารความเสี่ยงอย่างชัดเจน รวมถึง การสร้างวัฒนธรรมองค์กรที่เน้นการตระหนักถึงความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินธุรกิจ

2) กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy & Objective-Setting)

บริษัทมีกระบวนการวางแผนกลยุทธ์ที่บูรณาการหลักการบริหารความเสี่ยง และมีการพัฒนากลยุทธ์และกำหนดวัตถุประสงค์ทางธุรกิจให้สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้

3) ผลการปฏิบัติงาน (Performance)

บริษัทมีการระบุและประเมินความเสี่ยงที่อาจมีผลกระทบต่อความสำเร็จของกลยุทธ์และวัตถุประสงค์ทางธุรกิจ ซึ่งความเสี่ยงจะถูกจัดลำดับความสำคัญตามระดับของผลกระทบและโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสี่ยง รวมทั้งมีการกำหนดวิธีการตอบสนองต่อความเสี่ยง เพื่อนำไปใช้อย่างเหมาะสม และผลของกระบวนการข้างต้นนี้จะรายงานต่อผู้มีส่วนได้ส่วนเสียสำคัญของความเสี่ยง

4) การสอบทานและแก้ไขปรับปรุง (Review & Revision)

บริษัทมีการสอบทานผลการปฏิบัติงานอย่างสม่ำเสมอ เพื่อพิจารณาว่าองค์กรมีการบริหารความเสี่ยงที่มีประสิทธิผลเพียงใด และมีการทบทวนการบริหารความเสี่ยงเพื่อให้เกิดการปรับปรุงอย่างต่อเนื่อง

5) สารสนเทศ การสื่อสารและการรายงาน (Information, Communication & Reporting)

บริษัทมีระบบสารสนเทศที่ส่งเสริมให้การบริหารความเสี่ยงสามารถดำเนินไปอย่างมีประสิทธิภาพ ซึ่งระบบดังกล่าว จะช่วยสนับสนุนข้อมูลความเสี่ยง ข้อมูลผลการปฏิบัติงาน และการจัดทำรายงานผลการบริหารความเสี่ยง เพื่อให้มีการสื่อสารผลการบริหารความเสี่ยงต่อผู้มีส่วนได้เสียอย่างต่อเนื่องและเหมาะสม

4. กระบวนการบริหารความเสี่ยง

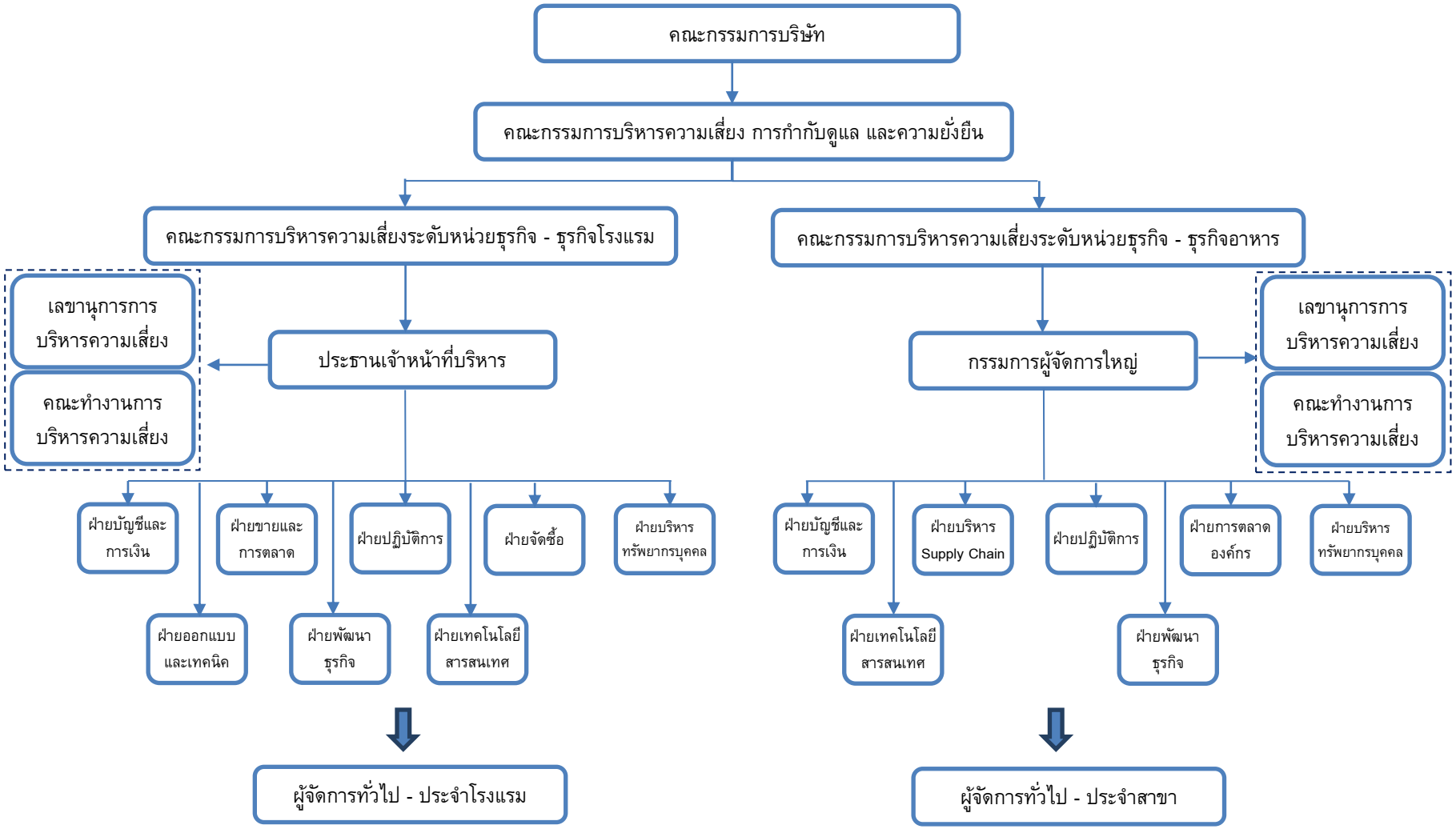
การบริหารความเสี่ยงขององค์กรเป็นกระบวนการที่ต้องทำอย่างต่อเนื่องทั้งองค์กร โดยครอบคลุมทุกระดับของการดำเนินงานในองค์กร เช่น ระดับแผนก ส่วนงาน หน่วยธุรกิจ กิจกรรมการดำเนินงาน และโครงการต่างๆ เพื่อให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการดำเนินงานในทุกระดับขององค์กร

กระบวนการบริหารความเสี่ยง หมายถึง กระบวนการที่บุคลากรทั่วทั้งองค์กรได้มีส่วนร่วมในการคิดวิเคราะห์ และคาดการณ์ถึงเหตุการณ์ หรือความเสี่ยงที่อาจจะเกิดขึ้น รวมทั้งการระบุแนวทางในการจัดการกับความเสี่ยงดังกล่าว ให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้ เพื่อช่วยให้องค์กรบรรลุในวัตถุประสงค์ที่ต้องการ ตามกรอบวิสัยทัศน์ และพันธกิจขององค์กร

