Asia Precision Public Company Limited

กรอบการบริหารความเสี่ยง

(ERM Framework)

(นางรัตนา อนุภาสนันท์)
ประธานกรรมการบริหารความเสี่ยง

(นายสมโภชน์ วัลยะเสวี)
ประธานกรรมการ

ฉบับลงวันที่ 27 กุมภาพันธ์ 2569 มีผลบังคับใช้ตั้งแต่วันที่ 27 กุมภาพันธ์ 2569 เป็นต้นไป
อนุมัติโดย คณะกรรมการบริษัท ครั้งที่ 1/2569 เมื่อวันที่ 27 กุมภาพันธ์ 2569

กรอบการบริหารความเสี่ยง

เพื่อให้การบริหารความเสี่ยงเป็นไปตามนโยบายของบริษัท บริษัทจึงได้กำหนดกรอบการบริหารความเสี่ยงขึ้น โดยกรอบการบริหารความเสี่ยงจะเป็นเครื่องมือที่ช่วยทำให้บริษัททราบความเสี่ยงที่อาจจะเกิดขึ้นในแต่ละกระบวนการทำงาน สามารถคาดการณ์ระดับความรุนแรง หรือผลกระทบถ้าเกิดเหตุการณ์นั้น และสามารถหาวิธีการจัดการบริหารความเสี่ยงนั้นให้ลดลงอยู่ในระดับที่บริษัทยอมรับได้ หรือเกิดผลกระทบต่อบริษัทอย่างน้อยที่สุด

ความเสี่ยง (Risks)

คือ โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ หรือการกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน ซึ่งอาจเกิดขึ้นในอนาคตและมีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์ การปฏิบัติงาน การเงินและการบริหารหรือผลกระทบที่มีต่อภาพลักษณ์และชื่อเสียงองค์กร

การบริหารความเสี่ยง (Risk Management)

คือ กระบวนการที่ปฏิบัติโดยคณะกรรมการ ผู้บริหาร และบุคลากรทุกคนในองค์กร เพื่อช่วยในการกำหนดกลยุทธ์และดำเนินงาน โดยกระบวนการบริหารความเสี่ยงได้รับการออกแบบเพื่อให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้น และมีผลกระทบต่อองค์กร และสามารถจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับ เพื่อให้ได้รับความมั่นใจอย่างสมเหตุสมผล ในการบรรลุวัตถุประสงค์ที่องค์กรกำหนดไว้

องค์ประกอบของการบริหารความเสี่ยงองค์กร ERM (Enterprise Risk Management)

บริษัทได้นำแนวคิดการบริหารความเสี่ยงตามหลัก COSO–ERM 2017 มาปรับใช้เรื่องของการบริหารความเสี่ยง เพื่อให้การดำเนินการบริหารความเสี่ยงมีการจัดการอย่างบูรณาการทั่วทั้งองค์กร ซึ่งมีองค์ประกอบ 5 ประการ ดังนี้

ข้อมูลอ้างอิง : Enterprise Risk Management Integrating with Strategy and Performance Executive Summary,2017, p10

1. **ความเป็นธรรมมาภิบาลและวัฒนธรรมองค์กร (Governance and Culture)** เพื่อแสดงให้เห็นว่าบริษัทมีจัดการด้านธรรมมาภิบาล และส่งเสริมการสร้างวัฒนธรรมองค์กร เพื่อเป็นเครื่องมือที่ที่จะทำให้บุคคลากรในบริษัท มีจริยธรรมที่ดี รู้คุณค่าเข้าใจและตระหนักในเรื่องของความเสี่ยง เป็นสังคมการทำงานที่บุคลากรแสดงความรับผิดชอบร่วมกันในการบริหารความเสี่ยงทั่วทั้งองค์กรอย่างเป็นระบบและมีประสิทธิผลขึ้น

2. **การกำหนดวัตถุประสงค์และเป้าหมายเชิงกลยุทธ์ (Strategy and Objective-Setting)** บริษัทจัดให้มีกระบวนการดำเนินงานด้านการบริหารความเสี่ยงควบคู่กับการจัดการด้านกลยุทธ์ โดยเฉพาะหากมีความเข้าใจและมีการระบุ ประเมินและ

การตอบสนองความเสี่ยงเป็นพื้นฐานการกำหนดเป้าหมายเชิงกลยุทธ์แล้ว จะส่งผลให้กระบวนการบริหารความเสี่ยงทั่วทั้งองค์กร และการจัดการกลยุทธ์เกิดประสิทธิภาพ

3. การจัดการความเสี่ยง (Performance) บริษัทเห็นความสำคัญในเรื่องความเสี่ยงที่อาจกระทบต่อความสำเร็จ ดังนั้น ระหว่างการนำแผนแนวทางจัดการความเสี่ยงไปสู่การปฏิบัติ จึงต้องมีการระบุ ประเมิน และการตอบสนองความเสี่ยงควบคู่กันไป เพื่อที่จะได้มีการประเมินลำดับความสำคัญของความเสี่ยง ควรเลือกวิธีการตอบสนอง และวิเคราะห์ความเสี่ยงเป็นรูปแบบรายงาน เสนอให้แก่ผู้มีส่วนได้ส่วนเสียได้ทราบ จะทำให้เกิดประสิทธิผลต่อการจัดการ

4. การทบทวนและปรับปรุง (Review and Revision) บริษัทจัดให้มีการทบทวนและปรับปรุงกระบวนการจัดการกลยุทธ์ อย่างน้อยปีละ 1 ครั้ง เพื่อความเหมาะสมตามสภาวะเศรษฐกิจและสังคม นอกจากนี้หากพิจารณาแล้วเห็นว่าจะผลการดำเนินงาน อาจมีแนวโน้มไม่บรรลุเป้าหมาย หรือสถานการณ์มีการเปลี่ยนแปลงเกิดขึ้นโดยไม่คาดหมาย แล้วมีการนำการจัดการความเสี่ยง มาใช้ ทางบริษัทจะทำการทบทวนผลจากการบริหารความเสี่ยงมาพิจารณาในการตัดสินใจประกอบ เพื่อพิจารณาทบทวน และทำ การปรับปรุงให้สามารถตัดสินใจได้อย่างถูกต้อง ถูกสถานการณ์ ถูกจังหวะเวลาที่เหมาะสม เพื่อการดำเนินงานที่ต่อเนื่องและยั่งยืน

