



N U S A S I R I

บริษัท อนุศาศิริ จำกัด (มหาชน)

คู่มือการบริหารความเสี่ยง

ประจำปี 2564

ได้รับอนุมัติจากที่ประชุมคณะกรรมการบริหาร ครั้งที่ 11/2564

เมื่อวันที่ 26 ตุลาคม 2564

คำนำ

บริษัท ฤๅศาศิริ จำกัด (มหาชน) ตระหนักถึงความสำคัญในเรื่องการบริหารความเสี่ยง ในระบบการบริหารงานและการปฏิบัติงาน โดยมุ่งหมายให้การบริหารความเสี่ยงเป็นวัฒนธรรมของผู้ปฏิบัติงานทุกคน ซึ่งนอกจากจะช่วยให้องค์กรสามารถบรรลุวัตถุประสงค์หลัก และเป้าหมายที่ตั้งไว้แล้ว ยังเป็นการสนับสนุนให้บริษัทฯ มีการดำเนินงานที่สร้างมูลค่าเพิ่มให้องค์กรอย่างเป็นรูปธรรม ดังนั้นเพื่อให้หน่วยงานต่างๆ ในบริษัทฯ มีแนวทางในการบริหารความเสี่ยงเป็นไปในทิศทางเดียวกัน คณะอนุกรรมการบริหารความเสี่ยง จึงจัดทำคู่มือการบริหารความเสี่ยงของบริษัทฯ ฉบับนี้ขึ้นเพื่อใช้เป็นคู่มือบริหารความเสี่ยงในการปฏิบัติงานสำหรับพนักงานทุกคน อันจะก่อให้เกิดการบรรลุวัตถุประสงค์การบริหารความเสี่ยงทั่วทั้งองค์กร และเกิดประโยชน์สูงสุดแก่บริษัทฯ ต่อไป

ทั้งนี้บริษัทฯ ได้กำหนดกรอบการดำเนินงานและขั้นตอนการบริหารความเสี่ยงที่สอดคล้องกับหลักเกณฑ์ตามมาตรฐานสากล ของ Committee to Sponsoring Organizations of the Treadway Commission (COSO) ERM เพื่อให้การบริหารความเสี่ยงของบริษัทฯ มีการดำเนินงานอย่างเป็นระบบ และเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพ และมีประสิทธิผลทั่วทั้งองค์กร อีกทั้งให้ผู้ที่เกี่ยวข้องมีความเข้าใจหลักการบริหารความเสี่ยงและนำไปประยุกต์ใช้ได้เหมาะสม โดยความเสี่ยงในระดับองค์กรจะมีการบริหารจัดการผ่านคณะกรรมการจัดการคณะต่างๆ ตามขอบเขตและหน้าที่รับผิดชอบอย่างเป็นระบบ ส่วนความเสี่ยงในระดับหน่วยธุรกิจ และระดับสายปฏิบัติการจะอยู่ภายใต้การกำกับดูแลของผู้บริหารที่รับผิดชอบ โดยถือเป็นหน้าที่รับผิดชอบของทุกหน่วยงานในการบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

นายสมพิจิตร ชัยชนะจาร์ักษ์

ประธานอนุกรรมการ

สารบัญ

	หน้า
1. นิยามและหลักทั่วไป	4
2. วัตถุประสงค์ของการบริหารความเสี่ยง	5
3. ขอบเขตการบริหารความเสี่ยง	5
4. ประโยชน์ของการบริหารความเสี่ยง	5
5. ประเภทความเสี่ยง	7
6. การบริหารความเสี่ยงของบริษัทฯ	8
7. บทบาทและความรับผิดชอบ	9
8. การบริหารความเสี่ยงระดับองค์กร	
1. สภาพแวดล้อมภายในองค์กร (Internal Environment)	11
2. การกำหนดวัตถุประสงค์ (Objective Setting)	12
3. การบ่งชี้เหตุการณ์ (Event Identification)	12
4. การประเมินความเสี่ยง (Risk Assessment)	13
5. การตอบสนองความเสี่ยง (Risk Response)	16
6. กิจกรรมการควบคุม (Control Activities)	16
7. ข้อมูลและการติดต่อสื่อสาร (Information and Communication)	17
8. การติดตาม (Monitoring)	17

1. นิยามและหลักทั่วไป

ความหมายของการบริหารความเสี่ยง

- ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบต่อสร้างความเสียหาย ความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบรรลุเป้าหมายและวัตถุประสงค์ทั้งในระดับองค์กร ระดับหน่วยงาน และระดับบุคคล

- ปัจจัยเสี่ยง (Risk Factor) คือ สิ่งที่เป็นต้นเหตุหรือสิ่งที่เป็นแหล่งที่มาของความเสี่ยง และเหตุการณ์ที่จะทำให้ไม่บรรลุวัตถุประสงค์ และเป้าหมายที่กำหนดไว้ โดยในแต่ละปัจจัยจะมีการกำหนดสาเหตุที่แท้จริงของปัจจัยต่างๆ ที่สามารถอธิบายได้ว่าสาเหตุของปัจจัยเสี่ยงดังกล่าว ส่งผลให้เกิดความเสี่ยงใดๆ และสามารถหามาตรการจัดการปัจจัยนั้น ๆ เพื่อลดความเสี่ยงที่จะเกิดขึ้นได้

- การบริหารความเสี่ยง (Risk Management) คือ กระบวนการที่พนักงานทุกระดับในองค์กรมีส่วนร่วมในการกำหนดกลยุทธ์ และแนวทางในการดำเนินการ เพื่อให้สามารถบ่งชี้เหตุการณ์ความเสี่ยง โอกาสที่จะเกิดขึ้น ประเมินและจัดการความเสี่ยง ที่มีผลกระทบต่อองค์กร เพื่อสร้างความสำเร็จให้บรรลุตามวัตถุประสงค์และเป้าหมายด้วยการลดโอกาสและผลกระทบที่ก่อให้เกิดความเสียหายหรือการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

แหล่งที่มาของการเกิดความเสี่ยง เกิดจากปัจจัย 2 ปัจจัย คือ ปัจจัยภายในและปัจจัยภายนอก

1. ปัจจัยภายใน เช่น วัตถุประสงค์ขององค์กร, นโยบายและกลยุทธ์, การดำเนินงาน, กระบวนการทำงาน โครงสร้างองค์กรและระบบการบริหารงาน, การเงิน, วัฒนธรรมองค์กร และเทคโนโลยีสารสนเทศ

2. ปัจจัยภายนอก เช่น นโยบายของรัฐ, สภาวะเศรษฐกิจ, สังคมการเมือง, การดำเนินการของหน่วยงานภายนอกที่เกี่ยวข้อง, การแข่งขัน (คู่แข่งทางการดำเนินธุรกิจ), ผู้ขายหรือผู้ส่งมอบสินค้า/บริการ และภัยธรรมชาติต่างๆ เป็นต้น

- การประเมินความเสี่ยง (Risk Assessment) คือ กระบวนการในการระบุระดับความรุนแรง และการจัดลำดับความสำคัญของปัจจัยเสี่ยง โดยประเมินจากโอกาสที่จะเกิดขึ้น (Likelihood) และผลกระทบ (Impact) ที่จะเกิดขึ้น

โอกาส (Likelihood) หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงขึ้น

ผลกระทบ (Impact) หมายถึง ความรุนแรงของความเสียหาย หรือผลที่เกิดขึ้นตามมาจากผลสืบเนื่องของเหตุการณ์ความเสี่ยง

ระดับความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยงแบ่งเป็น 5 ระดับ คือ สูงมาก สูง ปานกลาง น้อย และน้อยมาก

2. วัตถุประสงค์ของการบริหารความเสี่ยง

1. เพื่อให้มีความรับผิดชอบในการบริหารความเสี่ยงทั่วทั้งองค์กร โดยมีการจัดการอย่างเป็นระบบ และต่อเนื่อง มีมาตรฐานเดียวกัน

2. เพื่อนำการบริหารความเสี่ยงไปใช้ปฏิบัติเป็นส่วนหนึ่งของการดำเนินงานตามปกติ ทั้งด้านกระบวนการวางแผนเชิงกลยุทธ์ การตัดสินใจ และงานประจำวัน โดยนำเทคโนโลยีสารสนเทศมาประยุกต์เพื่อใช้ให้เกิดประโยชน์สูงสุด

3. เพื่อให้รายงานความเสี่ยงที่ประเมินและจัดลำดับความสำคัญ พร้อมทั้งระบุวิธีการจัดการความเสี่ยง และผู้รับผิดชอบ (เจ้าของความเสี่ยง) โดยรายงานนี้ต้องนำเสนอผู้บังคับบัญชาตามลำดับชั้น

4. เพื่อให้บังคับและจัดการความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของบริษัทฯ ได้รับการจัดการอย่างเป็นระบบ เพื่อให้ความเสี่ยงอยู่ในระดับที่บริษัทฯ ยอมรับได้และเป็นการป้องกันไม่ให้เกิดความสูญเสียที่ไม่ได้คาดหวังต่อธุรกิจ ตลอดจนใช้โอกาสที่มีอยู่ให้เป็นประโยชน์ ทั้งนี้เพื่อให้เกิดการสมดุลของการเติบโตทางธุรกิจ ความเสี่ยง และผลตอบแทนของบริษัทฯ

5. เพื่อให้มีการติดตาม ประเมินผลการบริหารความเสี่ยง โดยมีการทบทวนและมีส่วนร่วมในการปรับปรุง และพัฒนาระบบบริหารความเสี่ยงให้มีประสิทธิภาพ และประสิทธิผลอย่างต่อเนื่อง

3. ขอบเขตการบริหารความเสี่ยง

เพื่อให้การดำเนินงานมีความต่อเนื่องและบรรลุตามวัตถุประสงค์ของบริษัทฯ ดังนั้น ทุกหน่วยงานจะต้องมีการบริหารความเสี่ยงโดยให้การบริหารความเสี่ยงเป็นกระบวนการหนึ่งในการปฏิบัติงานประจำวันของพนักงานทุกคน โดยมีจุดมุ่งหมายให้การบริหารความเสี่ยงถูกปลูกฝังเป็นส่วนหนึ่งของวัฒนธรรมองค์กร

4. ประโยชน์ของการบริหารความเสี่ยง

เมื่อบริษัทฯ มีการบริหารความเสี่ยงที่ดีและเหมาะสมแล้ว บริษัทฯ จะได้ประโยชน์โดยตรงจากการบริหารความเสี่ยง ดังนี้

1. ผลการดำเนินงานของบริษัทฯ สามารถเป็นไปตามเป้าหมายและวัตถุประสงค์ของบริษัทฯ ที่ได้ตั้งไว้

2. ส่งเสริมให้เกิดความเจริญเติบโตทางธุรกิจอย่างต่อเนื่องและยั่งยืน เพื่อสร้างมูลค่าเพิ่มให้กับบริษัทฯ และผู้มีส่วนได้ส่วนเสีย

3. ส่งเสริมให้เกิดการกำกับดูแลกิจการที่ดี

4. ส่งเสริมให้พนักงานเกิดความรู้ความเข้าใจ และตระหนักถึงความสำคัญของการบริหารความเสี่ยง ซึ่งจะส่งผลต่อเนื่องให้เกิดความระมัดระวังในการทำงาน และลดโอกาสที่จะทำให้เกิดการสูญเสียจากการดำเนินงาน

5. ในการจัดทำแผนงานโครงการต่างๆ บริษัทฯ สามารถนำผลของการวิเคราะห์ความเสี่ยงที่เกิดขึ้นมาใช้เป็นส่วนหนึ่งเพื่อประกอบการตัดสินใจที่จะทำหรือไม่ทำโครงการใดๆ ที่จะส่งผลกระทบต่อบริษัทฯ ได้

6. ช่วยให้การกำหนดวัตถุประสงค์และกลยุทธ์ต่างๆ ของบริษัทฯ ให้มีความสมบูรณ์และความเป็นไปได้มากขึ้นและสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้

7. ส่งเสริมให้เกิดการเตรียมความพร้อมและแนวทางแก้ไขปัญหาต่างๆ ที่อาจจะเกิดขึ้นและส่งผลกระทบต่อผลการดำเนินงานของบริษัทฯ

นอกจากประโยชน์ทางตรงที่บริษัทฯ จะได้รับแล้วยังมีประโยชน์ด้านอื่นๆ ที่บริษัทฯ จะได้รับจากการบริหารความเสี่ยง ดังนี้

1. มีระบบเทคโนโลยีและสารสนเทศที่ช่วยในการจัดเก็บข้อมูล การคำนวณต่างๆ การรายงานและสอบทานข้อมูลได้อย่างถูกต้องครบถ้วนสมบูรณ์รวดเร็ว
2. ผู้บริหารมีข้อมูลเพื่อใช้ประกอบในการตัดสินใจได้อย่างถูกต้อง และรวดเร็วยิ่งขึ้น
3. มีการจัดสรรทรัพยากรอย่างเหมาะสมโดยคำนึงถึงความคุ้มค่าในการลงทุน
4. เกิดการมีส่วนร่วมของพนักงานในบริษัทฯ และการบูรณาการเข้ากับระบบงานส่วนอื่นๆ ขององค์กรที่จะร่วมกันผลักดันให้องค์กรเกิดผลสำเร็จตามวัตถุประสงค์ที่ตั้งไว้



5. ประเภทความเสี่ยง

การแบ่งประเภทความเสี่ยงได้จัดแบ่งเป็นดังนี้

1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk: S) หมายถึง ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ และการปฏิบัติตามแผนกลยุทธ์อย่างไม่เหมาะสม รวมถึงความไม่สอดคล้องกันระหว่างนโยบาย, เป้าหมาย กลยุทธ์, โครงสร้างองค์กร, ภาวะการแข่งขัน, ทรัพยากรและสภาพแวดล้อม อันส่งผลกระทบต่อวัตถุประสงค์ หรือเป้าหมายองค์กร

2. ความเสี่ยงด้านการดำเนินงาน (Operational Risk: O) หมายถึง ความเสี่ยงที่เกิดจากการปฏิบัติงาน ทุกๆ ขั้นตอน อันเนื่องมาจากขาดการกำกับดูแลที่ดีหรือขาดการควบคุมภายในที่ดี โดยครอบคลุมถึงปัจจัย ที่เกี่ยวข้องกับกระบวนการ / อุปกรณ์ / เทคโนโลยีสารสนเทศ / บุคลากรในการปฏิบัติงานและความปลอดภัย ของทรัพย์สิน