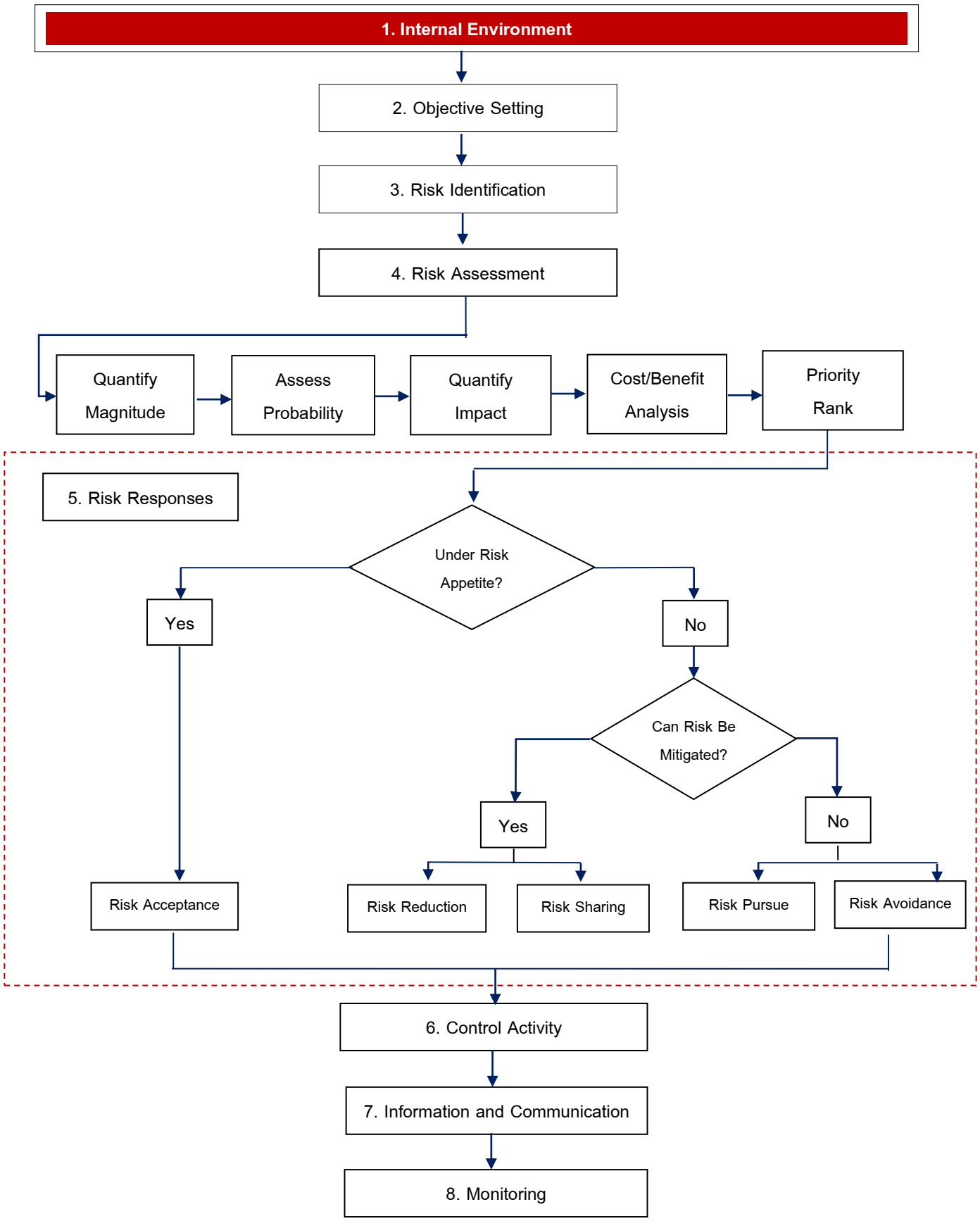
บริษัทกำหนดกระบวนการบริหารความเสี่ยง เพื่อให้ขั้นตอนและวิธีการในการบริหารความเสี่ยงเป็นไปอย่างมีระบบและดำเนินไปในทิศทางเดียวกันทั่วทั้งองค์กร ประกอบด้วย 8 ขั้นตอน ดังนี้

1) สภาพแวดล้อมภายในองค์กร (Internal Environment)
2) การกำหนดวัตถุประสงค์ (Objective Setting)
3) การระบุความเสี่ยง (Risk Identification)
4) การประเมินความเสี่ยง (Risk Assessment)
5) การตอบสนองความเสี่ยง (Risk Responses)
6) กิจกรรมการควบคุม (Control Activities)
7) สารสนเทศและการสื่อสาร (Information and Communication)
8) การติดตาม (Monitoring)

โครงสร้างการบริหารความเสี่ยงของบริษัท โรงแรมเซ็นทรัลพลาซา จำกัด (มหาชน)



แผนภาพขั้นตอนการบริหารความเสี่ยง



ขั้นตอนสำคัญของกระบวนการบริหารความเสี่ยงองค์กร ประกอบด้วย 8 ขั้นตอน ดังนี้

4.1 สภาพแวดล้อมภายในองค์กร (Internal Environment)

สภาพแวดล้อมภายในองค์กรเป็นปัจจัยสำคัญในการกำหนดทิศทางของกรอบการบริหารความเสี่ยง ขององค์กร ซึ่งประกอบด้วยหลายปัจจัย เช่น วัฒนธรรมองค์กร นโยบายของผู้บริหาร แนวทางการปฏิบัติงานบุคลากร กระบวนการทำงาน ระบบสารสนเทศ เป็นต้น