5. ระบบสารสนเทศ การสื่อสาร และการรายงาน (Information, Communication and Reporting) การบริหาร ความเสี่ยงเป็นกระบวนการที่ต้องการความต่อเนื่อง การเข้าถึงข้อมูลทั้งภายในและภายนอก และการถ่ายทอด รายงานข้อมูลเชิง ความเสี่ยงให้ทั่วถึงและเพียงพอในลักษณะจากล่างขึ้นบน และจากบนลงล่างที่ดีพอ จะส่งผลให้การจัดการเชิงกลยุทธ์มีประสิทธิผล และส่งผลต่อการเพิ่มคุณค่าให้แก่บริษัทในที่สุด

กระบวนการของการบริหารความเสี่ยง

บริษัทได้กำหนดกระบวนการของการบริหารความเสี่ยงไว้ ดังนี้

การกำหนดวัตถุประสงค์ (Objective Setting)

เพื่อให้ทราบขอบเขตการดำเนินงานในแต่ละระดับ และสามารถวิเคราะห์ความเสี่ยงที่คาดว่าจะเกิดขึ้นได้อย่างครบถ้วน ดังนั้น การกำหนดวัตถุประสงค์ในการบริหารความเสี่ยงที่ดีเพื่อให้บรรลุเป้าหมาย ควรจัดทำเป็นลายลักษณ์อักษรอย่างชัดเจน มีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่หน่วยงานยอมรับได้ รวมทั้งควรมีการสื่อสารให้แก่ทุกหน่วยงานรับทราบ เพื่อให้มีความเข้าใจที่ชัดเจน ถูกต้องตรงกัน สามารถวัดได้ สามารถปฏิบัติได้ มีเหตุผล และมีกรอบระยะเวลาที่จะดำเนินการได้แล้วเสร็จ ซึ่งเป็นไปตามหลักการ "SMART" ซึ่งย่อมาจาก

Specific	การกำหนดเป้าหมายที่ชัดเจน เฉพาะเจาะจงสอดรับกับ model ธุรกิจหลัก
Measurable	สามารถวัดได้ทั้งเชิงปริมาณ และคุณภาพ
Achievable	สามารถปฏิบัติให้บรรลุผลได้
Realistic	มีความสอดคล้องกับวัตถุประสงค์และเป้าหมายของบริษัท
Timely	มีกรอบเวลาที่ชัดเจนและเหมาะสม

การจัดประเภทความเสี่ยง สามารถแบ่งเป็น 6 ประเภท ดังนี้

1. **ความเสี่ยงด้านกลยุทธ์การดำเนินธุรกิจ** (Strategic Risk: S) หมายถึง ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์และการปฏิบัติตามแผนกลยุทธ์อย่างไม่เหมาะสม รวมถึงความไม่สอดคล้องกันระหว่างนโยบาย เป้าหมาย กลยุทธ์ โครงสร้างองค์กร สภาวการณ์แข่งขัน

2. **ความเสี่ยงด้านการดำเนินงาน** (Operational Risk: O) หมายถึง ความเสี่ยงที่เกิดจากการปฏิบัติงานทุก ๆ ขั้นตอน โดยครอบคลุมถึงปัจจัยที่เกี่ยวข้องกับกระบวนการ อุปกรณ์เทคโนโลยี และบุคลากรในการปฏิบัติงาน

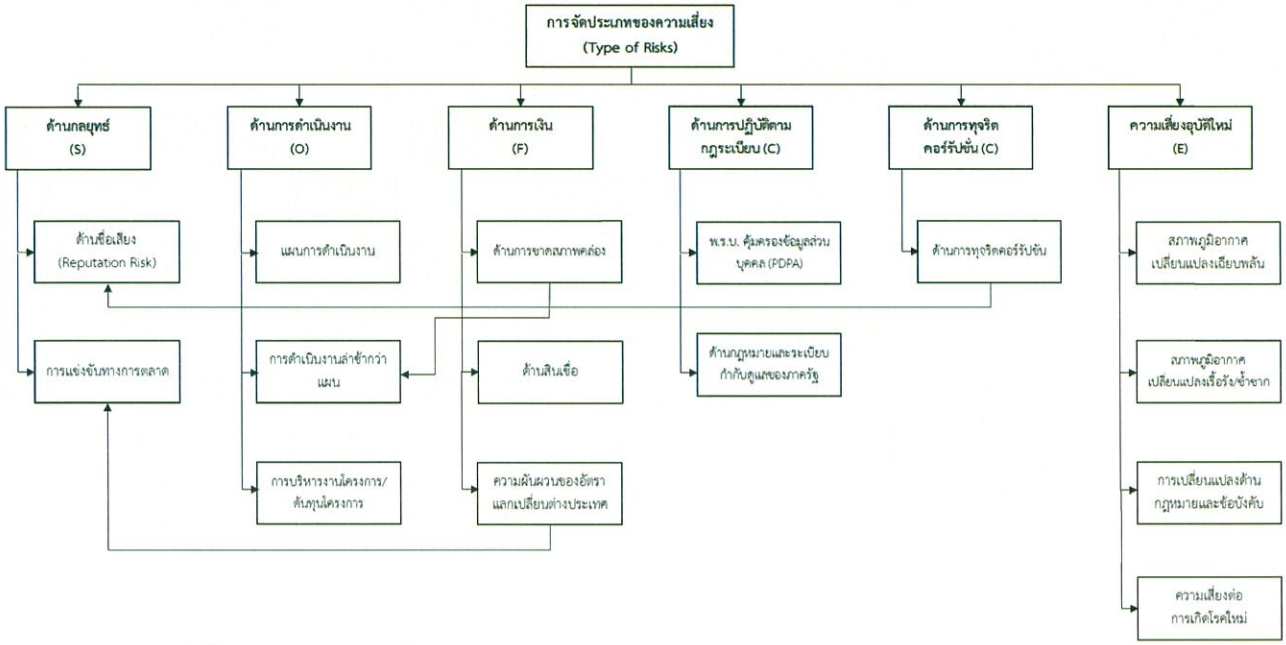
3. **ความเสี่ยงด้านการเงิน** (Financial Risk: F) หมายถึง ความเสี่ยงเกี่ยวกับการจัดทำข้อมูลทางการเงิน และข้อมูลสำคัญต่างๆ ให้มีความถูกต้อง ชัดเจน สร้างความน่าเชื่อถือ รวมไปถึงการรายงานข้อมูลทางการเงินดังกล่าวด้วย ตัวอย่างความเสี่ยง เช่น การรายงานผลประกอบการของบริษัท เป็นต้น