3. ความเสี่ยงด้านการเงิน (Financial Risk: F) หมายถึง ความเสี่ยงเกี่ยวกับสภาพคล่องทางการเงิน การบริหารทางการเงินและงบการเงิน เช่น ความเสี่ยงจากการจัดสรรงบประมาณไม่เหมาะสม ตั้งงบประมาณ ผิดพลาดและใช้งบประมาณเกิน รวมทั้งความเสี่ยงจากความผันผวนของปัจจัยทางการตลาด และความเสี่ยง จากการที่คู่สัญญาไม่ปฏิบัติตามภาระผูกพัน

4. ความเสี่ยงด้านกฎหมายและข้อกำหนดผูกพันองค์กร (Compliance Risk: C) หมายถึง ความเสี่ยง จากการที่หน่วยงานต่างๆ ต้องปฏิบัติตามกฎหมายและข้อกำหนดผูกพันองค์กร เช่น ความเสี่ยงจาก การผิดสัญญาข้อผูกพัน ความเสี่ยงจากการขาดการรายงานตามกฎหมายระเบียบ หรือการไม่ปฏิบัติตามกฎหมาย ระเบียบและข้อบังคับ

5. ความเสี่ยงที่จะเกิดใหม่ (Emerging Risk) หมายถึง ความเสี่ยงที่จะเกิดใหม่ เป็นความสูญเสีย ที่เกิดขึ้นจากความเสี่ยงที่ยังไม่ได้ปรากฏขึ้นในปัจจุบันแต่อาจจะเกิดขึ้นได้ในอนาคต เนื่องจากสภาวะแวดล้อม ที่เปลี่ยนแปลง ความเสี่ยงประเภทนี้เป็นความเสี่ยงที่เกิดขึ้นอย่างช้าๆ ยากที่จะระบุได้ มีความถี่ของการเกิดต่ำ แต่เมื่อเกิดขึ้นแล้วจะส่งผลกระทบอย่างรุนแรง ความเสี่ยงที่จะเกิดใหม่นี้มักจะถูกระบุขึ้นจากการคาดการณ์ บนพื้นฐานของการศึกษาจากหลักฐานที่มีปรากฏอยู่ ความเสี่ยงที่จะเกิดใหม่นี้มักจะเป็นผลมาจาก การเปลี่ยนแปลงทางการเมือง, กฎหมาย, สังคม, เทคโนโลยี, สภาพแวดล้อม ทางกายภาพ หรือการเปลี่ยนแปลง ตามธรรมชาติ ในบางครั้งผลกระทบของความเสี่ยงประเภทนี้ อาจจะไม่สามารถระบุได้ในปัจจุบัน ตัวอย่าง เช่น ปัญหาที่เกิดขึ้นจากนาโนเทคโนโลยี หรือการเปลี่ยนแปลงของสภาวะภูมิอากาศ เป็นต้น

6. ความเสี่ยงด้าน IT (IT Risk)

ความเสี่ยงจากการเปลี่ยนแปลงเทคโนโลยีดิจิทัล (Digital Transformation)

ปัจจุบันเทคโนโลยีดิจิทัลได้เข้ามามีบทบาทอย่างมากในการดำเนินชีวิตประจำวัน และการทำธุรกิจ อาทิ การนำเทคโนโลยีดิจิทัลมาใช้ในการให้บริการขนส่ง การทำการตลาดและการจำหน่ายสินค้าออนไลน์ ซึ่งในระยะยาวการเปลี่ยนแปลงดังกล่าว เป็นความเสี่ยงที่อาจส่งผลกระทบต่อรูปแบบการดำเนินธุรกิจ และช่องทางการ จัดจำหน่ายแบบเดิมจนทำให้บริษัทฯ สูญเสียความสามารถในการแข่งขัน รวมทั้งอาจเป็นโอกาสในการสร้าง ธุรกิจใหม่ๆ ที่สร้างมูลค่าเพิ่มให้กับองค์กร

6. การบริหารความเสี่ยงของบริษัท

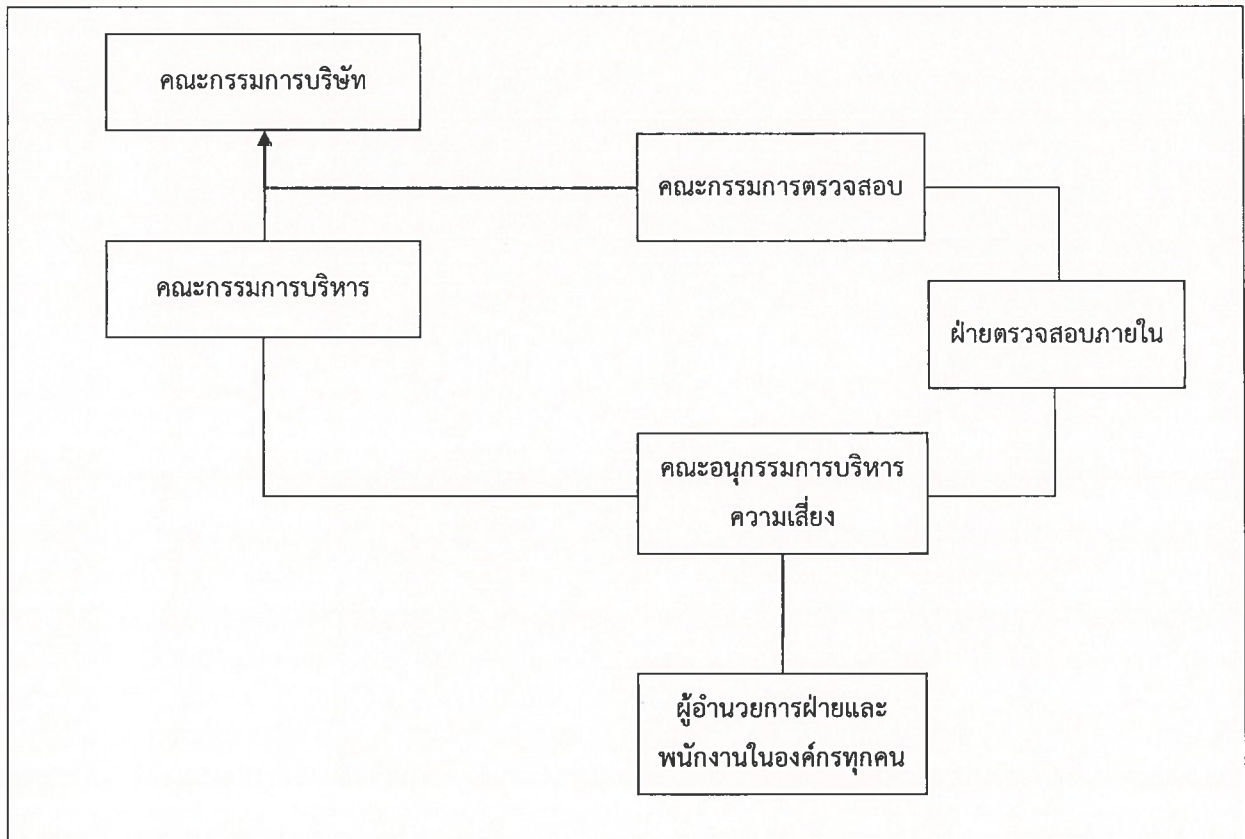
6.1 การบริหารความเสี่ยงของบริษัทในปัจจุบัน