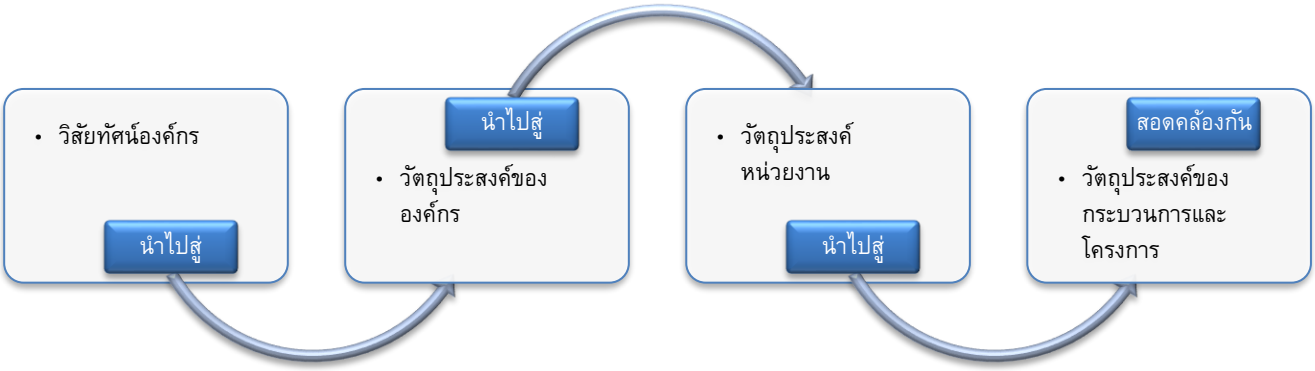
วัฒนธรรมองค์กรพัฒนาขึ้นมาจากการมีส่วนร่วมของพนักงานในทุกระดับ เนื่องจากสมาชิกในองค์กรและ พนักงานแต่ละคนนั้น มีความเข้าใจในการบริหารความเสี่ยง ที่แตกต่างกันไป ดังนั้น จึงมีวิธีการระบุ ประเมิน และ ตอบสนองต่อความเสี่ยงที่แตกต่างกัน การมีวัฒนธรรม องค์กรที่ตรงกันจะช่วยให้พนักงานเข้าใจเรื่องการบริหารความเสี่ยงองค์กรได้ในแนวทางเดียวกัน

4.2 การกำหนดวัตถุประสงค์ (Objective Setting)

การกำหนดวัตถุประสงค์ภายในองค์กรต้องมีความสอดคล้องและเป็นไปในทิศทางเดียวกัน เพื่อให้เกิดความมั่นใจว่ากิจกรรมต่างๆ ที่หน่วยงาน ผู้บริหาร และพนักงานจัดทำช่วยสนับสนุนให้สามารถบรรลุวัตถุประสงค์ขององค์กร

การกำหนดวัตถุประสงค์ในการบริหารความเสี่ยง ต้องให้มีความสอดคล้องกับกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ เพื่อวางเป้าหมายในการบริหารความเสี่ยงขององค์กรได้อย่างชัดเจน และเหมาะสม

ภาพด้านล่างแสดงถึงความสอดคล้องของวัตถุประสงค์ในระดับต่างๆ ที่บริษัทควรมี



ขั้นตอนการกำหนดวัตถุประสงค์

1. คณะกรรมการบริษัท และผู้บริหารระดับสูง กำหนดวิสัยทัศน์ พันธกิจ และวัตถุประสงค์เชิงกลยุทธ์ของบริษัท จากนั้นจึงกำหนดเป้าหมายภาพรวมของบริษัท ที่สอดคล้องและสนับสนุนการบรรลุซึ่งวิสัยทัศน์และพันธกิจ
2. คณะกรรมการบริษัท และผู้บริหารระดับสูงพิจารณาประเภทและระดับความเสี่ยงที่บริษัท ยอมรับได้ (Risk Appetite) และกำหนดกลยุทธ์ทางธุรกิจให้สอดคล้องกับระดับความเสี่ยงที่บริษัทยอมรับได้ เพื่อใช้เป็นแนวทางในการกำหนดกลยุทธ์ทางธุรกิจให้สอดคล้องกัน
3. ผู้บริหารกำหนดวัตถุประสงค์ระดับสายงาน ระดับกระบวนการหลัก หรือระดับโครงการต่างๆ ที่มีความสำคัญให้สอดคล้องกับกลยุทธ์เชิงธุรกิจของบริษัท วัตถุประสงค์ที่กำหนดขึ้นควรมีความสัมพันธ์ที่ชัดเจนกับวัตถุประสงค์เชิงกลยุทธ์ของบริษัท และสนับสนุนต่อการบรรลุวัตถุประสงค์เชิงกลยุทธ์ด้วย แม้ว่าวัตถุประสงค์ต่างๆ อาจมีความสำคัญไม่เท่าเทียมกัน แต่อย่างไรก็ตาม การกำหนดวัตถุประสงค์ควรเป็นไปตามหลักการ “SMART” ให้มากที่สุด

หลักในการกำหนดวัตถุประสงค์

วัตถุประสงค์ต้องมีความชัดเจนและเป็นไปได้ตามหลักการ ที่เรียกว่า SMART ดังนี้

หัวข้อ	ความหมาย
Specific ชัดเจน	วัตถุประสงค์ควรมีความชัดเจน เฉพาะเจาะจง และหลีกเลี่ยงความคลุมเครือ เพื่อให้เกิดความเข้าใจตรงกัน
Measurable วัดผลได้	วัตถุประสงค์ควรสามารถวัดผลได้ทั้งในเชิงปริมาณและคุณภาพ และ ควรมีการระบุหลักเกณฑ์และข้อมูลที่ต้องการใช้ในการวัดผล
Achievable บรรลุได้	วัตถุประสงค์ควรเป็นไปตามความเป็นจริง มีความสมเหตุสมผลและสามารถปฏิบัติให้บรรลุได้จริง โดยพิจารณาจากทรัพยากรและข้อจำกัดที่มีอยู่ เช่น สภาพตลาด ช่วงเวลา การจัดสรรทรัพยากร เป็นต้น
Relevant เกี่ยวข้องสอดคล้อง	ผลตอบแทนหรือผลลัพธ์ของวัตถุประสงค์ที่กำหนดขึ้นต้องสอดคล้องและสนับสนุนการบรรลุวัตถุประสงค์ในระดับที่สูงกว่า
Time bound กำหนดระยะเวลา	ควรกำหนดกรอบเวลาในการบรรลุวัตถุประสงค์ให้ชัดเจน

4.3 การระบุความเสี่ยง (Risk Identification)

การระบุความเสี่ยง (Risk Identification) เป็นการรวบรวมเหตุการณ์ซึ่งอาจจะเป็นความเสี่ยงต่อวัตถุประสงค์ขององค์กรที่ตั้งไว้ โดยผู้บริหารจะต้องพิจารณาความเสี่ยงทุกด้านที่อาจเกิดขึ้น การระบุความเสี่ยงอาจดำเนินการโดยการสัมภาษณ์ผู้บริหารระดับสูงหรือฝ่ายจัดการที่รับผิดชอบในแผนงานหรือการดำเนินการนั้น และรวมประเด็นความเสี่ยงสำคัญที่ได้รับความสนใจหรือประเด็นที่กังวล เพื่อนำมาจัดทำภาพรวมความเสี่ยงขององค์กร (Corporate Risk Profile) ซึ่งหมายถึงประเภทความเสี่ยงสำคัญ ที่อาจทำให้การดำเนินการไม่เป็นไปตามวิสัยทัศน์ วัตถุประสงค์ เป้าหมายที่กำหนด ซึ่งความเสี่ยงเหล่านี้มีความเป็นไปได้ที่จะเกิดขึ้นในอนาคตหรือเป็นเหตุการณ์ที่ทำให้องค์กรสูญเสียโอกาสในการดำเนินธุรกิจ โดยการระบุความเสี่ยงนั้นควรพิจารณาทั้งปัจจัยภายในและภายนอกองค์กร