4. **ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ ข้อบังคับ** (Compliance Risk: C) หมายถึง ความเสี่ยงที่เกิดจากการไม่สามารถปฏิบัติตามกฎระเบียบ กฎหมายที่เกี่ยวข้องได้ กฎระเบียบ กฎหมายที่มีอยู่ไม่เหมาะสม หรือเป็นอุปสรรคในการปฏิบัติงาน

5. **ความเสี่ยงด้านการทุจริตคอร์รัปชั่น** (Corruption Risk: C) หมายถึง ความเสี่ยงที่เกิดจากการกระทำโดยเจตนาทั้งการให้ และ/หรือการรับสินบน การขัดแย้งทางผลประโยชน์ การเรียกร้อง ข่มขู่ หรือการกระทำการใดๆ เพื่อให้ได้มาซึ่งผลประโยชน์อันมิชอบด้วยกฎหมายสำหรับองค์กร ตนเอง หรือผู้อื่น

6. **ความเสี่ยงอุบัติใหม่** (Emerging Risk: E) หมายถึง เหตุการณ์หรือปัจจัยที่ไม่เคยเกิดขึ้นมาก่อน หรือเกิดขึ้นแล้วแต่มีลักษณะเปลี่ยนไป ทั้งทางด้านโรคติดต่อ (เช่น โรคโควิด-19, ไวรัสซิกา, ฝีดาษลิง) และภัยทางธุรกิจ/สังคม เช่น ภัยภูมิอากาศ ภัยไซเบอร์ หรือการเปลี่ยนแปลงกฎหมาย ซึ่งมักมีความไม่แน่นอนสูงและอาจส่งผลกระทบรุนแรงอย่างรวดเร็ว

ตัวอย่างการจัดประเภทความเสี่ยง ทั้ง 6 ประเภท ดังนี้



การระบุเหตุการณ์เสี่ยง (Event Identification)

การระบุเหตุการณ์เสี่ยง คือ การระบุเหตุการณ์ที่อาจจะเกิดขึ้นและส่งผลกระทบต่อบริษัท ทั้งด้านที่เป็นโอกาสและความเสี่ยง โดยจะต้องมีความเข้าใจถึงปัจจัยต่าง ๆ ทั้งภายในและภายนอกองค์กร ต้องรวบรวมเหตุการณ์ที่เคยเกิดขึ้นในอดีต และความเสี่ยงที่อาจเกิดขึ้นใหม่ (Emerging Risks)

บริษัทจะจัดกลุ่มผู้เชี่ยวชาญที่มีความรู้และเกี่ยวข้องในความเสี่ยงเรื่องนั้นๆ เข้ามามีส่วนร่วมในการระบุเหตุการณ์ความเสี่ยงด้วย เพื่อให้การวิเคราะห์ความเสี่ยงนั้น สามารถจะระบุปัจจัยเสี่ยงหรือเหตุการณ์ความเสียหายที่เกี่ยวข้องกับกิจกรรมสำคัญ โดยต้องครอบคลุมทั้งความเสี่ยงที่มีอยู่โดยธรรมชาติ (Inherent Risk) และความเสี่ยงที่เหลืออยู่ (Residual Risk)

ขั้นตอนการระบุความเสี่ยง

1. การใช้ประสบการณ์ของผู้ประเมินในการระบุเหตุการณ์ที่เคยเกิดขึ้น (Experience) โดยการวิเคราะห์โอกาสที่จะเกิดความเสี่ยง จากข้อมูลเกี่ยวกับปัญหา หรือข้อผิดพลาดในกระบวนการทำงานที่เคยเกิดขึ้นในอดีตมาใช้เป็นแนวทางและเป็นข้อมูลเบื้องต้นได้

2. การใช้คู่มือปฏิบัติงาน (Work procedure Manual) เพื่อลำดับขั้นตอนของกระบวนการทำงาน และพิจารณาว่าในแต่ละขั้นตอนอาจจะเกิดเหตุการณ์ต่างๆ ซึ่งอาจจะทำให้กิจกรรมนั้นๆ หยุดชะงัก หรือผิดพลาดจนก่อให้เกิดความเสียหายขึ้นได้หรือไม่

3. การระดมความคิด (Brainstorming Group) จากพนักงาน หรือหน่วยงานที่มีส่วนเกี่ยวข้องกับกิจกรรมดังกล่าวทั้งภายในและภายนอกองค์กร เพื่อร่วมกันพิจารณาว่ามีเหตุการณ์ใดบ้างที่เกิดขึ้นแล้วส่งผลกระทบเสียหายต่องานที่ดูแล