ปัจจุบันบริษัทฯ ได้มีการบริหาร /จัดการความเสี่ยงด้านต่างๆ โดยการใช้เครื่องมือการบริหารหลายรูปแบบ เช่น การกำกับดูแลที่ดี (Good Corporate Governance : GCG) ระบบประเมินผลการทำงาน, ซึ่งในทางปฏิบัติที่ผ่านมา บริษัทฯ สามารถดำเนินการบริหารความเสี่ยงในการดำเนินงานได้ดีอยู่แล้ว อย่างไรก็ตามคณะกรรมการบริษัท ได้ให้ความสำคัญต่อการบริหารความเสี่ยงในองค์กรเป็นอย่างมาก เพื่อให้การบริหารความเสี่ยง เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

6.2 โครงสร้างการบริหารความเสี่ยง

การบริหารความเสี่ยงเป็นองค์ประกอบของทุกกระบวนการดำเนินงานกิจการ ตลอดจนมีความเชื่อมโยงกับทุกระดับ ดังนั้นโครงสร้างการบริหารความเสี่ยงจึงต้องมีความเชื่อมโยงกัน โดยมีคณะกรรมการบริษัทเป็นผู้กำหนดนโยบายหลักต้นและติดตาม ในขณะที่หน่วยปฏิบัติทำหน้าที่ประเมินและบริหารจัดการตามหน้าที่ความรับผิดชอบของแต่ละหน่วยงาน โดยมีโครงสร้างการบริหารดังนี้

โครงสร้างการบริหารความเสี่ยง บริษัท ฤศาศิริ จำกัด (มหาชน)



คณะอนุกรรมการบริหารความเสี่ยง

ณ วันที่ 26 ตุลาคม 2564 คณะอนุกรรมการบริหารความเสี่ยง มีจำนวน 7 ท่าน ดังนี้

- | | |
|------------------------------|--------------------------|
| 1. นายสมพิจิตร ชัยชนะจาร์ภัย | ประธานอนุกรรมการ |
| 2. นายณนทวัชร์ ธนสุวิวัฒน์ | รองประธานอนุกรรมการ |
| 3. นายมนตรี มกรานนท์ | อนุกรรมการ |
| 4. นายจิระ พันธุ์ปลื้มจิตต์ | อนุกรรมการ |
| 5. นายวงศกร เทพเจริญ | อนุกรรมการ |
| 6. นายเศรณี ทองทา | อนุกรรมการ |
| 7. นายกำพล แสงศรีจันทร์ | อนุกรรมการ และเลขานุการฯ |

7. บทบาทและความรับผิดชอบ

การบริหารความเสี่ยงเป็นงานที่ต้องปฏิบัติอย่างต่อเนื่อง และเป็นส่วนหนึ่งของงานประจำวัน บทบาทและความรับผิดชอบของผู้บริหารและพนักงานแต่ละระดับ มีรายละเอียดดังนี้

7.1 คณะกรรมการบริษัท และ/หรือ คณะกรรมการบริหาร

1. อนุมัตินโยบายการบริหารความเสี่ยงและนโยบายต่อต้านการทุจริตคอร์รัปชัน และระดับความเสี่ยงที่บริษัทฯ ยอมรับได้
2. กำกับดูแลการบริหารความเสี่ยงเพื่อให้มั่นใจว่านโยบายการบริหารความเสี่ยงได้รับการนำไปปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง
3. ติดตามความเสี่ยงที่สำคัญของบริษัทฯ เพื่อให้มั่นใจว่าความเสี่ยงได้รับการจัดการให้อยู่ในระดับที่บริษัทฯ ยอมรับได้
4. พิจารณาความเสี่ยงโดยรวมของบริษัทฯ และเปรียบเทียบกับระดับความเสี่ยงที่บริษัทฯ สามารถยอมรับได้
5. รับรายงานจากคณะกรรมการบริหารความเสี่ยงเกี่ยวกับการนำนโยบายการบริหารความเสี่ยงไปปฏิบัติ รวมทั้งข้อเสนอแนะต่างๆ จากคณะกรรมการบริหารความเสี่ยง

7.2 คณะอนุกรรมการบริหารความเสี่ยง ดังนี้

การกำหนดนโยบายและหลักเกณฑ์การบริหารความเสี่ยง

กำหนดนโยบาย วัตถุประสงค์ ขอบเขต ความรับผิดชอบ หลักเกณฑ์ และแนวทางบริหารความเสี่ยงให้สอดคล้องกับกลยุทธ์ เป้าหมาย แผนงาน และทิศทางการดำเนินธุรกิจ ซึ่งบริษัทฯ จะมีการทบทวนเป็นประจำทุกปี และจะดำเนินการจัดทำพร้อมกับแผนธุรกิจเพื่อให้มีความสอดคล้องกัน

การระบุความเสี่ยง

เพื่อระบุความเสี่ยงที่อาจมีผลกระทบต่อการบรรลุวัตถุประสงค์และเป้าหมายของบริษัทฯ โดยพิจารณาจากความเสี่ยงที่เกิดจากปัจจัยภายในและปัจจัยภายนอก เช่น สภาพแวดล้อม กฎหมาย การเงิน ระบบ

สารสนเทศ ระบบข้อมูล เพื่อการตัดสินใจ ความพึงพอใจของนักลงทุน การบริหารเงินลงทุน ทรัพยากรบุคคล ชื่อเสียงและภาพลักษณ์ ระบบรักษาความปลอดภัย เป็นต้น ซึ่งบริษัทฯ จะบริหารความเสี่ยงโดยพิจารณา จัดลำดับความเสี่ยง ซึ่งถ้าอยู่ในเกณฑ์สูงหรือสูงมาก บริษัทฯ จะนำความเสี่ยงเหล่านั้นมาวิเคราะห์ เพื่อดำเนินการจัดการทันที

การวิเคราะห์ความเสี่ยง

เพื่อประเมินระดับความเสี่ยงที่เหลืออยู่หลังจากได้ประเมินระบบการควบคุมที่มีอยู่ และการจัดลำดับ ความสำคัญของความเสี่ยง ซึ่งหากความเสี่ยงที่เหลือยังคงอยู่ในระดับสูงหรือสูงมาก จะต้องกำหนดมาตรการ การจัดการความเสี่ยงทันทีโดยผู้บริหารระดับสูงที่รับผิดชอบ และหากความเสี่ยงที่เหลืออยู่ในระดับปานกลาง หรือระดับต่ำ ให้กำหนดมาตรการจัดการในระดับฝ่ายหรือแก้ไขในกระบวนการปฏิบัติงาน

การจัดการความเสี่ยง

เพื่อกำหนดวิธีการจัดทำแผนในการจัดการความเสี่ยงที่มีความสำคัญ ตามที่ได้มีการจัดลำดับไว้ใน ขั้นตอนของการวิเคราะห์ความเสี่ยง ซึ่งการจัดการความเสี่ยงมีวิธีดังนี้ การลดความเสี่ยง การโอนความเสี่ยง การหลีกเลี่ยงความเสี่ยง การยอมรับความเสี่ยง

การติดตามผลและการสอบทาน

เพื่อติดตามผลการบริหารความเสี่ยงตามแผนที่กำหนดไว้ รวมทั้งประเมินผลการจัดการความเสี่ยง ซึ่งคณะกรรมการบริหารความเสี่ยง จะติดตามและรายงานให้ผู้บริหารระดับสูง และคณะกรรมการตรวจสอบ