1) ปัจจัยภายใน เป็นความเสี่ยงจากสิ่งที่เราควบคุมได้ เรากำหนดขึ้น หรือความเสี่ยงจากความสามารถของเราเอง เช่น วัตถุประสงค์ขององค์กร, นโยบายและกลยุทธ์, การดำเนินงาน, กระบวนการทำงาน, โครงสร้างองค์กร, วัฒนธรรมองค์กร รวมถึง ขีดความสามารถขององค์กร ในแง่ของทรัพยากรและความรู้ เช่น เงินทุน เวลา บุคลากร กระบวนการ ระบบและเทคโนโลยี เป็นต้น

2) ปัจจัยภายนอก เป็นความเสี่ยงที่เราไม่สามารถควบคุมได้ เกิดจากปัจจัยภายนอก ที่เราต้องหาวิธีการรับมือกับความเสี่ยงที่จะเกิดขึ้น เช่น นโยบายของรัฐ, สภาวะเศรษฐกิจ/สังคมการเมือง, การแข่งขัน, สงคราม และภัยธรรมชาติต่างๆ เป็นต้น

<u>ประเภทความเสี่ยง</u>

บริษัทได้จำแนกประเภทความเสี่ยง ได้ดังนี้

- **ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)**
  เป็นความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ หรือนโยบายการบริหารไม่เหมาะสม หรือไม่สอดคล้องกับปัจจัยต่างๆ เช่น นโยบายรัฐ การเปลี่ยนแปลงทางด้านกฎหมาย ปัญหาด้านมวลชน การไม่สามารถทำรายได้ให้เป็นไปตามเป้าหมาย แผนการลงทุนขาดความชัดเจน เป็นต้น ทำให้องค์กรไม่สามารถบรรลุวัตถุประสงค์หรือเป้าหมายขององค์กรได้
- **ความเสี่ยงด้านการเงิน (Financial Risk)**
  เป็นความเสี่ยงที่เกิดจากการขาดข้อมูล การวิเคราะห์ การวางแผน การควบคุม และจัดทำรายงานเพื่อนำมาใช้ในการบริหารการเงินอย่างถูกต้อง ส่งผลต่อสถานภาพหรือเสถียรภาพทางการเงินขององค์กร รวมถึงเกี่ยวข้องกับสภาพคล่องทางการเงิน เช่น ความผันผวนของอัตราดอกเบี้ย ความผันผวนของอัตราแลกเปลี่ยน ความเสี่ยงที่เกิดขึ้นจาก Counterparty เป็นต้น
- **ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)**
  เป็นความเสี่ยงที่ทุกธุรกิจจะต้องเผชิญอย่างหลีกเลี่ยงไม่ได้ โดยเป็นความเสี่ยงที่เกิดขึ้นจากบุคลากร กระบวนการทำงาน เทคโนโลยี และปัจจัยภายนอก ความเสี่ยงนี้เกิดขึ้นจากการดำเนินงานของธุรกิจตามปกติ แต่ธุรกิจจะต้องหาวิธีการในการควบคุม และจัดการป้องกันไม่ให้ความเสี่ยงเหล่านี้เกิดขึ้น ถ้าหากธุรกิจปล่อยให้มีความเสี่ยงในด้านปฏิบัติการเกิดขึ้นมาก

ผลการดำเนินงานของธุรกิจอาจไม่เป็นไปตามที่คาดการณ์ไว้ และส่งผลกระทบเสียหายต่อธุรกิจ เช่น ความล่าช้า ขาดอุปกรณ์ที่มีประสิทธิภาพ ระบบไอทีขัดข้อง

- **ความเสี่ยงด้านการปฏิบัติตามกฎ ระเบียบ ข้อบังคับและกฎหมาย (Compliance Risk)**
  เป็นความเสี่ยงที่เกิดจากการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หรือมาตรฐานที่เกี่ยวข้องกับการดำเนินงาน กฎหมายที่มีอยู่เป็นอุปสรรคต่อการปฏิบัติงาน และนโยบายและวิธีการปฏิบัติงานที่องค์กรกำหนดขึ้นไม่สามารถปฏิบัติได้ เช่น ไม่สามารถดำเนินงานตามกฎหมายใหม่ได้อย่างครบถ้วน ความสับสนในการเลือกกฎ/ระเบียบที่จะบังคับใช้
    - **ความเสี่ยงด้านการทุจริตคอร์รัปชั่น (Corruption Risk)**
      เป็นความเสี่ยงที่เกิดจากการกระทำใด ๆ เพื่อแสวงหาผลประโยชน์โดยมิชอบด้วยกฎหมาย โดยการให้หรือรับสินบน ไม่ว่าจะเป็นเงิน สิ่งของ การช่วยเหลือทางการเมือง การบริจาคเพื่อการกุศล ค่าบริการต้อนรับหรือค่าใช้จ่ายอื่นๆ โดยการเสนอให้ สัญญาว่าจะให้ ให้คำมั่น เรียกร้อง ให้หรือรับซึ่งเงิน หรือประโยชน์อื่นใดที่ไม่เหมาะสมแก่เจ้าหน้าที่รัฐ หน่วยงานรัฐ เอกชนหรือผู้มีหน้าที่ไม่ว่าโดยทางตรงหรือทางอ้อม เพื่อให้หน่วยงานหรือบุคคลดังกล่าวกระทำหรือยกเว้นการปฏิบัติหน้าที่โดยมิชอบ
- **ความเสี่ยงด้านไซเบอร์ (Cyber Risk)**
  เป็นความเสี่ยงที่เกี่ยวข้องกับเรื่องความปลอดภัยทางด้านไซเบอร์ที่เกิดจากการเปลี่ยนแปลงทางเทคโนโลยีสารสนเทศ รวมทั้งการเปลี่ยนแปลงเทคโนโลยีดิจิตัล (Digital Transformation) ซึ่งมีผลกระทบต่อการดำเนินงานของบริษัท และให้หมายรวมถึงระบบเทคโนโลยีสารสนเทศที่องค์กรใช้ในการดำเนินกิจกรรมทางธุรกิจที่สำคัญ
- **ความเสี่ยงจากการเปลี่ยนแปลงสภาพภูมิอากาศ (Climate Change Risk)**
  เป็นความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของสภาพอากาศและผลกระทบที่เกี่ยวข้อง ซึ่งอาจส่งผลต่อการดำเนินธุรกิจ ห่วงโซ่อุปทาน และความยั่งยืนขององค์กร

4.4 การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยง (Risk Assessment) เป็นกระบวนการที่ประกอบด้วย การวิเคราะห์ การประเมิน และการจัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร ซึ่งควรประเมินว่าความเสี่ยงเหล่านั้นมีผลกระทบในเชิงบวกหรือเชิงลบต่อการบรรลุวัตถุประสงค์อย่างไร และการประเมินความเสี่ยงจะเปรียบเทียบระหว่างระดับของความเสี่ยงที่ได้จากการวิเคราะห์ความเสี่ยงเทียบกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ในกรณีที่ระดับของความเสี่ยงไม่อยู่ในระดับที่ยอมรับได้ของเกณฑ์การยอมรับความเสี่ยง ความเสี่ยงดังกล่าวจะได้รับการจัดการทันที