4. การใช้แบบสอบถามความคิดเห็น (Questionnaires) ไปยังผู้รับผิดชอบกิจกรรมต่างๆ ว่ามีปัญหา หรือข้อผิดพลาด หรือความเสี่ยงในลักษณะใดบ้าง และก่อให้เกิดความเสียหายอย่างไร ข้อระวังคือ การเก็บ ให้เก็บข้อคิดเห็น แยกความรู้สึกออกมา เพราะหลายครั้งไม่ใช้ข้อเท็จจริงของเหตุการณ์

5. การใช้แบบตรวจสอบรายการ (Checklists) โดยผู้บริหารและพนักงานในหน่วยงานสามารถตรวจสอบขั้นตอนการทำงาน และมาตรฐานการทำงานตาม Checklist ที่ จัดทำได้ด้วยตนเอง และควรกำหนดระยะเวลาในการประเมินผลภายในหน่วยงาน ด้วย Checklists ที่ชัดเจนอย่างสม่ำเสมอ

การระบุความเสี่ยงและเหตุแห่งความเสี่ยง ควรครอบคลุมในเรื่องดังต่อไปนี้

1.) ความเสียหาย หรือเหตุการณ์ที่อาจมีผลกระทบในเชิงลบต่อองค์กร

2.) ความไม่แน่นอนที่อาจมีผลต่อการบรรลุวัตถุประสงค์และกลยุทธ์ขององค์กร

3.) เหตุการณ์ที่อาจทำให้องค์กรสูญเสียโอกาสในการสร้างรายได้ หรือสร้างโอกาสทางธุรกิจหรือการได้รับการยอมรับจากหน่วยงานภายนอก

4.) ความเสี่ยงที่อาจเกิดขึ้นทุกด้าน เช่น ความเสี่ยงด้านกลยุทธ์ การเงิน บุคลากร การดำเนินงาน ชื่อเสียง กฎหมาย ภาษีอากร ระบบงาน และสิ่งแวดล้อม เป็นต้น

5.) ความเสี่ยงที่อาจเกิดขึ้นจากสาเหตุทั้งจากปัจจัยภายในและภายนอกองค์กร

6.) ความเสี่ยงที่อาจเกิดขึ้นใหม่ หรือความเสี่ยงที่ยังไม่ปรากฏชัดเจนในปัจจุบัน แต่มีแนวโน้มว่าจะส่งผลกระทบอย่างมีนัยสำคัญต่อบริษัทฯ

การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยง หมายถึง การวัดระดับความรุนแรงของความเสี่ยงว่ามีมากน้อยเพียงใด โดยนำความเสี่ยงที่ได้จากการระบุเหตุความเสี่ยง มาประเมินความเสี่ยง โดยแนวคิดในการประเมินความเสี่ยงของบริษัท ทำได้ทั้งในเชิงคุณภาพและในเชิงปริมาณ และประเมินได้ตั้งแต่ระดับองค์กรไปจนถึงระดับหน่วยงาน ซึ่งจะต้องประเมินทั้งความเสี่ยงที่มีอยู่ตามธรรมชาติ (Inherent Risk) และความเสี่ยงที่เหลืออยู่หลังการตอบสนองต่อความเสี่ยง (Residual Risk) และบริษัทได้จัดทำแผนที่ความเสี่ยง (Risk map) โดยให้ความสำคัญกับความเสี่ยงต่างๆ ที่มีความสัมพันธ์กัน เนื่องจากเหตุการณ์หนึ่งอาจก่อให้เกิดความเสี่ยงหลายประการ

การประเมินความเสี่ยง (Risk Rating Scale)

เป็นขั้นตอนที่คณะกรรมการบริหารความเสี่ยง หรือคณะทำงานด้านบริหารความเสี่ยง ควรมีการดำเนินการร่วมกันทั้งองค์กร โดยพิจารณาเงื่อนไขในการกำหนดเกณฑ์การประเมินความเสี่ยงใน 2 มิติ คือ

1. โอกาสที่จะเกิดความเสี่ยง (Likelihood) พิจารณาจากหลักการสำคัญ ดังนี้

1) ความถี่ของการเกิดเหตุการณ์ในอดีต (Historical Frequency) ใช้ข้อมูลที่ผ่านมาเพื่อประเมินว่าความเสี่ยงนั้นเคยเกิดขึ้นบ่อยแค่ไหน เช่น ทุกเดือน ปีละครั้ง หรือไม่เคยเกิดขึ้นแต่มีแนวโน้มเกิดขึ้นได้ เป็นต้น

2) ปัจจัยภายนอกที่ควบคุมไม่ได้ (External Factors) โดยอาศัยการใช้เครื่องมือการวิเคราะห์ในการเข้าใจสภาพแวดล้อมที่ควบคุมไม่ได้ที่ส่งผลกระทบต่อบริษัทเกิดจากปัจจัยใด เช่น ปัจจัยด้านเศรษฐกิจ ปัจจัยด้านการเมืองและกฎหมาย ปัจจัยด้านสังคมและพฤติกรรมผู้บริโภค ปัจจัยด้านเทคโนโลยี หรือปัจจัยด้านสิ่งแวดล้อม เป็นต้น

3) ประสิทธิภาพของระบบควบคุม (Effectiveness of Controls) ประเมินประสิทธิภาพของระบบควบคุมภายในที่บริษัทมีว่าเพียงพอหรือไม่ ประสิทธิภาพการควบคุมภายในอยู่ระดับดีมากส่งผลให้โอกาสเกิดน้อย หรือประสิทธิภาพการควบคุมภายในอยู่ในระดับต่ำส่งผลให้โอกาสเกิดขึ้นมาก

4) ความซับซ้อนของกระบวนการทำงาน (Process Complexity) หากกระบวนการที่ซับซ้อน ยุ่งยาก มีหลายขั้นตอน หรืออาศัยบุคลากรจำนวนมาก ส่งผลให้มีโอกาสเกิดความผิดพลาดสูงขึ้น