7.3 คณะกรรมการตรวจสอบ ดังนี้

1. ดำเนินการเพื่อให้มั่นใจได้ว่ามีระบบการควบคุมภายในที่เหมาะสมเพื่อจัดการกับความเสียหายทั่วไป และความเสี่ยงอันเกิดจากการทุจริตคอร์รัปชันของบริษัทฯ
2. ดำเนินการสอบทานที่เป็นอิสระเพื่อให้มั่นใจว่าการบริหารความเสี่ยงทั่วไป และความเสี่ยง อันเกิดจากการทุจริตคอร์รัปชันมีการปฏิบัติอย่างมีประสิทธิภาพ มีการปรับปรุงแก้ไขให้เหมาะสมอยู่เสมอ
3. ประสานงานกับคณะกรรมการบริหารความเสี่ยง เพื่อรับทราบข้อมูลเกี่ยวกับความเสี่ยงทั่วไป และความเสี่ยงอันเกิดจากการทุจริตคอร์รัปชัน และการควบคุมภายในที่มีผลกระทบหรืออาจมีผลกระทบต่อ บริษัทฯ และมอบหมายให้หน่วยงานตรวจสอบภายในวางแผนและตรวจสอบความเสี่ยงดังกล่าว
4. ชี้แจงประสิทธิภาพของการควบคุมภายในและการบริหารความเสี่ยงที่สำคัญให้คณะกรรมการ บริษัทพิจารณา

7.4 ฝ่ายตรวจสอบภายใน ดังนี้

1. ให้การสนับสนุนคณะกรรมการบริษัท คณะกรรมการตรวจสอบ และผู้บริหารระดับสูง ในการปฏิบัติหน้าที่สอบทานกระบวนการบริหารความเสี่ยงทั่วไป และความเสี่ยงอันเกิดจากการทุจริตคอร์รัปชัน และการควบคุมภายใน และให้ข้อเสนอแนะเพื่อปรับปรุงกระบวนการบริหารความเสี่ยงให้มีความเพียงพอ และมีประสิทธิภาพ
2. ดำเนินการสอบทานเพื่อให้มั่นใจได้ว่าการควบคุมภายในได้ปฏิบัติอย่างเหมาะสม เพื่อจัดการ ความเสี่ยงของบริษัทฯ

3. นำข้อมูลความเสี่ยงทั่วไป และความเสี่ยงอันเกิดจากการทุจริตคอร์รัปชัน จากกระบวนการบริหารความเสี่ยงรวมทั้งการบ่งชี้ประเด็นที่คณะกรรมการ และผู้บริหารระดับสูง ให้ความสำคัญไปใช้วางแผนงานการตรวจสอบตามความเสี่ยง

4. ประสานงานร่วมกับคณะทำงานบริหารความเสี่ยงเพื่อการแลกเปลี่ยนความรู้ และข้อมูลความเสี่ยงที่มีผลกระทบหรืออาจมีผลกระทบต่อบริษัทฯ

7.5. พนักงานทุกคน ดังนี้

1. ดำเนินการเพื่อให้มั่นใจว่าความเสี่ยงได้รับการบ่งชี้และจัดการ เป็นส่วนหนึ่งของการปฏิบัติงานประจำวัน
2. ติดตามการจัดการความเสี่ยงเกี่ยวข้องกับงานตนอย่างสม่ำเสมอ
3. รายงานความเสี่ยงที่สำคัญและปัญหาที่เกิดขึ้นในการบริหารความเสี่ยงให้ผู้บังคับบัญชาทราบตามลำดับ

8. การบริหารความเสี่ยงระดับองค์กร

การบริหารความเสี่ยงองค์กร (Enterprise Risk Management) คือ กระบวนการที่ปฏิบัติโดยคณะกรรมการ ผู้บริหารและบุคลากรทุกคนในองค์กร เพื่อช่วยในการกำหนดกลยุทธ์และดำเนินงาน โดยกระบวนการบริหารความเสี่ยงได้รับการออกแบบเพื่อให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อองค์กร และสามารถจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับ เพื่อให้ได้รับความมั่นใจอย่างสมเหตุสมผล ในการบรรลุวัตถุประสงค์ที่องค์กรกำหนดไว้

การบริหารความเสี่ยง โดยยึดหลักการบริหารความเสี่ยงตามแนวทางของ The Committee of Sponsoring Organizations of the Treadway Commission - Enterprise risk management (COSO-ERM) ซึ่งการบริหารความเสี่ยงตามแนวทางนี้ประกอบด้วยองค์ประกอบ 8 ประการซึ่งสัมพันธ์กับการดำเนินธุรกิจและกระบวนการบริหารงาน ดังนี้

1. สภาพแวดล้อมภายในองค์กร (Internal Environment)

เป็นพื้นฐานที่สำคัญสำหรับกรอบการบริหารความเสี่ยง สภาพแวดล้อมนี้มีอิทธิพลต่อการกำหนดกลยุทธ์และเป้าหมายขององค์กร การกำหนดกิจกรรม การบ่งชี้ประเมิน และการจัดการความเสี่ยง สภาพแวดล้อมภายในองค์กรประกอบด้วยหลายปัจจัยเช่น จริยธรรม วิธีการทำงานของผู้บริหารและบุคลากร รวมถึงปรัชญา และวัฒนธรรมในการบริหารความเสี่ยง

ความเสี่ยงที่ยอมรับได้ (Risk Appetite) เป็นส่วนที่สำคัญอย่างหนึ่งของสภาพแวดล้อมภายในองค์กร และมีผลต่อการกำหนดกลยุทธ์เพื่อนำไปดำเนินการให้องค์กรบรรลุเป้าหมายทั้งด้านผลตอบแทน และการเติบโต กลยุทธ์แต่ละแบบนั้นมีความเสี่ยงที่เกี่ยวข้องแตกต่างกัน

2. การกำหนดวัตถุประสงค์ (Objective Setting)

การกำหนดวัตถุประสงค์ที่ชัดเจนคือ ขั้นตอนแรกสำหรับกระบวนการบริหารความเสี่ยงองค์กรควรมั่นใจว่าวัตถุประสงค์ที่กำหนดขึ้นมีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์ และความเสี่ยงที่องค์กรยอมรับได้ โดยทั่วไปวัตถุประสงค์และกลยุทธ์ควรได้รับการบันทึกเป็นลายลักษณ์อักษร และสามารถพิจารณาได้ในด้านต่างๆ ดังนี้

- 2.1 ด้านกลยุทธ์ เกี่ยวข้องกับเป้าหมายและพันธกิจในภาพรวมขององค์กร
- 2.2 ด้านปฏิบัติงาน เกี่ยวข้องกับประสิทธิภาพผลการปฏิบัติงานและความสามารถในการทำกำไร
- 2.3 ด้านการรายงาน เกี่ยวข้องกับการรายงานทั้งภายในและภายนอกองค์กร
- 2.4 ด้านการปฏิบัติตามกฎระเบียบ เกี่ยวข้องกับการปฏิบัติตามกฎหมาย และกฎระเบียบต่างๆ

การกำหนดวัตถุประสงค์ จะกำหนดเป็น 2 ระดับ คือ

- วัตถุประสงค์ระดับองค์กร เป็นวัตถุประสงค์หรือเป้าหมายการดำเนินงานขององค์กร รวมทั้งมีผลกระทบต่อเป้าหมายการดำเนินงาน

- วัตถุประสงค์ระดับฝ่ายงาน และกระบวนการหลัก เป็นวัตถุประสงค์ของแต่ละขั้นตอนการดำเนินงานหลักที่จะตอบสนองให้การดำเนินงานบรรลุผลสำเร็จตามวัตถุประสงค์ระดับองค์กร

วัตถุประสงค์ต้องมีความสอดคล้องทั่วทั้งบริษัทฯ เพื่อให้เกิดความมั่นใจว่า หน่วยงาน ผู้บริหาร และพนักงานกำลังดำเนินการเพื่อให้บรรลุวัตถุประสงค์ของบริษัทฯ โดยมีการลดกิจกรรม กระบวนการ และหน่วยงานต่างๆ ที่ไม่จำเป็นออกไป วัตถุประสงค์ต้องมีความชัดเจนและเป็นไปได้ตามหลักการที่เรียกว่า SMART ซึ่งระบุว่าวัตถุประสงค์ที่ดีต้องมีลักษณะดังนี้

1. ชัดเจน (Specific) วัตถุประสงค์ควรระบุผลตอบแทนหรือผลลัพธ์ที่ต้องการอย่างชัดเจน เพื่อให้ทุกคนสามารถเข้าใจได้


2. สามารถวัดผลได้ (Measurable) วัตถุประสงค์ต้องสามารถวัดผล และระบุหลักเกณฑ์ของการวัดผลนั้นได้ หากวัตถุประสงค์ไม่สามารถวัดผลได้ บริษัทฯ ควรพิจารณากิจกรรมที่เกี่ยวข้องกับวัตถุประสงค์ และขนาดของการลงทุนในกิจกรรมนั้นๆ แทน

3. สามารถบรรลุได้ (Achievable) วัตถุประสงค์หรือความคาดหวังต้องมีความเป็นไปได้ตามสภาพเหตุการณ์ในปัจจุบัน ระยะเวลา ทรัพยากรที่ถูกจัดสรร

4. มีความเกี่ยวข้องสอดคล้องกัน (Relevant) ผลตอบแทนหรือผลลัพธ์ของวัตถุประสงค์ต้องสอดคล้องกับวัตถุประสงค์ของส่วนอื่นๆ ในบริษัทฯ

5. มีการกำหนดระยะเวลา (Time bound) ต้องมีการระบุเวลาที่ชัดเจนว่าต้องการจะบรรลุวัตถุประสงค์เมื่อไร

3. การบ่งชี้เหตุการณ์ (Event Identification)

การทำธุรกิจมักมีความไม่แน่นอนเกิดขึ้นตามมา องค์กรไม่สามารถมั่นใจได้ว่าเหตุการณ์ใดเหตุการณ์หนึ่งจะเกิดขึ้นหรือไม่ หรือผลลัพธ์ที่เกิดขึ้นจะเป็นอย่างไร ในกระบวนการบ่งชี้เหตุการณ์ ผู้บริหารควรต้องพิจารณาสิ่งต่อไปนี้ 

3.1 ปัจจัยความเสี่ยงทุกด้านที่อาจเกิดขึ้น เช่น ความเสี่ยงด้านกลยุทธ์ การเงิน บุคลากร การปฏิบัติงาน กฎหมาย ภาษีอากร ระบบงานและสิ่งแวดล้อม

3.2 แหล่งความเสี่ยงทั้งจากภายในและภายนอกองค์กร

3.3 ความสัมพันธ์ระหว่างเหตุการณ์ที่เกิดขึ้น

การระบุความเสี่ยง (Risk Identification) เป็นการระบุเหตุการณ์ใดๆ ที่มีโอกาสจะเกิดขึ้นในอนาคต และมีผลกระทบก่อให้เกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ ทำให้การดำเนินงานของหน่วยงานไม่ประสบความสำเร็จตามเป้าประสงค์ที่ตั้งไว้ เหตุการณ์ที่มีผลกระทบในเชิงลบเป็นความเสี่ยงที่ต้องนำไปจัดการต่อไป และเหตุการณ์ที่มีผลกระทบในเชิงบวกจะต้องนำกลับไปกำหนดเป็นเป้าหมายหรือวัตถุประสงค์ของบริษัท เพื่อให้เกิดการนำไปปฏิบัติและสร้างมูลค่าเพิ่มให้กับบริษัทฯ การบ่งชี้เหตุการณ์สามารถจัดทำโดยบุคคลหรือกลุ่มบุคคล เช่น คณะผู้บริหาร และพนักงานที่เกี่ยวข้อง โดยใช้เทคนิคและเครื่องมือหลากหลายชนิด

4. การประเมินความเสี่ยง (Risk Assessment)

ขั้นตอนนี้นับเป็นการประเมินโอกาสเกิดและผลกระทบของเหตุการณ์ที่อาจเกิดขึ้นต่อวัตถุประสงค์ ขณะที่เกิดเหตุการณ์ใดเหตุการณ์หนึ่งอาจส่งผลกระทบในระดับต่ำ เหตุการณ์ที่เกิดขึ้นอย่างต่อเนื่องอาจมีผลกระทบในระดับสูงต่อวัตถุประสงค์ โดยทั่วไปการประเมินความเสี่ยงประกอบด้วย 2 มิติ ดังนี้

- โอกาสที่อาจเกิดขึ้น (Likelihood) เหตุการณ์มีโอกาสดังกล่าวเกิดขึ้นมาก น้อยเพียงใด

การประเมินโอกาสเกิดของความเสี่ยงเป็นเรื่องท้าทาย โดยทั่วไป การหาข้อมูลมาทำการสนับสนุน การประมาณการที่ถูกต้องเป็นไปได้ยาก การประเมินโอกาสที่จะเกิดเชิงคุณภาพ (Qualitative Assessment) ต้องอาศัยการวิเคราะห์ที่มีหลักการและต้องระมัดระวัง ในกรณีที่สามารถหาข้อมูลที่เกี่ยวข้องกับเหตุการณ์ ความล้มเหลวหรือความถี่ที่เกิดขึ้นในอดีตสามารถบ่งชี้ถึงความเป็นไปได้ของเหตุการณ์ในอนาคตได้ อีกทั้งยังสามารถใช้เพื่อการประมาณการทางคณิตศาสตร์ที่แม่นยำมากขึ้น แต่ในบางกรณี ความถี่ที่เกิดขึ้นในอดีตอาจมิได้เป็นตัวชี้้นำถึงความเป็นไปได้ในอนาคต ในกรณีดังกล่าว ผู้ประเมินจำเป็นต้องใช้วิจารณญาณในการเลือกใช้สถิติหรือความเป็นไปได้ในอนาคต เพื่อเป็นข้อมูลประกอบการประเมิน ในการประเมินโอกาสเกิด รายละเอียดความเสี่ยงที่ไม่ชัดเจน อาจก่อให้เกิดความผิดพลาดในการประเมิน ดังนั้นผู้ประเมินจึงควรพิจารณาและปรับปรุงรายละเอียดของความเสี่ยงให้ชัดเจน

- ผลกระทบ (Impact) หากมีเหตุการณ์เกิดขึ้นองค์กรจะได้รับผลกระทบมากน้อยเพียงใด

การประเมินความเสี่ยงควรพิจารณาถึงผลกระทบทั้งทางด้านการเงิน ตัวอย่างเช่น ผลกระทบต่อรายได้ และผลกระทบที่ไม่ใช่ทางการเงิน ตัวอย่างเช่น กฎระเบียบและข้อบังคับ ความพึงพอใจของลูกค้า ชื่อเสียง และบุคลากร เป็นต้น การประเมินมูลค่าของผลกระทบทางการเงินที่เกิดจากความเสียหายหนึ่ง เป็นเรื่องยากและซับซ้อน ดังนั้น ในการประเมินความเสี่ยงเบื้องต้นการพิจารณาผลกระทบที่เกิดจากความเสียหายในเชิงคุณภาพ เพื่อเป็นการประเมินระดับความสำคัญ ความเสี่ยงที่มีผลกระทบไม่มากและมีโอกาสเกิดน้อย ไม่จำเป็นต้องได้รับความสนใจมาก ในขณะที่ความเสี่ยงที่มีผลกระทบมากและมีโอกาสเกิดสูง จำเป็นต้องได้รับการพิจารณาจากผู้บริหารระดับสูงอย่างทันทั่วทั้งที่



ระดับความเสี่ยง (Level of Risk)

คือ ตัวชี้วัดที่ใช้ในการกำหนดความสำคัญของความเสี่ยง โดยค่าระดับความเสี่ยงได้จากการนำโอกาสที่จะเกิดความเสี่ยงเพื่อเป็นหลักเกณฑ์ในการประเมินความเสี่ยง ซึ่งต้องมีการทบทวนอย่างสม่ำเสมอ

แนวทางการพิจารณาความมีนัยสำคัญของความเสี่ยง

การประเมินความมีนัยสำคัญของความเสี่ยง สามารถทำได้โดยการอ้างอิงกับตารางแสดงการจัดลำดับความเสี่ยงข้างต้น การพิจารณาว่าความเสี่ยงใดมีความสำคัญที่ต้องนำมาดำเนินการก่อนหลัง โดยทั่วไปอาจใช้การกำหนดค่าลำดับความเสี่ยงทั้งในด้านของผลกระทบและโอกาสเกิด และแบ่งกลุ่มระดับความสำคัญของความเสี่ยง เช่น บริษัทฯ กำหนดให้ความเสี่ยงที่มีผลกระทบและโอกาสเกิดตั้งแต่ 20 ขึ้นไป คือความเสี่ยงสำคัญที่ต้องนำมาพิจารณาจัดการก่อน เป็นต้น

ทั้งนี้การกำหนดนัยสำคัญของความเสี่ยงของบริษัทฯ ควรได้รับการพิจารณาจากผู้บริหารระดับสูง และผ่านความเห็นชอบจากคณะกรรมการบริหารความเสี่ยง การกำหนดนัยสำคัญของความเสี่ยงของบริษัทฯ สามารถแสดงได้จากภาพข้างล่างนี้ โดย Likelihood แสดงถึงโอกาสของความเสี่ยงที่อาจเกิดขึ้น และ Impact แสดงถึงผลกระทบที่อาจเกิดขึ้น โดยลำดับความสำคัญของความเสี่ยงได้ถูกกำหนดตั้งแต่ระดับ 1-5 ระดับความเสี่ยงที่ได้จากการประเมินข้างต้น หากมีค่าต่ำหมายถึง ความเสี่ยงอยู่ในระดับต่ำมาก และหากมีค่าสูงขึ้น ความเสี่ยงจะมีระดับสูงขึ้น โดยความหมายของแต่ละระดับความเสี่ยง แสดงดังภาพและตาราง

ตารางการประเมินความเสี่ยงขององค์กร (Risk Assessment Matrix)

	โอกาส (Likelihood)					
	ระดับ	ต่ำมาก (1)	ต่ำ (2)	ปานกลาง (3)	สูง (4)	สูงมาก (5)
ผลกระทบ (Impact)	สูงมาก (5)	5	10	15	20	25
	สูง (4)	4	8	12	16	20
	ปานกลาง (3)	3	6	9	12	15
	ต่ำ (2)	2	4	6	8	10
	ต่ำมาก (1)	1	2	3	4	5

การประเมินความเสี่ยง เกิดจากผลคูณของระดับโอกาสในการเกิดความเสี่ยง (Likelihood) และระดับผลกระทบ (Impact) แบ่งออกเป็น 5 ระดับ ดังนี้

สูงมาก	คะแนน 20-25	ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
สูง	คะแนน 10-19	ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องมีการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
ปานกลาง	คะแนน 5-9	ระดับที่ไม่สามารถยอมรับได้ ควรมีการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
ต่ำ	คะแนน 3-4	ระดับที่พอยอมรับได้แต่ต้องมีการควบคุมที่เพียงพอ
ต่ำมาก	คะแนน 1-2	ระดับที่ยอมรับได้ / ความเสี่ยงน้อย

คะแนนที่อยู่ในแต่ละช่อง เกิดจากการพิจารณาระดับความเสี่ยงทั้งโอกาสเกิดและผลกระทบ โดยให้น้ำหนักผลกระทบมากกว่าโอกาสเกิด เช่น การประเมินความเสี่ยงกรณีโอกาสเกิดเป็น 4 ผลกระทบเป็น 5 ค่าความเสี่ยงเท่ากับ 20 แสดงว่าเป็นความเสี่ยงที่สำคัญมาก เป็นต้น

เมื่อได้ระดับความเสี่ยงแล้ว ควรนำความเสี่ยงที่มีระดับรุนแรงมาก สามารถก่อให้เกิดความเสียหายได้มาก มีโอกาสในการเกิดสูง มาเร่งจัดการก่อนข้ออื่นๆ ส่วนความเสี่ยงที่ไม่รุนแรงมีโอกาสเกิดได้น้อย จะจัดเป็นความเสี่ยงที่ไม่ต้องดำเนินการใดๆ ในกรณีมีงบประมาณ กำลังคนหรือเวลาจำกัด การจัดลำดับความเสี่ยง จะช่วยให้สามารถวางแผนและจัดสรรทรัพยากรต่างๆ ได้อย่างถูกต้อง โดยเลือกการวัดความเสี่ยงที่มีความรุนแรงมากและมีโอกาสเกิดขึ้นบ่อยไปหาความเสี่ยงที่ไม่รุนแรงและโอกาสเกิดขึ้นบ่อย

เมื่อได้ระดับโอกาสด้านดีขององค์กรแล้ว ควรนำผลกระทบด้านดีที่มีระดับต่ำ สามารถก่อให้เกิดโอกาสดีทางธุรกิจต่ำ มาเร่งจัดการก่อนข้ออื่นๆ ส่วนผลกระทบด้านดีที่มีระดับสูง สามารถก่อให้เกิดโอกาสดีทางธุรกิจสูงมาก นำมาจัดการในลำดับต่อไป

ดังนั้นความเสี่ยง (Risk) คือ ภัยอันตรายหรือความเป็นไปได้ที่บางสิ่งบางอย่างที่เป็นอันตรายหรือไม่พึงปรารถนาจะเกิดขึ้น โดยทั่วไป ความเสี่ยงกับโอกาส (Opportunity) มักจะถูกมองว่าเป็นของคู่กันและควรจะอยู่ในสภาพที่สมดุลกันให้มากที่สุด โดยคาดหวังว่าผลลัพธ์ที่ได้จะก่อให้เกิดประโยชน์มากกว่าโทษ ดังนั้นวัตถุประสงค์หลักของการบริหารความเสี่ยง จึงเป็นการลดความเสี่ยงที่อาจจะเกิดขึ้นให้เหลือน้อยที่สุด และเพิ่มโอกาสที่อาจจะเกิดขึ้นได้ให้มากที่สุดกับการดำเนินงานขององค์กร

5. การตอบสนองความเสี่ยง (Risk Response)

เป็นการประเมินกิจกรรมการควบคุมที่ควรจะมี หรือที่มีอยู่แล้วว่าสามารถช่วยควบคุมความเสี่ยงหรือปัจจัยเสี่ยงได้อย่างเพียงพอหรือไม่ หรือเกิดประสิทธิผลตามวัตถุประสงค์ของการควบคุมเพียงใด โดยพิจารณาจากต้นทุนและผลประโยชน์ที่เกิดขึ้น การจัดการความเสี่ยง คือกลยุทธ์หรือกิจกรรมที่กำหนดเพื่อจัดการความเสี่ยง โดยลดโอกาสเกิดและผลกระทบของความเสี่ยงให้สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ของบริษัทฯ

ในการพิจารณาการจัดการความเสี่ยงจะต้องคำนึงถึงต้นทุนและผลประโยชน์ที่จะได้รับ โดยใช้กลยุทธ์ใดกลยุทธ์หนึ่งหรือทั้งหมด เช่น

1. การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือ การจัดการความเสี่ยงที่อยู่ในระดับสูงมากและหน่วยงานไม่อาจยอมรับได้ จึงตัดสินใจยกเลิกโครงการ/กิจกรรมนั้น ทั้งนี้หากทำการใช้กลยุทธ์นี้อาจต้องทำการพิจารณาวัตถุประสงค์ว่าสามารถบรรลุได้หรือไม่ เพื่อทำการปรับเปลี่ยนต่อไป

2. การลด/การควบคุมความเสี่ยง (Risk Reduction) คือ การปรับปรุงระบบการทำงานหรือออกแบบวิธีการทำงานใหม่เพื่อลดโอกาสเกิด หรือลดผลกระทบของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

3. การกระจายความเสี่ยง หรือการโอนย้ายความเสี่ยง (Risk Sharing) เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้กับบุคคลหรือบริษัทอื่นช่วยแบ่งความรับผิดชอบไป เพื่อลดโอกาสเกิดและผลกระทบของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

4. การยอมรับความเสี่ยง (Risk Acceptance) ความเสี่ยงที่เหลือในปัจจุบันอยู่ในระดับที่ยอมรับได้ โดยไม่ต้องดำเนินการใดๆ เพื่อลดโอกาสหรือผลกระทบที่อาจเกิดขึ้นอีก มักใช้กับความเสี่ยงที่ต้นทุนของมาตรการจัดการสูงไม่คุ้มกับประโยชน์ที่ได้รับ

6. กิจกรรมการควบคุม (Control Activities)

กิจกรรมการควบคุม คือนโยบายและกระบวนการปฏิบัติงาน เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง เนื่องจากแต่ละองค์กรมีการกำหนดวัตถุประสงค์และเทคนิคการนำไปปฏิบัติเป็นเฉพาะขององค์กร ดังนั้นกิจกรรมการควบคุมจึงมีความแตกต่างกัน การควบคุมเป็นการสะท้อนถึงสภาพแวดล้อมภายในองค์กร ลักษณะธุรกิจ โครงสร้าง และวัฒนธรรมขององค์กร และหากการปฏิบัติงานมีการใช้ระบบเทคโนโลยีสารสนเทศ จำเป็นที่จะต้องมีการพิจารณาถึงการควบคุมทั่วไปในระบบเทคโนโลยีสารสนเทศ และการควบคุมสำหรับแต่ละระบบงานด้วย

ประเภทของกิจกรรมการควบคุม

• การควบคุมแบบป้องกัน (Preventive) การดำเนินการ หรือการควบคุมที่จัดไว้ล่วงหน้าเพื่อลดโอกาสเกิดของผลลัพธ์/ผลกระทบที่ไม่ดี เช่น

- การแบ่งแยกหน้าที่
- การใช้รหัสผ่าน
- การฝึกอบรม

• การควบคุมแบบค้นหาที่ผิด (Detective) การดำเนินการ หรือการควบคุมเพื่อค้นหาสาเหตุเมื่อความผิดพลาดหรือสิ่งผิดปกติได้เกิดขึ้นแล้ว เช่น

- รายงานการสอบทาน
- การยืนยัน
- การนับทรัพย์สิน
- รายงานข้อผิดพลาด

• การควบคุมแบบแก้ไข (Corrective) การดำเนินการหรือการควบคุมเพื่อแก้ไขความเสียหายหรือลดความเสียหายที่เกิดขึ้นจากความผิดพลาด หรือความผิดปกติ เช่น การระงับยodobบัญชี

• การควบคุมแบบส่งเสริม (Directive) การดำเนินการ หรือควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ เช่น การให้รางวัลแก่ผู้มีผลงานดี

7. ข้อมูลและการติดต่อสื่อสาร (Information and Communication)

เป็นสิ่งจำเป็นสำหรับองค์กรในการบ่งชี้ ประเมิน และจัดการความเสี่ยง ข้อมูลสารสนเทศที่เกี่ยวข้องกับบริษัทฯ ทั้งจากแหล่งภายนอกและภายใน ควรได้รับการบันทึกและสื่อสารอย่างเหมาะสมทั้งในด้านรูปแบบและเวลา เพื่อช่วยให้บุคลากรที่เกี่ยวข้องสามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและมีประสิทธิภาพ

การรายงานความเสี่ยง

เป็นการรายงานความมีประสิทธิภาพของกระบวนการบริหารความเสี่ยงที่ได้ดำเนินการทั้งหมดตามลำดับให้ฝ่ายบริหารรับทราบ และให้ความเห็นชอบดำเนินการตามแผนการบริหารความเสี่ยง

ประโยชน์ของรายงานความเสี่ยง มีดังต่อไปนี้

- ทำให้คณะกรรมการบริษัทมั่นใจว่าความเสี่ยงของบริษัทฯ สอดคล้องกับกลยุทธ์ความเสี่ยงที่ได้รับอนุมัติ และพิจารณาได้ว่าหน้าที่การบริหารความเสี่ยงได้รับการปฏิบัติอย่างมีประสิทธิภาพ
- ผู้บริหารระดับสูงสามารถบ่งชี้และเข้าใจความเสี่ยงที่เกิดขึ้น และกำหนดกิจกรรมลดความเสี่ยงที่มีประสิทธิภาพในระดับกลยุทธ์และระดับปฏิบัติการ
- ผู้บริหารของฝ่ายงานต่างๆ สามารถยืนยันได้ว่าการควบคุมที่เกี่ยวข้องเกี่ยวกับความเสี่ยงที่สำคัญได้ถูกนำไปปฏิบัติและดำเนินการอย่างประสบความสำเร็จ และข้อผิดพลาดที่เกิดขึ้นได้รับการรายงานอย่างเหมาะสม

8. การติดตาม (Monitoring)

เป็นกิจกรรมที่ใช้เพื่อติดตาม และปรับปรุงกิจกรรมการจัดการต่อความเสี่ยงต่างๆ เพื่อให้มั่นใจได้ว่าการดำเนินการตามมาตรการจัดการความเสี่ยง โดยทั่วไปแล้วกิจกรรมการติดตามความเสี่ยงเป็นกิจกรรมที่กระทำอยู่เป็นประจำอย่างต่อเนื่อง แต่ในบางกรณีอาจเป็นกิจกรรมเฉพาะก็ได้ วัตถุประสงค์ของการติดตามความเสี่ยงและการจัดการต่อความเสี่ยง ได้แก่

- การให้ความมั่นใจว่าความเสี่ยงเหล่านั้นได้ถูกจัดการตามแผนที่วางไว้
- การประเมินประสิทธิภาพของแผนการและกิจกรรมการบริหารความเสี่ยง
- การพิจารณาถึงความเสี่ยงใหม่เมื่อสถานการณ์เปลี่ยนแปลงไป