โดยพิจารณาทั้งความเสี่ยงก่อนการควบคุม (Inherent Risk) ความเสี่ยงหลังการควบคุม (Residual Risk) และความเสี่ยงที่ต้องการ (Target Risk)

1) ความเสี่ยงก่อนการควบคุม (Inherent Risk)

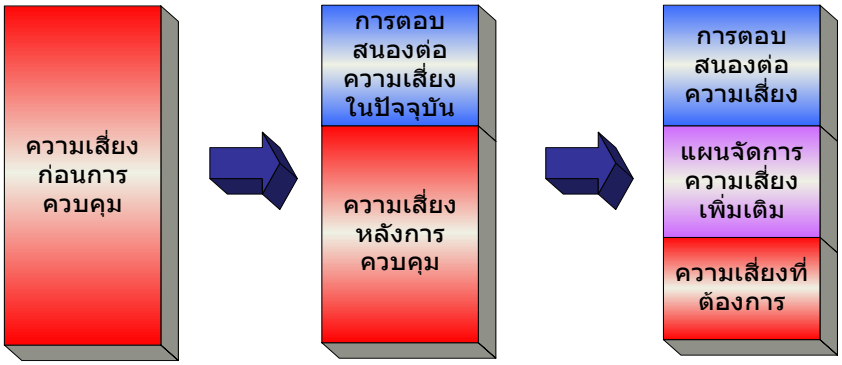
ความเสี่ยงก่อนการควบคุม คือ ความเสี่ยงขององค์กรที่ผู้บริหารยังไม่ได้มีการดำเนินการใดๆ เพื่อลดผลกระทบหรือโอกาสเกิดของความเสี่ยงนั้น การประเมินความเสี่ยงก่อนการควบคุมจะทำให้ผู้บริหารสามารถประมาณการทรัพยากรที่ต้องใช้และระดับการควบคุมที่ต้องมีในการจัดการความเสี่ยง

2) ความเสี่ยงหลังการควบคุม (Residual Risk)

ความเสี่ยงหลังการควบคุม คือ ความเสี่ยงที่คงเหลืออยู่ภายหลังจากการดำเนินกิจกรรมต่างๆ ที่มีอยู่ในปัจจุบันเพื่อจัดการความเสี่ยงแล้ว การประเมินความเสี่ยงหลังการควบคุมทำให้ผู้บริหารสามารถพิจารณาได้ว่าการควบคุมที่มีอยู่ในปัจจุบันมีประสิทธิภาพเพียงพอ ขาดประสิทธิภาพ หรือมีการควบคุมเกินความจำเป็น หลังจากการประเมินความเสี่ยงหลังการควบคุม หากผู้บริหารมีความประสงค์ที่จะลดระดับความเสี่ยง ผู้บริหารสามารถจัดทำแผนจัดการความเสี่ยงเพิ่มเติมได้

3) ความเสี่ยงที่ต้องการ (Target Risk)

ความเสี่ยงที่ต้องการ คือ ระดับความเสี่ยงที่องค์กรต้องการ หลังจากที่มีการดำเนินการตามแผนจัดการความเสี่ยงแล้ว



แผนภาพนี้แสดงให้เห็นถึงลำดับในการพิจารณาความเสี่ยง โดยผู้บริหารสามารถทำตามขั้นตอนดังต่อไปนี้

- ประเมินความเสี่ยงก่อนการควบคุม
- นำการตอบสนองต่อความเสี่ยงที่มีในปัจจุบันมาใช้เพื่อประเมินความเสี่ยงหลังการควบคุม
- กำหนดระดับความเสี่ยงที่ต้องการโดยจัดทำแผนจัดการความเสี่ยงเพิ่มเติมเพื่อลดระดับความเสี่ยงให้ถึงระดับที่ต้องการ

การกำหนดเกณฑ์ความเสี่ยง

เกณฑ์ที่ใช้ในการประเมินความเสี่ยงควรสะท้อนถึงคุณค่า วัตถุประสงค์และทรัพยากรขององค์กร โดยเกณฑ์บางประเภทอาจพัฒนาได้จากข้อกำหนดทางกฎหมายหรือข้อบังคับของหน่วยงานกำกับดูแลหรือหน่วยงานที่เป็นสมาชิกอยู่ ซึ่งเกณฑ์ที่กำหนดต้องสอดคล้องกับนโยบายความเสี่ยงขององค์กรและมีการทบทวนอย่างต่อเนื่อง

ในการประเมินความเสี่ยง จะพิจารณาจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบจากเหตุการณ์ความเสี่ยง (Impact) เพื่อจัดระดับความสำคัญของความเสี่ยง โดยใช้แผนภูมิความเสี่ยง (Risk Map) รวมทั้งกำหนดระดับความเสี่ยงที่ยอมรับได้ และตัวชี้วัดความเสี่ยง (Key Risk Indicators)

- โอกาสที่จะเกิด (Likelihood) คือ การพิจารณาความเป็นไปได้ที่จะเกิดเหตุการณ์ความเสี่ยงในช่วงเวลาหนึ่ง หรือจะเรียกว่า ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงก็ได้
- ผลกระทบ (Impact) คือ ระดับความรุนแรงของผลเสียหายที่จะเกิดขึ้น จากความเสี่ยง และมีผลกระทบต่อองค์กรซึ่งอาจเป็นได้ทั้งในด้านบวกและด้านลบ โดยสามารถแบ่งเป็นผลกระทบทางด้านการเงินและผลกระทบที่ไม่ใช่ทางการเงิน

ผู้บริหารสามารถประเมินระดับโอกาสเกิดและผลกระทบของความเสี่ยง โดยการให้คะแนน ตั้งแต่ 1 ถึง 5 แผนภาพด้านล่างแสดงถึงแนวทางในการประเมินโอกาสเกิดและผลกระทบ

เกณฑ์การประเมินความเสี่ยงต้องได้รับอนุมัติโดยคณะกรรมการบริหารความเสี่ยง การกำกับดูแล และความยั่งยืนและควรได้รับการสอบทานอย่างสม่ำเสมอเพื่อให้สอดคล้องกับการเปลี่ยนแปลงทางธุรกิจ

➢ เกณฑ์การประเมินความเสี่ยงด้านโอกาสเกิด (Likelihood Assessment Criteria)

เกณฑ์การประเมินความเสี่ยงด้านโอกาสเกิด เป็นเกณฑ์ที่กำหนดขึ้นเพื่อใช้สำหรับพิจารณาระดับของโอกาสหรือความเป็นไปได้ที่เหตุการณ์ความเสี่ยงจะเกิดขึ้นจริง โดยจะต้องคำนึงสภาพแวดล้อมจากปัจจัยภายในและปัจจัยภายนอกองค์กรที่มีอิทธิพลต่อความเสี่ยง กำหนดไว้ 5 ระดับ ดังนี้

เกณฑ์	1	2	3	4	5
โอกาสที่จะเกิด	เป็นไปไม่ได้	ไม่น่าจะเกิดขึ้น	เป็นไปได้	เป็นไปได้มาก	เกิดขึ้นอย่างแน่นอน
L:1 ปริมาณของโอกาสที่จะเกิด	โอกาส < 10%หรือ 1 ครั้งต่อปี	โอกาส 10–20% หรือ 2 ครั้งต่อปี	โอกาส 20–30% หรือ 3-4 ครั้งต่อปี	โอกาส 30–40% หรือ 5-12 ครั้งต่อปี	โอกาส > 40% หรือ 12 ครั้งขึ้นไปต่อปี
L:2 ประวัติการเกิดเหตุการณ์	ไม่เคยเกิดขึ้นมาก่อนในกลุ่มธุรกิจโรงแรม / อาหาร	เคยเกิดขึ้นมาก่อนในกลุ่มธุรกิจโรงแรม / อาหาร แต่ไม่เคยเกิดขึ้นมาก่อนในบริษัท	เคยเกิดขึ้น 1-3 ครั้ง ในบริษัท	เคยเกิดขึ้นบ่อยครั้งในบริษัท 3-5 ครั้ง	เคยเกิดขึ้นบ่อยครั้งมากๆในบริษัท >5 ครั้ง
L:3 สถานะของเหตุการณ์ที่เกิดขึ้นจริง	สาเหตุที่แท้จริงของเหตุการณ์ได้รับการแก้ไขแล้ว และได้จัดให้มีมาตรการเชิงป้องกันเพื่อลดโอกาสที่จะเกิดซ้ำ	สาเหตุที่แท้จริงของเหตุการณ์อยู่ระหว่างการแก้ไขและจัดทำมาตรการเชิงป้องกัน	เหตุการณ์ที่เกิดสามารถจัดการแก้ไขได้แล้ว/เฝ้าติดตามอย่างใกล้ชิด	เหตุการณ์ที่เกิดขึ้นอยู่ระหว่างการจัดการแก้ไข	เหตุการณ์ที่เกิดขึ้นได้ถูกรายงาน และปัจจุบันอยู่ระหว่างการตรวจสอบจากหน่วยงานที่กำกับดูแลทั้งภายในหรือภายนอก

➢ เกณฑ์การประเมินความเสี่ยงด้านผลกระทบ (Impact Assessment Criteria)

เกณฑ์การประเมินความเสี่ยงด้านผลกระทบ เป็นเกณฑ์ที่กำหนดขึ้นเพื่อใช้สำหรับพิจารณา ระดับความเสียหายหรือความรุนแรงที่อาจจะเกิดขึ้น เมื่อความเสี่ยงที่ระบุไว้เกิดขึ้นจริง โดยการประเมินผลกระทบของความเสี่ยง สามารถประเมินเป็นมูลค่าความเสียหาย (ด้านการเงิน) เพื่อเปรียบเทียบกับเกณฑ์ที่กำหนดว่าระดับผลกระทบที่จะเกิดขึ้นต่อองค์กรในภาพรวมอยู่ในระดับใด กรณีที่การประเมินผลกระทบของความเสี่ยงไม่สามารถ ประเมินเป็นมูลค่าความเสียหายได้ ผู้ประเมินสามารถพิจารณาเกณฑ์การประเมินผลกระทบในด้านอื่นๆ กำหนดไว้ 5 ระดับ ดังนี้

สถานะ		ความหมาย
I1	สถานะสีน้ำเงิน	ผลกระทบน้อยมาก
I2	สถานะสีเขียว	ผลกระทบน้อย
I3	สถานะสีเหลือง	ผลกระทบปานกลาง
I4	สถานะสีส้ม	ผลกระทบสูง
I5	สถานะสีแดง	ผลกระทบสูงมาก

การจัดระดับความเสี่ยง

ในการประเมินความเสี่ยงจะต้องมีการกำหนดแผนภูมิความเสี่ยง (Risk Matrix) ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบที่เกิดขึ้น (Impact) และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้ (Risk Appetite Boundary)

ระดับความเสี่ยง = (โอกาสในการเกิดเหตุการณ์ต่าง ๆ) X (ผลกระทบของเหตุการณ์ต่าง ๆ)

ตารางจัดระดับความเสี่ยง

โอกาสที่จะเกิด	ผลกระทบ				
	1	2	3	4	5
5	(5)	(10)	(15)	(20)	(25)
4	(4)	(8)	(12)	(16)	(20)
3	(3)	(6)	(9)	(12)	(15)
2	(2)	(4)	(6)	(8)	(10)
1	(1)	(2)	(3)	(4)	(5)

ระดับความเสี่ยงที่ยอมรับได้

ระดับความเสี่ยงแบ่งเป็น 5 ระดับ สามารถแสดงเป็น Risk Profile มีเกณฑ์การจัดแบ่งดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
20-25 คะแนน	สูงมาก (Extreme)	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที เพื่อให้ความเสี่ยงลดลงมาอยู่ในระดับความเสี่ยงที่ยอมรับได้
10-16 คะแนน	สูง (High)	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ โดยต้องกำหนดมาตรการควบคุมเพิ่มเติม และติดตามอย่างใกล้ชิด เพื่อให้ความเสี่ยงลดลงมาอยู่ในระดับความเสี่ยงที่ยอมรับได้
6-9 คะแนน	ปานกลาง (Medium)	ระดับความเสี่ยงทีพอยอมรับได้ แต่ต้องมีมาตรการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่สูงขึ้น โดยกำหนดผู้รับผิดชอบและกรอบระยะเวลาที่ชัดเจน
4-5 คะแนน	ต่ำ (Low)	ระดับความเสี่ยงที่ยอมรับได้ มีผลกระทบต่อองค์กรเล็กน้อย โดยไม่ต้องมีมาตรการจัดการเพิ่มเติม และไม่ต้องมีกระบวนการควบคุมเพิ่มเติม
1-3 คะแนน	ไม่มีนัยสำคัญ (Insignificant)	ระดับความเสี่ยงที่ยอมรับได้ ไม่มีผลกระทบต่อองค์กรที่เป็นสาระสำคัญ โดยไม่ต้องมีมาตการจัดการเพิ่มเติม แม้จะไม่มีกระบวนการควบคุม

หลังจากได้รับผลการประเมินแล้ว หน่วยงานบริหารความเสี่ยง และฝ่ายบริหารจะดำเนินการ ดังนี้

- **วิเคราะห์และสรุปผลการประเมิน** โดยใช้ Risk Profile ข้างต้น และจัดลำดับความสำคัญของประเด็นความเสี่ยง
- **นำเสนอผลการประเมินต่อที่ประชุมคณะผู้บริหาร** เพื่อดำเนินการคัดเลือกประเด็นความเสี่ยงสำคัญที่ต้องจัดการดูแลรวมถึงการกำหนดฝ่ายจัดการที่รับผิดชอบ (Risk Owner) เพื่อดำเนินการจัดหามาตรการจัดการความเสี่ยงเพิ่มเติมจากที่มีอยู่ ณ ปัจจุบัน
- **รายงานคณะกรรมการบริหารความเสี่ยง การกำกับดูแล และความยั่งยืน** นำเสนอประเด็นความเสี่ยงและมาตรการต่างๆ ที่กำหนดให้ต้องจัดการดูแลเพิ่มเติมต่อคณะกรรมการบริหารความเสี่ยง การกำกับดูแล และความยั่งยืน เพื่อทราบ

4.5 การตอบสนองความเสี่ยง (Risk Response)

การตอบสนองความเสี่ยง (Risk Response) เป็นการกำหนดแผนการจัดการเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยผู้บริหารอาจเลือกใช้วิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรืออาจใช้หลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์เพื่อให้ความเสี่ยงอยู่ในระดับที่องค์กรยอมรับได้ (Risk Appetite) โดยมีแนวทางในการจัดการความเสี่ยง ดังนี้

1) **การยอมรับความเสี่ยง (Risk Acceptance)** เป็นการยอมรับความเสี่ยงที่มีอยู่โดยไม่ดำเนินการใดๆ เพิ่มเติม เนื่องจากเป็นความเสี่ยงที่อยู่ในระดับที่บริษัทยอมรับได้อยู่แล้ว สำหรับความเสี่ยงที่ไม่ได้อยู่ต่ำกว่าระดับความเสี่ยงที่ยอมรับได้ แต่ผู้บริหารต้องการยอมรับความเสี่ยง จะต้องขออนุมัติจากคณะกรรมการบริษัท
2) **การลดความเสี่ยง (Risk Reduction)** เป็นการดำเนินงานเพื่อลดความเสี่ยงหรือหาวิธีการควบคุมเพิ่มเติม เพื่อลดโอกาสการเกิดเหตุการณ์ หรือลดความรุนแรงหรือความเสียหายของเหตุการณ์ที่จะเกิดขึ้นในอนาคตให้อยู่ในระดับที่องค์กรยอมรับได้ เช่น การออกแบบการควบคุมภายใน การปรับปรุงแก้ไขกระบวนการดำเนินงาน และการจัดทำแผนฉุกเฉิน (Contingency Plan) เป็นต้น
3) **การแบ่งปันความเสี่ยง (Risk Sharing)** เป็นการดำเนินการเพื่อลดความรุนแรงของความเสี่ยงโดยการโอนหรือแบ่งปันความเสี่ยงบางส่วนไปยังบุคคล หรือหน่วยงานภายนอกองค์กรให้ช่วยแบกรับภาระความเสี่ยงแทน เช่น การจัดจ้างผู้ให้บริการที่มีความเชี่ยวชาญจากภายนอก การซื้อประกันภัย การกระจายการลงทุน เป็นต้น เพื่อให้ความเสี่ยงที่เหลืออยู่ลดลงจนอยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้
4) **การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)** เป็นการหยุด ยกเลิกกิจกรรมที่ก่อให้เกิดความเสี่ยง มักใช้ในกรณีที่ความเสี่ยงมีความรุนแรงสูง ไม่สามารถหาวิธีการตอบสนองความเสี่ยงที่จะลดผลกระทบของความเสี่ยงให้อยู่ในระดับความรุนแรงที่ยอมรับได้
5) **การดำเนินการต่อ (Risk Pursuance)** เป็นการดำเนินการต่อโดยการยอมรับความเสี่ยงที่สูงขึ้นเพื่อให้สามารถบรรลุผลการปฏิบัติงานที่สูงขึ้น วิธีการนี้อาจเกี่ยวข้องกับการใช้กลยุทธ์เพื่อการเติบโตที่ค่อนข้างรุนแรง เมื่อเลือกที่จะรับความเสี่ยง ผู้บริหารต้องเข้าใจถึงลักษณะและ

ขอบเขตของการเปลี่ยนแปลงที่จำเป็นต่างๆ เพื่อให้บรรลุผลการปฏิบัติงานที่ต้องการในขณะที่ต้องระวังไม่ให้มีความเสี่ยงสูงเกินกว่าขอบเขตของช่วงที่ยอมรับได้

ผู้บริหารต้องพิจารณาถึงปัจจัยดังต่อไปนี้ก่อนการกำหนดแนวทางการจัดการความเสี่ยง

1) **กำหนดกลยุทธ์การบริหารความเสี่ยง:** กำหนดกลยุทธ์การจัดการความเสี่ยงขึ้นเพื่อลดผลกระทบและโอกาสเกิดของความเสี่ยง ให้เป็นไปตามระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ของบริษัท
2) **วางแผนการจัดการความเสี่ยง:** พัฒนารายละเอียดของแผนจัดการความเสี่ยง
3) **กำหนดเจ้าของความเสี่ยง:** กำหนดเจ้าของความเสี่ยงเพื่อให้รับผิดชอบในการตัดสินใจและดำเนินการที่เกี่ยวกับแผนจัดการความเสี่ยงนั้นๆ
4) **อนุมัติและรับรองแผนความเสี่ยง:** แผนจัดการความเสี่ยงต้องได้รับการอนุมัติและเห็นชอบจากคณะกรรมการบริหารความเสี่ยง การกำกับดูแล และความยั่งยืน
5) **รับผิดชอบในการดำเนินการ:** เจ้าของความเสี่ยงเป็นผู้รับผิดชอบในการนำแผนไปปฏิบัติ

4.6 กิจกรรมการควบคุม (Control Activity)

กิจกรรมการควบคุม (Control Activity) คือนโยบายและกระบวนการปฏิบัติงานที่ทำให้มั่นใจได้ว่ามีการนำการจัดการความเสี่ยงไปปฏิบัติอย่างเป็นรูปธรรม เพื่อจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และป้องกันไม่ให้เกิดผลกระทบต่อเป้าหมายขององค์กร

กิจกรรมการควบคุมเป็นเครื่องมือในการบริหารจัดการให้องค์กรสามารถบรรลุวัตถุประสงค์ หลังจากการกำหนดการจัดการความเสี่ยงที่เหมาะสม ผู้บริหารจะกำหนดกิจกรรมการควบคุมเพื่อให้มั่นใจได้ว่าการจัดการความเสี่ยงจะดำเนินไปได้อย่างมีประสิทธิภาพและประสิทธิผล โดยแบ่งกิจกรรมการควบคุมออกเป็น 3 ประเภท ดังนี้

กิจกรรมการควบคุม	การดำเนินการ
1. การควบคุมเชิงป้องกัน (Preventive)	เป็นการดำเนินการเพื่อป้องกันไม่ให้เกิดเหตุการณ์ หรือความผิดพลาดขึ้นตั้งแต่แรก เช่น • การแบ่งแยกหน้าที่ • การใช้รหัสผ่านเพื่อจำกัดการเข้าถึงเครือข่ายสารสนเทศ • การฝึกอบรม
2. การควบคุมเชิงค้นหา (Detective)	เป็นการดำเนินการเพื่อค้นหากิจกรรม เหตุการณ์ หรือความผิดพลาดที่ได้เกิดขึ้นแล้ว เพื่อให้มีการดำเนินการแก้ไขอย่างเหมาะสม เช่น • การยืนยันข้อมูล • การกระทบยอดบัญชี • การตรวจนับทรัพย์สินคงคลัง • รายงานความผิดพลาด

กิจกรรมการควบคุม	การดำเนินการ
3. การควบคุมเชิงแก้ไข (Corrective)	เป็นการดำเนินการเพื่อแก้ไขความผิดพลาด หรือความเสียหายที่เกิดและป้องกันไม่ให้เกิดซ้ำอีกในอนาคต • แผนดำเนินธุรกิจอย่างต่อเนื่อง (Business continuity plans) • แผนฟื้นฟูธุรกิจ (Disaster recovery plans)

4.7 สารสนเทศและการสื่อสาร (Information and Communication)

สารสนเทศและการสื่อสาร (Information and Communication) คือ การจัดให้มีการสื่อสารและระบบสารสนเทศความเสี่ยงที่ดี เพื่อให้มั่นใจว่าผู้บริหารและพนักงานทุกคนเข้าใจกระบวนการและบทบาทหน้าที่ความรับผิดชอบของตนเกี่ยวกับการบริหารความเสี่ยง เพื่อให้เกิดการผลักดันการนำแผนบริหารความเสี่ยงไปสู่การปฏิบัติอย่างมีประสิทธิภาพ

4.8 การติดตาม (Monitoring)

การติดตามผล (Monitoring) คือ กระบวนการติดตามเพื่อให้ทราบถึงผลการดำเนินการว่ามีความเหมาะสม และสามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพหรือไม่

การติดตามการบริหารความเสี่ยง ต้องทำเป็นกิจกรรมที่ต่อเนื่องสามารถทำได้ 2 ลักษณะ คือ

1) การติดตามอย่างต่อเนื่อง เป็นการดำเนินการอย่างสม่ำเสมอ เพื่อให้สามารถตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน
2) การติดตามรายครั้ง เป็นการดำเนินการภายหลังจากเกิดเหตุการณ์ ดังนั้นปัญหาที่เกิดขึ้นจะได้รับการแก้ไขอย่างรวดเร็ว

วัตถุประสงค์หลักของการติดตามผล

- เพื่อให้มั่นใจได้ว่ามีการดำเนินการตามแผนจัดการความเสี่ยงที่กำหนดไว้
- เพื่อประเมินประสิทธิผลการจัดการความเสี่ยงและความสอดคล้องกันของกิจกรรมการควบคุม
- เพื่อพิจารณาความเสี่ยงใหม่หรือการเปลี่ยนแปลงของความเสี่ยงเดิมตามสภาวะแวดล้อมของธุรกิจที่เปลี่ยนไป

ความเสี่ยงและกิจกรรมการควบคุมความเสี่ยงมีการเปลี่ยนแปลงตลอดเวลา แผนจัดการความเสี่ยงหรือกิจกรรมการควบคุมที่เคยใช้ได้ดีอาจมีประสิทธิผลน้อยลง หรืออาจมีการละเลยการปฏิบัติกิจกรรมการควบคุมนั้น รวมทั้งอาจเกิดการเปลี่ยนแปลงวัตถุประสงค์หรือกระบวนการต่างๆ ด้วย ภายใต้ความเปลี่ยนแปลงทั้งหลาย ผู้บริหารต้องประเมินกระบวนการบริหารความเสี่ยงอย่างสม่ำเสมอเพื่อให้เกิดความมั่นใจว่าการบริหารความเสี่ยงยังคงมีประสิทธิภาพ

บริษัท จึงควรสนับสนุนให้มีการสื่อสารเชิงรุกอย่างต่อเนื่องเพื่อติดตามประเด็นต่างๆ เช่น ความเปลี่ยนแปลงในระดับความเสี่ยง ความก้าวหน้าของแผนจัดการความเสี่ยง หรือประสิทธิผลของการบริหารความเสี่ยงในองค์กร เป็นต้น โดยผู้บริหารอาจบรรจุการติดตามเป็นหนึ่งประเด็นในการหารือในที่ประชุม

ต่างๆ เช่น การประชุมผู้บริหาร การประชุมคณะทำงาน รายงานรายเดือนสำหรับผู้บริหาร การประชุมคณะกรรมการบริหารความเสี่ยง การกำกับดูแล และความยั่งยืน เป็นต้น การสื่อสารอย่างต่อเนื่องทำให้มีข้อมูลความเสี่ยงที่ตรงตามความต้องการ ง่ายต่อการเลือกใช้ และสามารถใช้เพื่อประกอบการตัดสินใจได้อย่างทันท่วงที ในบางกรณีช่องทางการสื่อสารที่ไม่เป็นทางการอาจมีความเหมาะสมมากกว่า เช่น สำหรับความเสี่ยงที่ต้องจัดการอย่างเร่งด่วน อาจมีการหารือและรายงานความเสี่ยงทางโทรศัพท์เพื่อตัดสินใจและจัดการความเสี่ยงทันที เพื่อไม่ให้เกิดความล่าช้าที่อาจเกิดขึ้นจากการรายงานตามช่องทางที่เป็นทางการ

หลังจากการนำกรอบการบริหารความเสี่ยงไปปฏิบัติ บริษัทควรสอบทาน และปรับปรุงกรอบการบริหารความเสี่ยงให้สอดคล้องกับการเปลี่ยนแปลงของธุรกิจอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าการควบคุมต่างๆ มีประสิทธิผล ทั้งนี้ ปัจจัยที่เกี่ยวข้องกับโอกาสและผลกระทบของความเสี่ยงอาจเปลี่ยนแปลงได้เช่นเดียวกับต้นทุนของการจัดการความเสี่ยง ดังนั้นแล้วผู้บริหารจึงควรทบทวนความเสี่ยงตามกระบวนการทั้ง 8 ขั้นตอนของการบริหารความเสี่ยงอย่างสม่ำเสมอ

กรอบการบริหารความเสี่ยง ฉบับทบทวน ปี 2569 ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 7/2568 ในวันที่ 14 พฤศจิกายน 2568 โดยมีผลบังคับใช้ตั้งแต่ วันที่ 1 มกราคม 2569 เป็นต้นไป

- ลงนาม -

นายนรชิต สิงหเสนี

ประธานกรรมการ

บริษัท โรงแรมเซ็นทรัลพลาซา จำกัด (มหาชน)