5) ปัจจัยมนุษย์ (Human Factors) ความผิดพลาดของบุคลากรล้วนส่งผลต่อโอกาสการเกิดความเสี่ยง เช่น การขาดทักษะ การทำงานภายใต้ความกดดัน อัตราการลาออกสูง เป็นต้น

6) ปัจจัยจากระบบเทคโนโลยี (Technology & System Factors) ระบบที่มีปัญหา ซอฟต์แวร์เก่า โครงสร้างพื้นฐานไม่พร้อม เพิ่มโอกาสการหยุดชะงักและความผิดพลาด

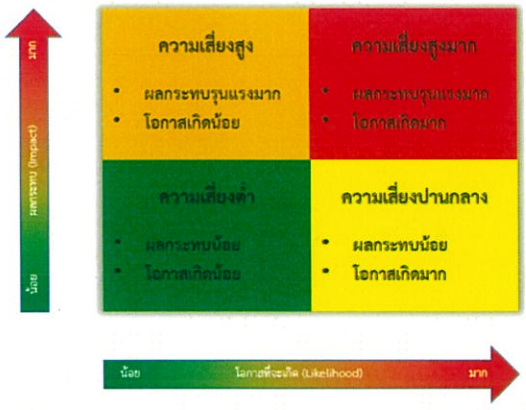
7) ปัจจัยอื่นๆ ที่เพิ่มโอกาสที่จะเกิดความเสี่ยง

2. ระดับความรุนแรงของผลกระทบ (Impact) กำหนดไว้ 4 ระดับ ดังนี้

ระดับ	ผลกระทบ (Impact)
4	ส่งผลกระทบอย่างรุนแรงและมีนัยสำคัญ : กระทบต่อชื่อเสียง / ภาพพจน์ / ความน่าเชื่อถือ / กระทบต่อราคาหุ้น / จำนวนเงิน /ความสามารถในการแข่งขันของบริษัท อย่างมีนัยสำคัญ
3	ส่งผลกระทบในระดับปานกลาง : กระทบต่อชื่อเสียง / ภาพพจน์ / ความน่าเชื่อถือ / กระทบต่อราคาหุ้น / จำนวนเงิน /ความสามารถในการแข่งขันของบริษัท ในระดับปานกลาง
2	ส่งผลกระทบในระดับน้อยมาก / ควบคุมได้ : กระทบต่อชื่อเสียง / ภาพพจน์ / จำนวนเงิน / โดยอาจจะเป็นข่าวที่เป็นที่สนใจของบุคคลทั่วไปน้อย รวมถึงกระทบความสามารถในการแข่งขันในระดับน้อยมาก
1	ไม่ส่งผลกระทบต่อบริษัท : ไม่ส่งผลกระทบต่อต่อชื่อเสียง / ภาพพจน์ / ราคาหุ้น / ความสามารถในการแข่งขันของบริษัท

จากนั้นทำการคำนวณหาค่าของความเสี่ยงที่เกิดขึ้นเพื่อนำมาพิจารณาทบทวนความสำคัญของความเสี่ยงด้านที่เกิดขึ้นตามสูตรการคำนวณดังนี้

- ระดับความเสี่ยง = โอกาสในการเกิดความเสี่ยง (Likelihood) X ระดับความรุนแรงของผลกระทบ (Impact)



การจัดลำดับความเสี่ยง (Risk Ranking)

เกณฑ์การจัดลำดับความสำคัญความเสี่ยงหรือความรุนแรงของความเสี่ยง ต้องพิจารณาดำเนินการ ดังนี้

ความรุนแรงของความเสี่ยง สามารถแบ่งออกเป็น 4 ระดับ ได้แก่

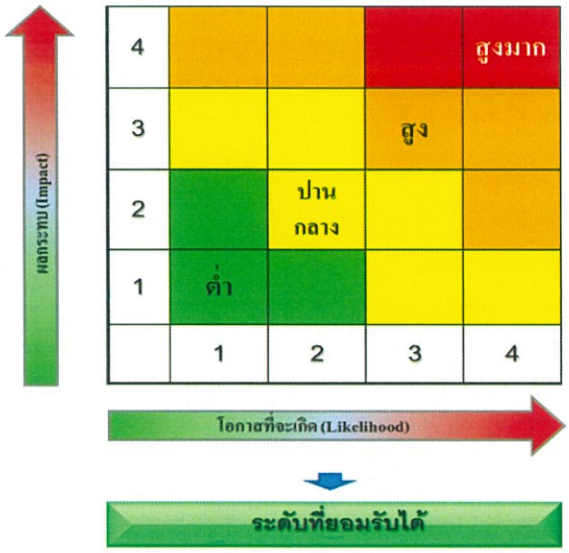
สีแดง	=	ระดับความรุนแรงสูง ต้องดำเนินการโดยทันที
สีเหลืองเข้ม	=	ระดับความรุนแรงค่อนข้างมาก ซึ่งต้องบริหารความเสี่ยงโดยผู้บริหารต้องให้ความสนใจเฝ้าระวัง
สีเหลืองอ่อน	=	ระดับความรุนแรงปานกลาง ซึ่งต้องกำหนดความรับผิดชอบในการบริหารความเสี่ยง
สีเขียว	=	ระดับความรุนแรงต่ำ แต่ต้องติดตามสถานะความเสี่ยงอย่างสม่ำเสมอ

ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)

ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) คือ ระดับความเสี่ยงโดยรวมที่บริษัทสามารถยอมรับได้ ในการดำเนินงานเพื่อให้บรรลุเป้าหมายเชิงกลยุทธ์ของบริษัท โดยพิจารณาจากความสมดุลระหว่างความเสี่ยงที่อาจจะเกิดขึ้นและโอกาสหรือผลตอบแทนที่คาดว่าจะได้รับ

ผู้บริหารจึงต้องกำหนด กลยุทธ์ และ การตัดสินใจด้านธุรกิจ ให้สอดคล้องกับระดับความเสี่ยงที่บริษัทสามารถรับได้จริง เพื่อป้องกันไม่ให้เกิดความเสี่ยงเกินกว่าขีดความสามารถในการจัดการ (Risk Capacity)

"คณะกรรมการบริหารความเสี่ยง กำหนดระดับความเสี่ยงที่ยอมรับได้ไว้ที่ระดับความเสี่ยงปานกลาง และต่ำ"



ระดับความเบี่ยงเบนความเสี่ยง (Risk Tolerance)

ระดับความเบี่ยงเบนความเสี่ยง คือ ระดับความผันผวนหรือความยืดหยุ่นที่บริษัทสามารถยอมรับได้ จากค่ามาตรฐานของระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) โดยมักกำหนดในรูปแบบของ อัตราร้อยละ (+/-) ค่าดัชนี (Index) หรือค่าความเปลี่ยนแปลงตามตัวชี้วัดวัตถุประสงค์ของบริษัท (KPI Variance)

การกำหนด Risk Tolerance ที่ชัดเจนช่วยให้องค์กรมั่นใจว่า การบริหารความเสี่ยงยังอยู่ ภายในกรอบที่ปลอดภัย และไม่ก่อให้เกิด ผลกระทบเชิงลบต่อความเสี่ยงรวมของบริษัทอย่างมีนัยสำคัญ

การดำเนินการตอบสนองความเสี่ยง

เมื่อมีการประเมินความเสี่ยงได้แล้ว ต้องดำเนินการจัดการตอบสนองความเสี่ยงที่เกิดขึ้นเหล่านั้น การจัดการความเสี่ยง คือ กลยุทธ์ หรือกิจกรรมที่กำหนดเพื่อจัดการความเสี่ยงให้สอดคล้องกับระดับที่องค์กรยอมรับได้

ผู้บริหาร เป็นผู้กำหนดว่าจะประเมินค่าความเสี่ยงที่เชื่อมโยงกันได้อย่างไร การตอบสนองรวมถึงการหลีกเลี่ยงความเสี่ยง การลดความเสี่ยง การกระจายความเสี่ยง และการยอมรับความเสี่ยง ในการพิจารณาการตอบสนองความเสี่ยง รวมไปถึงการพิจารณาต้นทุนและผลประโยชน์ และเลือกการตอบสนองที่นำมาซึ่งความน่าจะเกิด (Likelihood) ที่คาดหวังและผลกระทบภายในระดับความเสี่ยงที่ยอมรับได้ที่ปรารถนา

วัตถุประสงค์ของการตอบสนองความเสี่ยง

1. ลดโอกาสเกิดความเสี่ยงและผลกระทบของความเสี่ยงให้เหลือน้อยที่สุด โดยการจัดการสาเหตุของความเสี่ยงอย่างมีประสิทธิภาพ หรือจัดการผลกระทบที่อาจจะเกิดขึ้นของความเสี่ยง

2. การลดผลกระทบของความเสี่ยง ซึ่งโดยมากมักใช้ระบบการเตือนภัยหรือระบบการบริหาร พร้อมด้วยการจัดทำแผนฉุกเฉิน หรือแผนฟื้นฟู

3. การเพิ่ม / สร้าง หรือจัดการโอกาสเกิดความเสี่ยงและผลกระทบจากความเสี่ยง เพื่อให้ได้ผลลัพธ์ที่ดีขึ้น

กลยุทธ์ในการตอบสนอง / บริหารจัดการความเสี่ยง

1. การหลีกเลี่ยงความเสี่ยง (Risk avoidance) หมายถึง การเลิก หรือหลีกเลี่ยงการกระทำและเหตุการณ์ที่ก่อให้เกิดความเสี่ยง เช่น ในงานที่องค์กรไม่ถนัด อาจหลีกเลี่ยงโดยการเลิกหรือลดการกระทำให้เหลือเท่าที่จำเป็นเพื่อการเรียนรู้ การเพิ่มการใช้บริการจากบุคคลภายนอก หรือการทำสัญญารับช่วงเหมาต่อ เป็นต้น กล่าวโดยสรุป การหลีกเลี่ยงความเสี่ยง คือ การไม่ยอมรับความเสี่ยง และอาจทำให้ต้องเปลี่ยนวัตถุประสงค์ของแผนงานหรือยกเลิกแผนงานโครงการนั้นเสีย

2. การควบคุม และการจัดการกับความเสี่ยง (Risk Control) หมายถึง การหาวิธีการควบคุมสาเหตุหรือต้นเหตุของปัจจัยเสี่ยงและกำหนดวิธีการจัดการที่เหมาะสม เพื่อขับเคลื่อนให้แผนงานและโครงการตามกิจกรรมที่กำหนดไว้ดำเนินการไปสู่เป้าประสงค์ได้ในเวลาที่กำหนด หากผู้ที่เกี่ยวข้องไม่อาจดำเนินการได้ต้องรายงานให้ผู้บังคับบัญชาทราบว่าไม่อาจดำเนินการต่อไปได้

การลดโอกาสความน่าจะเกิด หรือการลดความเสียหาย หรือการลดทั้ง 2 ด้านพร้อมกันก็เป็นการควบคุมและการจัดการความเสี่ยงแบบหนึ่ง การลดความเสี่ยงที่สำคัญ คือ การจัดระบบการควบคุมเพื่อป้องกัน หรือค้นพบความเสี่ยงเฉพาะวัตถุประสงค์นั้นอย่างเหมาะสมและทันกาลมากขึ้น รวมถึงการกำหนดแผนสำรองในเหตุฉุกเฉิน (Contingency Planning) ได้แก่ การกำหนดแผนฉุกเฉินสำหรับความเสี่ยงที่คาดการณ์ไว้ล่วงหน้าแล้ว (Known risk) เช่นแผนฉุกเฉินเมื่อไฟฟ้าดับ และเครื่องคอมพิวเตอร์จะไม่ทำงาน ฯลฯ และการควบคุมโดยเครื่องจักรอัตโนมัติ การใช้ระบบการรายงานและการใช้เทคโนโลยีสารสนเทศเพื่อการบริหารและควบคุมที่ดี

3. การกระจายความเสี่ยง (Sharing) หมายถึง การลดโอกาสความน่าจะเกิดหรือการลดความเสียหาย โดยการแบ่งโอน การหาผู้รับผิดชอบร่วมในความเสี่ยง การจัดประกันภัย การกระจายความเสี่ยง (Diversify the risk) ออกไปในหลายกิจกรรม หลายผลิตภัณฑ์ หลายตลาด เป็นต้น หรือถ้าหากแผนงาน/โครงการภายใต้กลยุทธ์มีความเสี่ยงเกินกว่าจะยอมรับได้ หรือเกิดความล้มเหลว

ทางฝ่ายบริหารขององค์กร ก็อาจจะให้น้ำหนักแผนงานหรือโครงการอื่นๆ ภายใต้กลยุทธ์เดียวกันนั้น หรือให้น้ำหนักกับแผนงานอื่นภายใต้กลยุทธ์เดียวกันหรือกลยุทธ์อื่นที่เหมาะกว่าก็ได้

4. การยอมรับความเสี่ยง (Acceptance) เป็นการยอมรับ โดยใช้วิธีการเดิมต่อไปในการจัดการกับความเสี่ยง หมายถึง กิจกรรมของแผนงานนั้นๆ มีความเสี่ยงในระดับหนึ่ง แต่องค์กร รวมทั้งเจ้าของแผนงานสามารถควบคุมและจัดการได้ และสามารถผลักดันกิจกรรมและขั้นตอนต่างๆ ของแผนงานนั้นๆ ไปสู่เป้าประสงค์ได้ในเวลาที่กำหนด หรืออาจอธิบายการยอมรับความเสี่ยงได้ว่า การไม่กระทำการใดๆ เพิ่มเติม กรณีนี้ใช้กับความเสี่ยงที่มี

มุมมองการพัฒนาภาพรวมความเสี่ยงขององค์กร

เพื่อให้เข้าใจภาพรวมการจัดทำความเสี่ยง โดยทำการลดความเสี่ยงเพื่อให้แนวคิดในการที่จะติดตามผลเพื่อทำรายงานการบริหารความเสี่ยงให้มีหลักในการทบทวนผลกระทบในการจัดการความเสี่ยงอย่างโดยเอาแนวคิดการให้คะแนนความเสี่ยงมาอธิบายภาพรวมของความเสี่ยง

การทบทวนและปรังปรุงความเสี่ยง (Review and Revision)

ประเมินการเปลี่ยนแปลงที่มีสาระสำคัญ

การเปลี่ยนแปลงที่มีสาระสำคัญ บริษัทต้องนำมาเป็นเงื่อนไขในการทบทวนและปรับปรุงความเสี่ยงโดยบริษัท จะต้องกำหนดแนวทางการประเมินการเปลี่ยนแปลงที่มีสาระสำคัญไว้ในการประเมินความเสี่ยงภาพรวม ตามขั้นตอนการดำเนินงานประเมินความเสี่ยง

สอบทานความเสี่ยงและผลของการจัดการความเสี่ยง

การสอบทานความเสี่ยงและผลการจัดการ คือ การประเมินมาตรการควบคุมที่มีอยู่เพื่อหาความเสี่ยงคงเหลือ (Residual Risk) โดยความเสี่ยงคงเหลือ (Residual Risk) เป็นเรื่องที่องค์กรจะต้องนำมาทบทวนและปรับปรุงเพื่อกำหนดว่ามาตรการควบคุมดังกล่าว บริษัทสามารถยอมรับได้ สาเหตุที่ต้องสอบทานความเสี่ยงด้วยการประเมินมาตรการควบคุม เพื่อให้ทราบผลการจัดการความเสี่ยง ว่ามีคะแนนอยู่ในระดับการควบคุม (Control Score) หรือไม่ โดยพิจารณาจากหลักเกณฑ์ ต่อไปนี้

ความเสี่ยงคงเหลือ (Residual Risk) = ความเสี่ยงตามธรรมชาติที่ยังไม่ได้ดำเนินการใดๆ – มาตรการควบคุม

แนวทางปรับปรุงการบริหารความเสี่ยงขององค์กร

หลังจากที่ทราบผลการจัดการความเสี่ยง หากพบว่า มีคะแนนที่ได้มากกว่า ระดับการควบคุม (Control Score) บริษัทต้องพิจารณาเพิ่มระดับมาตรการควบคุม (Action Control) ที่มีประสิทธิผลมากยิ่งขึ้น หรือการหลีกเลี่ยงการดำเนินกิจกรรม หรือธุรกิจที่ทำให้เกิดความเสี่ยงนั้นๆ ทำให้บริษัทสามารถใช้ระดับคะแนนความเสี่ยง (Risk Score) และระดับการควบคุม (Control Score) ได้อย่างเหมาะสม โดยต้องทำการประเมินมาตรการควบคุมความเสี่ยงควบคู่กัน

หากพิจารณาแล้วว่ามาตรการนั้น สามารถดำเนินได้แต่ต้องได้รับการอนุมัติจากคณะกรรมการบริหารความเสี่ยง และอยู่ภายในงบประมาณที่วางไว้ได้ ก็สามารถวางแผนการบริหารจัดการความเสี่ยง เพื่อป้องกันหรือลดความเสี่ยงเป็นระดับโครงการนั้น ๆ ต่อไป

ระบบสารสนเทศ การสื่อสาร และการรายงาน (Information, Communication and Reporting)

ระบบสารสนเทศ การสื่อสาร เป็นส่วนสำคัญที่จะช่วยให้การบริหารความเสี่ยงภายในองค์กรมีการดำเนินการได้สำเร็จ เนื่องจากระบบสารสนเทศและการสื่อสารจะเป็นเครื่องมือที่ผู้บริหารสามารถใช้ในการถ่ายทอดนโยบายการกำกับดูแลและติดตามผลสำเร็จของการดำเนินงาน เพื่อให้มีระบบสารสนเทศและการสื่อสารที่ดี บริษัทจึงจัดให้มีระบบสารสนเทศที่ประกอบด้วย

1. การควบคุมสิทธิ์ของผู้ใช้งาน โดยแบ่งออกเป็นลำดับขั้นตอนตามความรับผิดชอบ และประเภทของงาน

2. มีระบบสำรองข้อมูลเพื่อป้องกันปัญหาระบบล่ม หรือเกิดเหตุสุดวิสัยที่ส่งผลต่อข้อมูลสำคัญขององค์กร

3. มีระบบงานที่สามารถเชื่อมโยงแต่ละฝ่าย สามารถบริหารจัดการการใช้ข้อมูลร่วมกันอย่างมีประสิทธิภาพ

4. มีหน่วยงานสำรองที่มีอุปกรณ์และระบบที่สามารถให้หน่วยงานสำคัญ สามารถเข้าปฏิบัติงานได้ทันที หากเกิดเหตุการณ์ฉุกเฉิน เช่น ไฟไหม้ ตึกถล่ม เป็นต้น

5. มีระบบการจัดการสินทรัพย์ที่ สามารถตอบสนองความต้องการของผู้ใช้งาน การใช้งานไม่ยุ่งยากซับซ้อน สะดวกต่อการปฏิบัติงาน

การรายงาน เป็นสิ่งยืนยันว่า บริษัทได้มีการติดตามผลเป็นสิ่งที่ดำเนินงานที่มีความต่อเนื่องอย่างสม่ำเสมอ เมื่อมีการประเมินผลที่ทุกหน่วยงานทราบ และสามารถดำเนินการเมื่อถึงรอบระยะเวลา การติดตามประเมินผลที่กำหนด เช่น รายเดือน รายไตรมาส หรือทุกสิ้นปีงบประมาณ โดยวิธีการสร้างระบบการรายงานสถานะความเสี่ยงให้ชัดเจน รวมถึงความถี่ของการติดตามและจัดทำรายงาน รูปแบบรายงาน ตลอดจนวิธีการนำเสนอรายงานต่อผู้บริหาร นอกจากนี้ควรกำหนดให้มีการรายงานในกรณีที่มีเหตุการณ์พิเศษเกิดขึ้น (Exception Reports) เช่น เหตุการณ์ที่ไม่เกิดขึ้นบ่อยแต่ผลกระทบสูงและมีนัยสำคัญ

วัตถุประสงค์สำคัญที่ต้องมีการรายงานติดตามประเมินผล เพื่อให้ผู้เกี่ยวข้องทราบข้อมูลต่อไปนี้

1) ผลประเมินคุณภาพและความเหมาะสมของการจัดการความเสี่ยง

2) ติดตามผลการจัดการความเสี่ยงที่ได้ดำเนินการไปแล้วหรืออยู่ระหว่างดำเนินการว่าบรรลุผลตามวัตถุประสงค์ของการบริหารความเสี่ยงที่วางไว้หรือไม่

3) ความคืบหน้าของมาตรการควบคุม ว่าสามารถลดโอกาส หรือผลกระทบต่อเหตุการณ์ความเสี่ยงให้อยู่ในระดับที่ยอมรับได้หรือไม่

ดังนั้นรายงานบริหารความเสี่ยงเป็นเครื่องมือสื่อสารอย่างเป็นทางการที่แสดงถึงความสามารถในการบริหารความเสี่ยงของบริษัท โดยแต่ละหน่วยงานต้องสามารถดำเนินการตามแผนการบริหารจัดการความเสี่ยงให้ได้ผล และพิจารณายกเลิก หรือปรับปรุงการดำเนินการตามแผนการจัดการความเสี่ยงที่ยังมีข้อบกพร่อง นอกจากนี้ แต่ละหน่วยงานอาจต้องมีการจัดทำรายงานการติดตามประเมินผลสำหรับใช้ในหน่วยงานเป็นพิเศษ เช่น การจัดทำ Checklist สำหรับใช้เฉพาะแต่ละฝ่าย และกำหนดความถี่ในการติดตามเองภายในฝ่าย ซึ่งจัดเป็นการติดตามประเมินผลอย่างไม่เป็นทางการ โดยสามารถแบ่งรูปแบบการรายงานผลออกเป็น 2 รูปแบบ ประกอบด้วย

1) การรายงานการติดตามผลอย่างเป็นทางการ เป็นการติดตามผลรายครั้ง ตามรอบระยะเวลาที่กำหนด โดยรายงานดังกล่าวต้องนำมาประชุมทบทวนความเสี่ยงประจำปี และสรุปผลเป็นรายงานทบทวนความเสี่ยงประจำปี

2) **การรายงานการติดตามอย่างไม่เป็นทางการ** เป็นการติดตามผลโดยแต่ละหน่วยงานระหว่างการปฏิบัติงาน ซึ่งเป็นการติดตามการทำงานในระดับกิจกรรมที่แต่ละหน่วยงานปฏิบัติตามหน้าที่งานประจำวัน เช่น การจัดทำแผนงาน การตรวจสอบเงินสด การตรวจสอบรายงานของผู้บังคับบัญชา เป็นต้น

การทำรายงานการบริหารความเสี่ยงอย่างเป็นทางการนั้น ทำให้การตรวจสอบภายในทำได้ง่าย และการดำเนินงานมีความโปร่งใส ตรวจสอบได้ และทำให้องค์กรสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง