



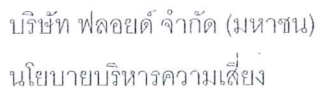
นโยบายการบริหารความเสี่ยง

Risk Management Policy

บริษัท ฟลอยด์ จำกัด (มหาชน)

อนุมัติโดยคณะกรรมการบริษัท ครั้งที่ 1/2568 เมื่อวันที่ 26 กุมภาพันธ์ 2568
ประกาศและให้มีผลบังคับใช้ตั้งแต่วันที่ 1 มีนาคม 2568 เป็นต้นไป

ผู้จัดทำ (Issued By)	ผู้ทบทวน (Checked By)	ลงนามอนุมัติ (Approved By)
 (นางสาวลักษมี เลิศสุกุล) กรรมการและ เลขานุการบริษัท วันที่ 28 FEB 2025	 (นายอภิรัช เมืองเกษม) กรรมการและ รองกรรมการผู้จัดการ วันที่ 28 FEB 2025	 (นายทศพร จิตตวีระ) กรรมการและ กรรมการผู้จัดการ วันที่ 28 FEB 2025



บันทึกการเปลี่ยนแปลง

[illegible]



คำนำ

บริษัท ฟลอยด์ จำกัด (มหาชน) ("บริษัท") ตระหนักถึงความสำคัญในเรื่องการบริหารความเสี่ยง (RISK MANAGEMENT) ซึ่งเป็นส่วนหนึ่งของการกำกับดูแลกิจการที่ดี ในระบบการบริหารงานและการปฏิบัติงาน โดยมุ่งหมายให้การบริหารความเสี่ยงเป็นวัฒนธรรมของผู้ปฏิบัติงานทุกคน ซึ่งนอกจากจะช่วยให้องค์กรสามารถบรรลุวัตถุประสงค์หลัก และจะช่วยสนับสนุนให้บริษัทมีการดำเนินงานที่สร้างมูลค่าเพิ่มให้องค์กรอย่างเป็นรูปธรรม สามารถบรรเทาผลกระทบจากเหตุการณ์ที่อาจเกิดขึ้นกับบริษัทได้

ดังนั้น เพื่อให้หน่วยงานต่าง ๆ ในบริษัทมีแนวทางในการบริหารความเสี่ยงเป็นไปในทิศทางเดียวกัน คณะกรรมการบริหารความเสี่ยงจึงจัดทำคู่มือการบริหารความเสี่ยงของบริษัทฉบับนี้ขึ้น เพื่อใช้เป็นคู่มือการบริหารความเสี่ยงในการปฏิบัติงานสำหรับการดำเนินงาน รวมถึงผู้บริหาร และพนักงานทุกคนของบริษัท โดยกำหนดกรอบการปฏิบัติงานในกระบวนการบริหารความเสี่ยงของบริษัท เพื่อให้นำไปปฏิบัติตัวองค์กร และเพื่อความมั่นใจว่ามีการกำหนดหน้าที่ความรับผิดชอบไว้อย่างเหมาะสม

จัดทำโดย

คณะกรรมการบริหารความเสี่ยง

กุมภาพันธ์ 2568



สารบัญ

	หน้า
วิสัยทัศน์ พันธกิจ	5
ความหมายของการบริหารความเสี่ยง	5
โครงสร้างการบริหารความเสี่ยง	6
หน้าที่ความรับผิดชอบในการบริหารความเสี่ยง	7
วัตถุประสงค์และขอบเขตการบริหารความเสี่ยง.....	9
องค์ประกอบการบริหารความเสี่ยง	11
กระบวนการของการบริหารความเสี่ยง	12
ขั้นตอนที่ 1. การกำหนดวัตถุประสงค์	13
ขั้นตอนที่ 2. การระบุความเสี่ยง	13
ขั้นตอนที่ 3. การประเมินความเสี่ยง	16
ขั้นตอนที่ 4. การจัดทำแผนการจัดการความเสี่ยง	21
ขั้นตอนที่ 5. กิจกรรมการควบคุม	22
ขั้นตอนที่ 6. การติดตามและประเมินผล.....	22
รายงานที่ต้องจัดทำและขั้นตอนการรายงาน	23



วิสัยทัศน์ และพันธกิจ

เพื่อให้ทราบถึงผลกระทบทั้งทางด้านการเงินและไม่ใช้การเงิน ที่อาจเกิดขึ้นจากการปฏิบัติงาน ที่มีอยู่ทั้งหมดในบริษัท และจะได้ร่วมกันหามาตรการควบคุมความเสี่ยงที่มีอยู่ก่อนที่จะเกิดอุบัติเหตุและการสูญเสีย

➤ วิสัยทัศน์ (Vision)

"เป็น 1 ใน 5 ผู้ให้บริการวิศวกรรมด้วยคุณภาพ ปลอดภัย และเติบโตอย่างยั่งยืน"

➤ พันธกิจ (Mission)

1. ให้บริการงานระบบวิศวกรรมอย่างมืออาชีพ มีคุณภาพ ใสใจ และมีมาตรฐาน
2. พัฒนาการให้บริการสู่ความเป็นเลิศ เพื่อให้ลูกค้าเกิดความพึงพอใจสูงสุด
3. พัฒนาการให้บริการควบคู่กับการส่งเสริมให้พนักงานใสใจในความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน
4. พัฒนาบุคลากรและกระบวนการทำงานอย่างยั่งยืนด้วยนวัตกรรมที่ทันสมัย

ความหมายของการบริหารความเสี่ยง

คำนิยาม

ความเสี่ยง คือ เหตุการณ์ที่อาจเกิดขึ้น และจะส่งผลกระทบต่อหรือสร้างความเสียหายแก่บริษัท โดยสามารถวัดความเสี่ยงได้จากผลกระทบและโอกาสที่จะเกิด หรือโอกาสที่จะลดการบรรลุความสำเร็จของเป้าหมายและวัตถุประสงค์ของบริษัททั้งในระดับองค์กรระดับหน่วยงาน และระดับบุคคลได้

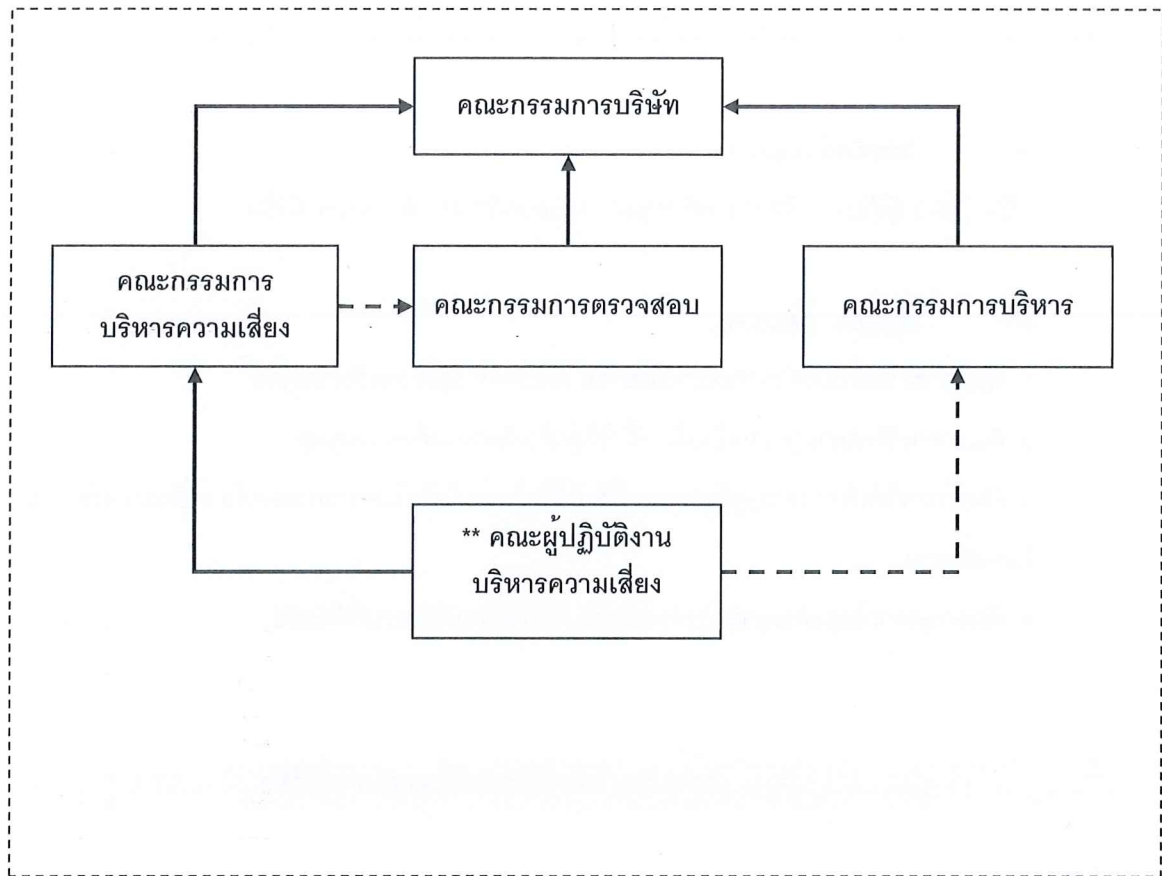
การบริหารความเสี่ยง

การบริหารความเสี่ยง คือ กระบวนการดำเนินการเกี่ยวกับความเสี่ยง ในการดำเนินงานของบริษัทตามเป้าหมายที่ได้วางไว้ โดยจัดให้มีกรอบการปฏิบัติงานในการบริหารความเสี่ยงของบริษัทที่สอดคล้องตามหลักเกณฑ์การบริหารความเสี่ยงที่กำหนดไว้ เพื่อการจัดการหรือบรรเทาความเสี่ยงที่ส่งผลกระทบต่อบริษัทให้ระดับและขนาดของผลกระทบที่จะเกิดขึ้นอยู่ในระดับที่สามารถยอมรับได้ รวมทั้งมีการประเมินควบคุมและการตรวจสอบได้อย่างมีระบบโดยคำนึงถึงการบรรลุเป้าหมายของบริษัทเป็นสำคัญ



โครงสร้างการบริหารความเสี่ยง

บริษัท ฟลอยด์ จำกัด (มหาชน)



หมายเหตุ

**ผู้จัดการฝ่าย และพนักงานในองค์กรทุกคน ขอเรียกว่า ผู้ปฏิบัติงานบริหารความเสี่ยงของฝ่าย หรือ คณะผู้ปฏิบัติงานบริหารความเสี่ยง

โครงสร้างการบริหารความเสี่ยง ประกอบด้วย คณะกรรมการบริหารความเสี่ยงและคณะทำงานบริหารความเสี่ยง ในทุกระดับ

➢ ระดับองค์กร ได้แก่ คณะกรรมการบริหารความเสี่ยงภายใต้นโยบาย และการกำกับดูแลของคณะกรรมการบริหารโดยมีประธานคณะกรรมการบริหารความเสี่ยง เป็นประธาน มีหน้าที่และความรับผิดชอบเป็นไปตามแนวทางปฏิบัติของบริษัท

ระดับ ฝ่าย ได้แก่ ผู้จัดการฝ่าย/แผนก และพนักงานภายในองค์กรทุกคน (เรียกว่า "คณะผู้ปฏิบัติงานบริหารความเสี่ยง") ภายใต้การกำกับดูแลของคณะกรรมการบริหารความเสี่ยง



หน้าที่และความรับผิดชอบในการบริหารความเสี่ยง

คณะกรรมการบริหารความเสี่ยง มีหน้าที่และความรับผิดชอบในการดำเนินการ ดังนี้

1. กำหนดนโยบายและโครงสร้างการบริหารความเสี่ยง เพื่อเสนอต่อคณะกรรมการบริหารโดยใช้แนวทางการบริหารความเสี่ยงของตลาดหลักทรัพย์แห่งประเทศไทยและสมาคมผู้ตรวจสอบภายในแห่งประเทศไทย
2. วางกลยุทธ์ให้สอดคล้องกับนโยบายการบริหารความเสี่ยง เพื่อให้สามารถประเมิน ติดตามและควบคุมความเสี่ยงแต่ละประเภทให้อยู่ในระดับที่ยอมรับได้ โดยให้หน่วยงานต่าง ๆ มีส่วนร่วม ในการบริหารและควบคุมความเสี่ยง
3. ประเมินความเสี่ยงในระดับองค์กร และกำหนดวิธีการบริหารความเสี่ยงนั้นให้อยู่ในระดับที่ยอมรับได้ รวมทั้งควบคุมดูแลให้มีการบริหารความเสี่ยงตามวิธีการที่กำหนดไว้
4. ทบทวนนโยบายการบริหารความเสี่ยงและปรับปรุงให้มีประสิทธิภาพและประสิทธิผลอย่างเพียงพอที่จะควบคุมความเสี่ยง
5. มีอำนาจในการเรียกบุคคลที่เกี่ยวข้องมาชี้แจงหรือแต่งตั้งและกำหนดบทบาทที่ให้ผู้ปฏิบัติงานทุกระดับมีหน้าที่บริหารความเสี่ยงตามความเหมาะสม และให้รายงานต่อคณะกรรมการบริหารความเสี่ยงเพื่อให้การบริหารความเสี่ยงบรรลุวัตถุประสงค์
6. รายงานผลของการบริหารความเสี่ยงต่อคณะกรรมการบริหารและคณะกรรมการตรวจสอบ เพื่อนำเสนอต่อคณะกรรมการบริษัททุกครั้งเมื่อมีการจัดประชุม
7. ทบทวนแผนดำเนินงานต่อเนื่อง (Business Continuity Plan) อย่างน้อยปีละ 1 ครั้ง และจัดทำการบันทึกสรุปผลการทดสอบ พร้อมทั้งปรับปรุงแผนให้เป็นปัจจุบัน

นอกจากนี้ คณะกรรมการบริหารความเสี่ยงยังมีหน้าที่ที่ต้องดำเนินการดังต่อไปนี้

1. จัดทำคู่มือการบริหารความเสี่ยง
2. ระบุความเสี่ยงด้านต่าง ๆ พร้อมทั้ง วิเคราะห์ และประเมินความเสี่ยงที่อาจเกิดขึ้น รวมทั้งแนวโน้มซึ่งมีผลกระทบต่อบริษัท
3. จัดทำแผนงานเพื่อป้องกัน หรือลดความเสี่ยง
4. ติดตาม ประเมินผล และจัดทำรายงานการบริหารความเสี่ยง
5. จัดวางระบบบริหารความเสี่ยงแบบบูรณาการโดยเชื่อมโยงระบบสารสนเทศ
6. ปฏิบัติงานอื่น ๆ ตามที่คณะกรรมการบริหารความเสี่ยงเห็นสมควร

หน้าที่ความรับผิดชอบของคณะผู้ปฏิบัติงาน คณะผู้ปฏิบัติงาน ได้แก่ ผู้จัดการฝ่ายและพนักงานในองค์กรทุกคนจะเป็นผู้รับแนวทางการจัดการความเสี่ยงไปจัดทำแผนรองรับความเสี่ยงที่เกี่ยวข้อง ดำเนินการและรายงานผลการดำเนินการตามแผนให้เลขาธิการคณะกรรมการบริหารความเสี่ยงตามกำหนดเวลา ภายใต้การกำกับดูแลของคณะกรรมการบริหารความเสี่ยง ซึ่งแต่ละฝ่ายจะต้องดำเนินการดังต่อไปนี้

1. ระบุความเสี่ยงด้านต่าง ๆ พร้อมทั้งวิเคราะห์ และประเมินความเสี่ยงที่อาจเกิดขึ้น รวมทั้งแนวโน้มซึ่งมีผลกระทบต่อบริษัท
2. จัดทำแผนเพื่อป้องกัน หรือ ลดความเสี่ยง
3. ประเมินผล และจัดทำรายงานการบริหารความเสี่ยงของแผน
4. จัดวางระบบบริหารความเสี่ยงเชื่อมโยงกับระบบสารสนเทศ
5. ปฏิบัติงานอื่น ๆ ตามที่คณะกรรมการบริหารความเสี่ยงมอบหมาย



➤ หน้าที่ความรับผิดชอบของคณะกรรมการตรวจสอบ (Audit Committee)

คณะกรรมการตรวจสอบ (Audit Committee) มีหน้าที่สอบทานให้บริษัทมีระบบบริหารความเสี่ยงที่เหมาะสมและมีประสิทธิภาพ กำกับดูแลและติดตามการบริหารความเสี่ยงอย่างเป็นอิสระตลอดจนสื่อสารกับคณะกรรมการบริหารความเสี่ยงเพื่อให้เข้าใจความเสี่ยงที่สำคัญและเชื่อมโยงกับการควบคุมภายใน รายงานต่อคณะกรรมการบริษัทเกี่ยวกับความเสี่ยงและการจัดการความเสี่ยง

➤ หน้าที่ความรับผิดชอบของฝ่ายตรวจสอบภายใน (Internal Audit)

ฝ่ายตรวจสอบภายใน (Internal Audit) มีหน้าที่สอบทานและประเมินประสิทธิภาพของกระบวนการบริหารความเสี่ยง



วัตถุประสงค์และขอบเขตการบริหารความเสี่ยง

วัตถุประสงค์ของการบริหารความเสี่ยง เพื่อจัดการปัญหาอุปสรรคในการทำงาน ป้องกันหรือลดโอกาสที่จะเกิดเหตุการณ์ไม่พึงประสงค์และผลกระทบที่อาจเกิดขึ้น ซึ่งจะทำให้การดำเนินงานไม่บรรลุวัตถุประสงค์และเป้าหมายขององค์กร นอกจากนี้ ยังเป็นการส่งเสริมให้มีการกำกับดูแลกิจการที่ดี

➤ ขอบเขตการบริหารความเสี่ยง

เพื่อให้การดำเนินงานมีความต่อเนื่องและบรรลุตามวัตถุประสงค์ของบริษัท ดังนั้น ทุกหน่วยงานจะต้องมีการบริหารความเสี่ยงโดยให้การบริหารความเสี่ยงเป็นกระบวนการหนึ่งในการปฏิบัติงานประจำวันของพนักงานทุกคน โดยมีจุดมุ่งหมายให้การบริหารความเสี่ยงถูกปลูกฝังเป็นส่วนหนึ่งของวัฒนธรรมองค์กร

➤ ปัจจัยที่ผลักดันให้มีการบริหารความเสี่ยง

- ข้อกำหนดของหน่วยงานที่กำกับดูแลองค์กร
- คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์แห่งประเทศไทย
- สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย
- ทศนคติของผู้บริหาร

นโยบายการบริหารความเสี่ยง ทุกหน่วยงานต้องจัดให้มีการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่องภายใต้กระบวนการบริหารความเสี่ยงที่เป็นมาตรฐานเดียวกัน โดยการนำเทคโนโลยีสารสนเทศมาใช้ เพื่อให้เกิดความรวดเร็วในการสื่อสารและประมวลผลตลอดจนต้องมีการติดตามและประเมินผลพร้อมปรับแผนการบริหารความเสี่ยงเป็นระยะ ๆ อย่างสม่ำเสมอเพื่อให้การดำเนินการบรรลุวัตถุประสงค์

ประโยชน์ของการบริหารความเสี่ยง เมื่อบริษัทมีการบริหารความเสี่ยงที่ดีและเหมาะสมแล้วบริษัทจะได้ประโยชน์โดยตรงจากการบริหารความเสี่ยง ดังนี้

1. ผลการดำเนินงานของบริษัทสามารถเป็นไปตามเป้าหมายและวัตถุประสงค์ของบริษัทที่ตั้งไว้
2. ส่งเสริมให้เกิดความเจริญเติบโตทางธุรกิจอย่างต่อเนื่องและยั่งยืนเพื่อสร้างมูลค่าเพิ่มให้กับบริษัทและผู้มีส่วนได้ส่วนเสีย
3. ส่งเสริมให้เกิดการกำกับดูแลกิจการที่ดี
4. ส่งเสริมให้พนักงานเกิดความรู้ความเข้าใจและตระหนักถึงความสำคัญของการบริหารความเสี่ยง ซึ่งจะส่งผลต่อเนื่องให้เกิดความระมัดระวังในการทำงานและลดโอกาสที่จะทำให้เกิดการสูญเสียจากการดำเนินงาน



5. ในการจัดทำแผนงานโครงการต่าง ๆ บริษัทสามารถนำผลของการวิเคราะห์ความเสี่ยงที่เกิดขึ้นมาใช้เป็นส่วนหนึ่งเพื่อประกอบการตัดสินใจที่จะทำหรือไม่ทำโครงการใด ๆ ที่จะส่งผลกระทบต่อบริษัทได้
6. ช่วยให้การกำหนดวัตถุประสงค์และกลยุทธ์ต่าง ๆ ของบริษัทให้มีความสมบูรณ์และความเป็นไปได้มากขึ้นและสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้
7. ส่งเสริมให้เกิดการเตรียมความพร้อมและแนวทางแก้ไขปัญหาดังกล่าวที่อาจเกิดขึ้นและส่งผลกระทบต่อผลการดำเนินงานของบริษัท

นอกจากประโยชน์ทางตรงที่บริษัทจะได้รับแล้วยังมีประโยชน์ด้านอื่น ๆ ที่บริษัทจะได้รับจากการบริหารความเสี่ยง ดังนี้

1. มีระบบเทคโนโลยีและสารสนเทศที่ช่วยในการจัดเก็บข้อมูล การคำนวณต่าง ๆ การรายงานและสอบถามข้อมูลได้อย่างถูกต้องครบถ้วนสมบูรณ์รวดเร็ว
2. ผู้บริหารมีข้อมูลเพื่อใช้ประกอบในการตัดสินใจได้อย่างถูกต้องและรวดเร็วยิ่งขึ้น
3. มีการจัดสรรทรัพยากรอย่างเหมาะสมโดยคำนึงถึงความคุ้มค่าในการลงทุน
4. เกิดการมีส่วนร่วมของพนักงานในบริษัท และการบูรณาการเข้ากับระบบงานส่วนอื่น ๆ ขององค์กรที่จะร่วมกันผลักดันให้องค์กรเกิดผลสำเร็จตามวัตถุประสงค์ที่ตั้งไว้



องค์ประกอบการบริหารความเสี่ยง

บริษัทได้นำองค์ประกอบระบบการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management Integrated Framework) ของ The Committee of Sponsoring Organizations of the Tread way Commission (COSO) มาใช้เป็นแนวทางในการบริหารความเสี่ยง ซึ่งมีองค์ประกอบการบริหารความเสี่ยง ดังนี้

1. กำหนดวัตถุประสงค์ (Objective Setting)
2. การระบุความเสี่ยง (Risk Identification)
3. การประเมินความเสี่ยง (Risk Assessment)
4. การจัดทำแผนจัดการความเสี่ยง (Risk Response)
5. กิจกรรมการควบคุม (Control Activities)
6. ติดตาม และประเมินผล (Monitoring & Evaluation)

จากองค์ประกอบกระบวนการบริหารความเสี่ยงตามแนวทางของ COSO ข้างต้น มีกระบวนการที่ทุกหน่วยงานต้องดำเนินการอย่างต่อเนื่อง 6 ขั้นตอน เรียกว่า “กระบวนการการบริหารความเสี่ยง”

นอกจากนี้ อีก 2 ข้อ คือ สภาพแวดล้อมภายในองค์กรและสารสนเทศและการสื่อสาร เป็นองค์ประกอบที่เสริมให้กระบวนการบริหารความเสี่ยงทั้ง 6 ขั้นตอน มีประสิทธิภาพและเพิ่มโอกาสให้การบริหารความเสี่ยงบรรลุวัตถุประสงค์

สภาพแวดล้อมภายในองค์กร (Internal Environment)

บริษัทจะจัดให้มีสภาพแวดล้อมและบรรยากาศที่เอื้ออำนวย ซึ่งเป็นพื้นฐานสำหรับขั้นตอนอื่น ๆ ในการบริหารความเสี่ยงในองค์กรหากไม่มีสภาพแวดล้อมภายในองค์กรที่ดีจะมีผลต่อการกำหนดกลยุทธ์และเป้าหมายของบริษัทที่กำหนดกิจกรรมการป้องกันที่ประเมินและการจัดการกับความเสี่ยง

องค์ประกอบที่สำคัญต่อสภาพแวดล้อม ประกอบด้วย

1. ปรัชญา ความเชื่อ วัฒนธรรมในการบริหารความเสี่ยงเพื่อสร้างมูลค่าให้กับบริษัทในระยะยาว
2. บทบาทของคณะกรรมการตรวจสอบเป็นปัจจัยสำคัญในการกำกับดูแลการบริหารความเสี่ยง
3. คัดเลือกบุคลากรที่มีความรู้ความสามารถ ความซื่อสัตย์ และพัฒนาให้เหมาะสมกับงานที่ได้รับมอบหมาย
4. จัดให้มีโครงสร้างองค์กรที่เหมาะสม
5. การกำหนดอำนาจหน้าที่ที่เหมาะสม ใหพนักงานสามารถปฏิบัติหน้าที่ ให้บรรลุวัตถุประสงค์ของบริษัท

สารสนเทศและการสื่อสาร (Information & Communication)

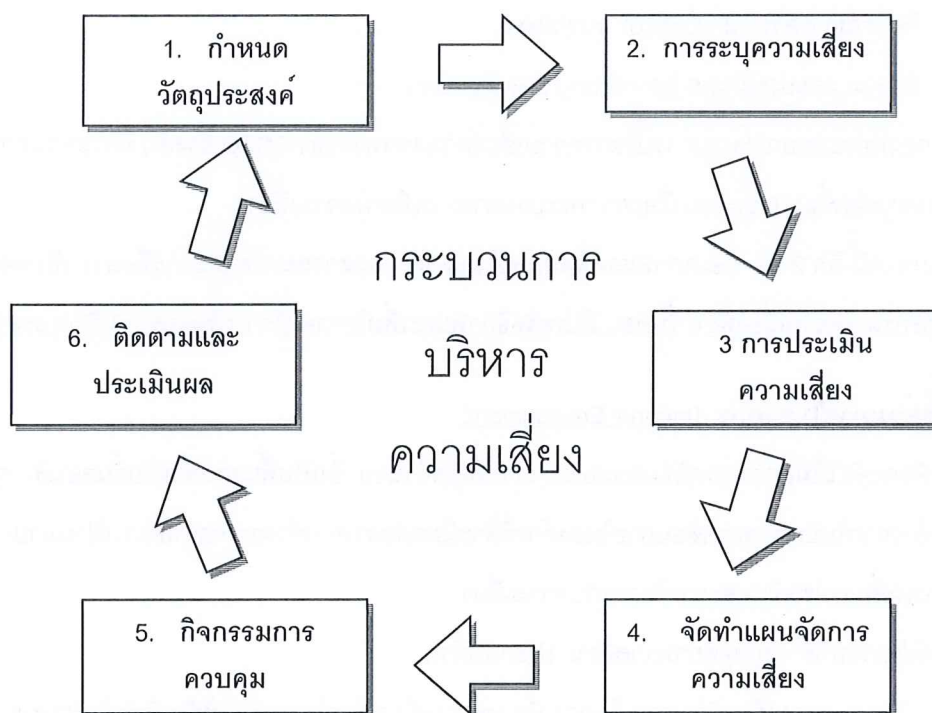
1. ต้องมีการสื่อสารที่ชัดเจนจากคณะกรรมการบริษัท และผู้บริหารระดับสูงเกี่ยวกับนโยบายการบริหารความเสี่ยง และให้พนักงานทุกคนได้เข้าใจบทบาทหน้าที่ของตนในการบริหารความเสี่ยงเพื่อปรับเปลี่ยนพฤติกรรม และ/กิจกรรมที่ต้องดำเนินการ โดยคาดหวังให้ความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้



2. ต้องมีการระบุแหล่งที่มาและรวบรวมสารสนเทศทั้งจากภายในและภายนอกองค์กรจัดเก็บและสื่อสารในรูปแบบที่กำหนดและภายในระยะเวลาที่กำหนดเพื่อให้ผู้บริหารและพนักงานสามารถรับรู้ทันต่อเหตุการณ์ปฏิบัติงานที่และติดต่อสื่อสารทางด้านการบริหารความเสี่ยงอย่างสม่ำเสมอและมีประสิทธิภาพ

กระบวนการของการบริหารความเสี่ยง ของบริษัท ฟลอยด์ จำกัด (มหาชน)

กระบวนการบริหารความเสี่ยงของบริษัทตามแนวทางของ COSO ประกอบด้วย 6 ขั้นตอน ดังนี้



- | | | |
|------------|----|---|
| ขั้นตอนที่ | 1. | การกำหนดวัตถุประสงค์ (Objective Setting) |
| ขั้นตอนที่ | 2. | การระบุความเสี่ยง (Risk Identification) |
| ขั้นตอนที่ | 3. | การประเมินความเสี่ยง (Risk Assessment) |
| ขั้นตอนที่ | 4. | การจัดทำแผนการจัดการความเสี่ยง (Risk Response) |
| ขั้นตอนที่ | 5. | กิจกรรมการควบคุม (Control Activities) |
| ขั้นตอนที่ | 6. | การติดตามและประเมินผล (Monitoring & Evaluation) |



➤ ขั้นตอนที่ 1 การกำหนดวัตถุประสงค์ (Objective Setting)

เพื่อให้ทราบขอบเขตการดำเนินงานในแต่ละระดับ และสามารถวิเคราะห์ความเสี่ยงที่คาดว่าจะเกิดขึ้นได้อย่างครบถ้วน ดังนั้น การกำหนดวัตถุประสงค์ในการบริหารความเสี่ยงที่ดีของระดับหน่วยงาน และเพื่อให้วัตถุประสงค์ในภาพรวมบรรลุเป้าหมายมีดังนี้

1. จะต้องมีความชัดเจน สามารถวัดได้ สามารถปฏิบัติได้ มีเหตุผล และมีกรอบระยะเวลาที่จะดำเนินการได้แล้วเสร็จ ซึ่งเป็นไปตามหลักการ "SMART" ซึ่งย่อมาจาก

- Specific : เฉพาะเจาะจง / ชัดเจน
- Measurable : สามารถวัดได้
- Achievable : สามารถบรรลุผลได้ / ปฏิบัติได้
- Reasonable : เป็นจริงได้ / สมเหตุสมผล
- Time constrained : มีกำหนดเวลา / กรอบเวลา

จะต้องมีการเชื่อมโยงกับเป้าหมายและสอดคล้องกับวัตถุประสงค์ของบริษัทฯ หรือตัวชี้วัดของหน่วยงานและสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และระดับของความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance)

Risk Appetite หมายถึง ประเภทปัจจัยความเสี่ยงและระดับของความเสี่ยงที่บริษัทยอมรับได้ เพื่อช่วยให้บริษัทฯ บรรลุวิสัยทัศน์และภารกิจของบริษัท

Risk Tolerance หมายถึง ระดับความเบี่ยงเบนจากประเภทปัจจัยความเสี่ยงและระดับของความเสี่ยงที่ยอมรับได้

➤ ขั้นตอนที่ 2 การระบุความเสี่ยง (Risk Identification)

การระบุความเสี่ยง เป็นการค้นหาว่ามีความเสี่ยงใดที่มีโอกาสเกิดขึ้นและทำให้หน่วยงานและองค์กรไม่บรรลุวัตถุประสงค์ซึ่งการระบุความเสี่ยงมีขั้นตอน ดังนี้

1. พิจารณาจาก กิจกรรม โครงการ กระบวนการทำงานที่เกี่ยวข้อง ตามแผนงานต่างๆ ของบริษัทฯ เช่น แผนปฏิบัติการประจำปีและแผนธุรกิจประจำปีและอื่นๆ เป็นต้น ที่ทำให้ไม่สามารถบรรลุวัตถุประสงค์และเป้าหมาย
2. ระบุความเสี่ยงหรือค้นหาความเสี่ยงและสาเหตุ โดยพิจารณาแหล่งที่มาของความเสี่ยงทั้งปัจจัยภายในและปัจจัยภายนอกที่มีผลทำให้การดำเนินงานของแต่ละกิจกรรม โครงการ กระบวนการทำงาน ไม่บรรลุวัตถุประสงค์และเป้าหมาย

➤ วิธีการระบุความเสี่ยงที่สำคัญ มีดังนี้

1. วิเคราะห์ทางเดินของงานและเอกสาร หรือวิเคราะห์กระบวนการ
2. การระดมสมอง
3. จัดประชุมเชิงปฏิบัติการ
4. การเก็บข้อมูลประวัติเหตุการณ์ความเสียหายที่เกิดขึ้น



➤ แหล่งที่มาของความเสี่ยงจากปัจจัยภายใน อาจมาจากปัจจัยต่าง ๆ ดังนี้

1. วัตถุประสงค์ของบริษัทฯ
2. นโยบายและกลยุทธ์
3. การดำเนินงาน กระบวนการทำงาน
4. โครงสร้างองค์กรและระบบการบริหารงานการเงิน

➤ แหล่งที่มาของความเสี่ยงจากปัจจัยภายนอก อาจมาจากปัจจัยต่าง ๆ ดังนี้

1. นโยบายของรัฐบาล
2. สภาพเศรษฐกิจ
3. การแข่งขัน (คู่แข่งทางการดำเนินธุรกิจ)
4. กฎระเบียบ
5. เหตุการณ์ธรรมชาติ
6. อื่น ๆ

3. การจัดประเภทความเสี่ยงสามารถแบ่งเป็น 6 ประเภท ดังนี้

3.1 ความเสี่ยงด้านกลยุทธ์ (Strategic Risk: S) หมายถึง ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ทางการตลาด, กลยุทธ์ทางด้านพันธมิตรธุรกิจ, กลยุทธ์การเข้าสู่ธุรกิจใหม่ และการปฏิบัติตามแผนกลยุทธ์อย่างไม่เหมาะสม รวมถึงความไม่สอดคล้องกันระหว่างนโยบาย เป้าหมาย กลยุทธ์ โครงสร้างองค์กร ภาวะการแข่งขัน

3.2 ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk: O) หมายถึง ความเสี่ยงที่เกิดจากการปฏิบัติงานทุก ๆ ขั้นตอนโดยครอบคลุมถึงปัจจัยที่เกี่ยวข้องกับกระบวนการ อุปกรณ์เทคโนโลยีและความสามารถของระบบงาน (IT), ความสามารถของบุคคล, การสร้างประสบการณ์ลูกค้า และการฟ้องร้องความเสียหายจากคู่สัญญา

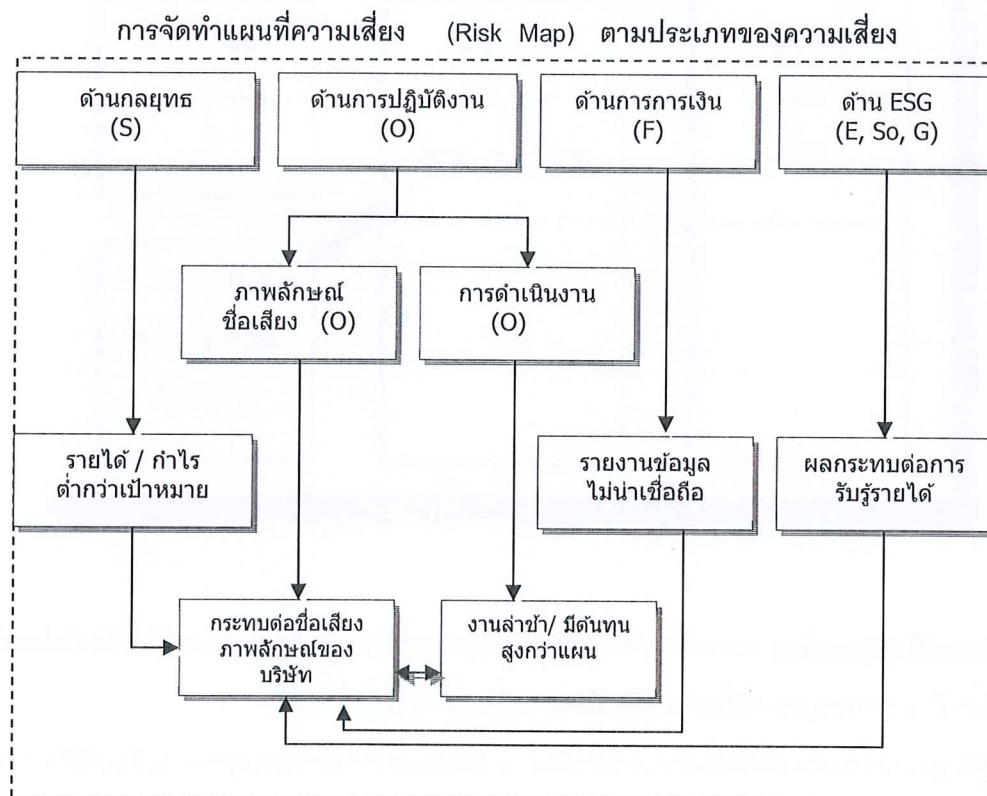
3.3 ความเสี่ยงด้านการเงิน (Financial Risk: F) หมายถึง ความเสี่ยงที่อาจเกิดจากสภาพคล่องทางการเงิน, ความสามารถในการจัดการหนี้, มูลค่ากิจการ, ความมีประสิทธิภาพ และการบันทึกบัญชี ซึ่งอาจส่งผลให้บริษัทฯ ไม่สามารถบรรลุได้ตามเป้าหมาย และส่งผลกระทบต่อความเสี่ยงเกี่ยวกับการรายงานข้อมูลต่าง ๆ ให้มีความถูกต้องชัดเจน

3.4 ความเสี่ยงด้านสภาพแวดล้อม (Environmental Risk: E) หมายถึง ความเสี่ยงที่เกิดขึ้นจากสภาพการเปลี่ยนแปลงของสิ่งแวดล้อมธรรมชาติ และก่อให้เกิดผลกระทบต่อการดำรงชีวิตของสิ่งมีชีวิตทั้งหลาย และส่งผลกระทบต่อ การดำเนินธุรกิจของบริษัท

3.5 ความเสี่ยงด้านสังคม (Social Risk: So) หมายถึง ความเสี่ยงที่เกิดขึ้นจากความสัมพันธ์ระหว่างบริษัทกับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับบริษัททั้งภายในและภายนอก ได้แก่ พนักงาน ลูกค้า ผู้มีส่วนได้ส่วนเสีย ชุมชนท้องถิ่น และผู้ทำงานในห่วงโซ่คุณค่า (Value Chain) เพราะธุรกิจที่มีความสัมพันธ์ที่ดีกับผู้มีส่วนที่เกี่ยวข้องย่อมมีแนวโน้มที่การดำเนินงานของธุรกิจจะเป็นไปอย่างราบรื่น รวมทั้งได้รับความไว้วางใจจากลูกค้าของธุรกิจ

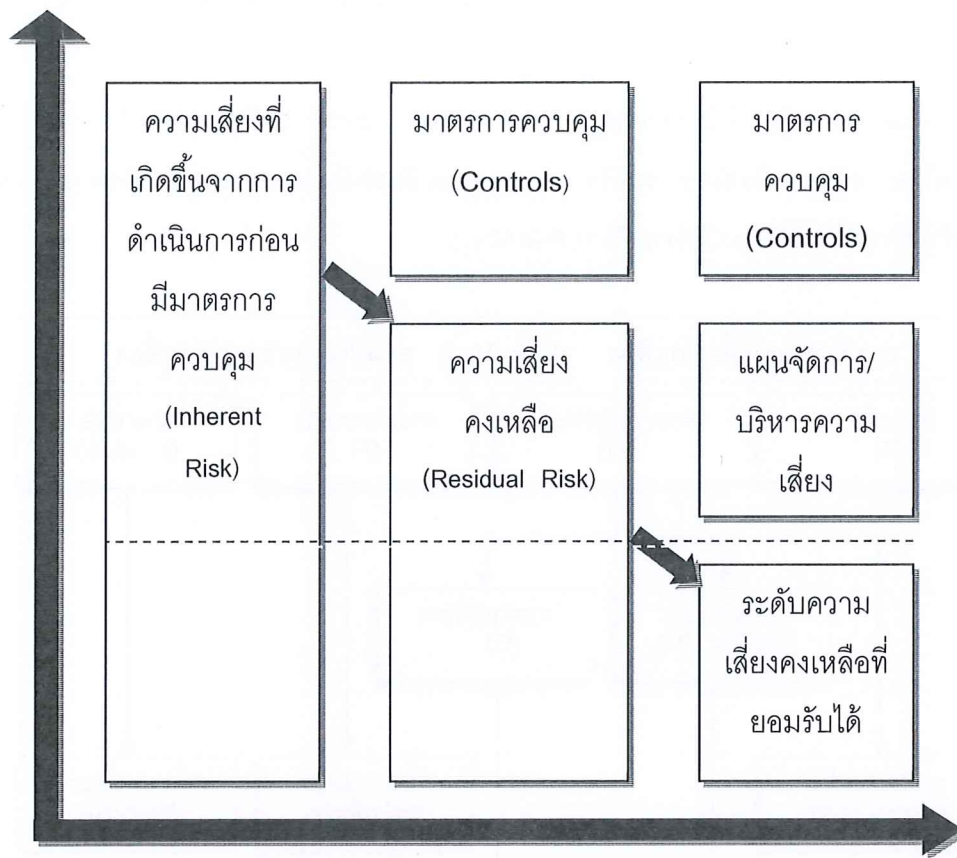
3.6 ความเสี่ยงด้านธรรมาภิบาล (Governance Risk: G) หมายถึง ความเสี่ยงที่เกิดขึ้นจากความโปร่งใสในการดำเนินงานของธุรกิจ รวมไปถึงนโยบายที่เกี่ยวข้องกับการต่อต้านการทุจริตและการตรวจสอบเพื่อผลประโยชน์ที่เป็นธรรมกับผู้มีส่วนเกี่ยวข้องของธุรกิจ โดยทุกขั้นตอนการดำเนินงานต้องโปร่งใส ยุติธรรม และตรวจสอบได้

การจัดประเภทความเสี่ยงให้เป็นหมวดหมู่ (S O F E So G) จะแสดงให้เห็นความสัมพันธ์ของความเสี่ยงแต่ละประเภทแต่ละเรื่องได้อย่างชัดเจนเพื่อให้สามารถบริหารจัดการความเสี่ยงที่เป็นต้นเหตุของความเสียหายอย่างแท้จริง โดยสามารถแสดงให้เห็นได้จากการจัดทำแผนที่ความเสี่ยง (Risk Map)





➤ **ขั้นตอนที่ 3 การประเมินความเสี่ยง (Risk Assessment)**



การประเมินความเสี่ยง หมายถึง การวัดระดับความรุนแรงของความเสี่ยงว่ามีมากน้อยเพียงใดโดยนำความเสี่ยงที่ได้จากขั้นตอนที่ 2 (การระบุความเสี่ยง) มาประเมินความเสี่ยงโดยมีขั้นตอน ดังนี้

1. พิจารณารisk ที่เกิดขึ้นจากการดำเนินการก่อนมีมาตรการการควบคุมความเสี่ยงที่ได้จากการระบุความเสี่ยงในขั้นตอนที่ 2 โดยพิจารณาระดับความรุนแรงของความเสี่ยง และ โอกาสที่อาจจะเกิดขึ้นก่อนมีมาตรการควบคุม (Inherent Risk)
2. ระบุมาตรการควบคุมที่มีอยู่ (Controls) เพื่อควบคุม/ ลดความเสี่ยงของแต่ละสาเหตุความเสี่ยง
3. ประเมินความเสี่ยงที่เหลืออยู่หลังจากมีมาตรการควบคุม (Residual Risk) โดยวิเคราะห์หาโอกาสที่จะเกิดความเสี่ยง (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) ตามเกณฑ์ในการพิจารณาระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) ซึ่งสามารถพิจารณาได้ทั้งเชิงคุณภาพและเชิงปริมาณโดยบริษัท กำหนดเกณฑ์ในการประเมินไว้ 5 ระดับ

คำจำกัดความของผลกระทบ และโอกาสที่จะเกิดในการประเมินความเสี่ยง

Definition	rating	Impact Factor				การดำเนินงาน
		การเงิน	ชื่อเสียง	กฎระเบียบ	พนักงาน	
5 Severe	5	ค่าปรับ 2 เท่าของมูลค่า หรือประโยชน์ที่ได้รับ หรือ > 50 ล้านบาท	เป็นข่าวเชิงลบในหน้าหนังสือพิมพ์ระดับประเทศ ติดต่อกันมากกว่า 1 สัปดาห์	- บริษัทถูกขึ้นบัญชีต้องห้าม - หน่วยงานกำกับดูแลมีคำสั่งให้ผู้บริหารหยุดการบริหารงาน - ภาพลักษณ์บริษัทติดลบในเรื่องการกำกับดูแลกิจการที่ดี	เสียชีวิต	การปฏิบัติงานหยุดชะงักมากกว่า 20 วัน
4 Significant	4	ระหว่าง 5 - 50 ล้านบาท	สื่อลงข่าวกรณีต่อเนื่องและสังคมเริ่มให้ความสนใจ	ถูกหน่วยงานรัฐตรวจสอบและชี้มูลความผิด	ได้รับบาดเจ็บจนต้องเข้าโรงพยาบาลต่อเนื่องมากกว่า 3 เดือน	การปฏิบัติงานหยุดชะงักมากกว่า 5 - 20 วัน
3 Moderate	3	ระหว่าง 1 - 5 ล้านบาท	สื่อสังคมออนไลน์เผยแพร่ข่าวหรือข้อมูลเชิงลบที่บริษัทเกี่ยวข้อง	บริษัทอาจต้องส่งหลักฐานและเข้าชี้แจงหากหน่วยงานตรวจสอบรับเรื่อง	ได้รับบาดเจ็บจนต้องเข้าโรงพยาบาลต่อเนื่องมากกว่า 1 เดือน แต่ไม่เกิน 3 เดือน	การปฏิบัติงานหยุดชะงักมากกว่า 7 - 15 วัน
2 Minor	2	ระหว่าง 1 หมื่น - 1 ล้านบาท	ปรากฏข่าวลือที่อาจพาดพิงคนภายในบริษัทหรือบริษัท	เป็นการทำความผิดที่อาจถูกตักเตือน หรือปรับตามค่าธรรมเนียมที่มูลค่าไม่มีนัยสำคัญ	ได้รับบาดเจ็บจนต้องเข้าโรงพยาบาล < 1 เดือน	การปฏิบัติงานหยุดชะงักมากกว่า 3 - 7 วัน
1 Negligible	1	ต่ำกว่า 1 หมื่นบาท	แทบจะไม่มี	แทบจะไม่มี	แทบจะไม่มี	แทบจะไม่มี

คำจำกัดความโอกาสที่จะเกิด

คะแนน	คำอธิบาย	ความถี่ที่สามารถเกิดความเสี่ยงขึ้นได้	ความเป็นไปได้ที่จะเกิดความเสียหาย
1	ยากที่จะเกิด	เหตุการณ์ที่ไม่น่ามีโอกาสเกิดขึ้นได้ในการดำเนินธุรกิจ	1 ครั้ง/ 5-10 ปี
2	ไม่น่าจะเกิด	เหตุการณ์ที่อาจเกิดขึ้นน้อยมากในการดำเนินธุรกิจ	1 ครั้ง/ใน 5 ปี
3	เป็นไปได้ที่จะเกิด	เหตุการณ์ที่น่าจะเป็นไปได้ หรืออาจเกิดขึ้นได้บางครั้งในการดำเนินธุรกิจ	1 ครั้ง/ใน 3-5 ปี
4	น่าจะเกิด	เหตุการณ์ที่เป็นไปได้อย่างสูง หรือเกิดขึ้นเป็นประจำในการดำเนินธุรกิจส่วนใหญ่	1 ครั้ง /ใน 2 ปี
5	ค่อนข้างแน่นอน	เหตุการณ์ที่มีความแน่นอน หรือเกิดขึ้นเป็นประจำในทุกๆการดำเนินธุรกิจ	>1 ครั้ง /ปี

“ระดับความเสี่ยง” หรือ “ค่าคะแนนความเสี่ยง” เท่ากับ ผลคูณของ “โอกาสที่จะเกิดความเสียหาย” (Likelihood) กับ “ระดับความรุนแรงของผลกระทบ” (Impact)



4. นำ “ระดับความเสี่ยง” ที่ได้ประเมินแล้วตามข้อ 3. มาจัดลำดับโดยระดับความสำคัญของความเสี่ยงมีทั้งหมด 4 ระดับ ดังนี้

คำจำกัดความของระดับความเสี่ยง		
ค่าคะแนนความเสี่ยง (ผลกระทบ X โอกาสที่จะเกิด)	ระดับความเสี่ยงโดยรวม	แนวทางการตอบสนองต่อความเสี่ยง
16 – 25	สูงมาก ระดับ 1. E: Extremely Risk	เป็นความเสี่ยงระดับสูงมากและเกินกว่าค่าระดับความเสี่ยงที่ยอมรับได้ขององค์กร (16-25) ซึ่งจำเป็นต้องได้รับการพิจารณาถึงระดับ ความเสี่ยงที่ยอมรับได้ในรายละเอียด เพื่อจัดทำแผนการดำเนินงานเพิ่มเติมสำหรับบริหารจัดการความเสี่ยง
9 - 15	สูง ระดับ 2. H: High Risk	เป็นความเสี่ยงระดับสูงซึ่งอยู่ในช่วงเบี่ยงเบนระดับความเสี่ยงที่ยอมรับได้ (9-14) โดยผู้บริหารควรพิจารณาจัดทำแผนการดำเนินงานเพิ่มเติม หรือดำเนินการปรับปรุงประสิทธิภาพของมาตรการหรือการควบคุมภายในที่มีในปัจจุบัน
4 – 8	ปานกลาง ระดับ 3. M: Moderate Risk	เป็นความเสี่ยงระดับปานกลาง (4-8) ซึ่งอาจไม่จำเป็นต้องมีแผนการดำเนินงานเพิ่มเติม โดยผู้บริหารควรมอบหมายให้ผู้รับผิดชอบในส่วนงานดำเนินการติดตามประสิทธิภาพการควบคุมภายในกระบวนการเป็นประจำ
1 – 3	ต่ำ ระดับ 4. L: Low Risk	เป็นความเสี่ยงระดับต่ำ (1-3) ซึ่งอาจไม่จำเป็นต้องมีแผนการดำเนินงานเพิ่มเติม โดยผู้บริหารควรมอบหมายให้ผู้รับผิดชอบในส่วนงานดำเนินการติดตามผลกระทบที่เกี่ยวข้องเนื่องกันของความเสี่ยงเป็นประจำ

การประเมินความเสี่ยงต้องดำเนินการทั้งก่อนการจัดทำแผนจัดการ/บริหารความเสี่ยงและหลังจากที่ได้ดำเนินการตามแผนจัดการ/บริหารความเสี่ยงแล้ว ซึ่งจะทำให้ทราบว่าแผนจัดการ/บริหารความเสี่ยงมีประสิทธิภาพและประสิทธิผลเพียงพอหรือไม่ หรือปรับปรุงแผนจัดการ/บริหารความเสี่ยงหรือไม่



ตารางจัดลำดับความเสี่ยง (Risk Matrix) และระดับความเสี่ยงที่ยอมรับได้
 “คณะกรรมการบริหารความเสี่ยง กำหนดระดับความเสี่ยงที่ยอมรับได้ไว้ที่ระดับความเสี่ยงไม่เกิน 5”

		ระดับความเสี่ยงและผลกระทบ				
ความน่าจะเป็น		ไม่มีนัยสำคัญ	ต่ำ	กลาง	สูง	สูงมาก
		Insignificant	Minor	Moderate	Major	Catastrophic
		1	2	3	4	5
ค่อนข้างแน่นอน	5					
น่าจะเกิด	4					
เป็นไปได้ที่จะเกิด	3					
ไม่น่าจะเกิด	2					
ยากที่จะเกิด	1					

แผนภูมิความเสี่ยงการจัดการความเสี่ยง (Risk Map)

Likelihood	1	2	3	4	5
	Highly Unlikely	Unlikely	Possible	Likely	High
5 Severe	สูง	สูง	สูงมาก	สูงมาก	สูงมาก
4 Significant	ปานกลาง	สูง	สูง	สูงมาก	สูงมาก
3 Moderate	ต่ำ	ปานกลาง	สูง	สูง	สูงมาก
2 Minor	ต่ำ	ต่ำ	ปานกลาง	สูง	สูงมาก
1 Negligible	ต่ำ	ต่ำ	ปานกลาง	สูง	สูง



ขั้นตอนที่ 4 การจัดทำแผนการจัดการความเสี่ยง (Risk Response)

การจัดทำแผนการจัดการความเสี่ยง หมายถึง การกำหนดแนวทางการดำเนินงานเพื่อลดโอกาสที่จะเกิดความเสี่ยง โดยนำผลจากการประเมินความเสี่ยงที่ได้จากขั้นตอนที่ 3 มาจัดทำแผนจัดการ/บริหารความเสี่ยงตามลำดับความสำคัญของความเสี่ยง โดยหน่วยงานเจ้าของความเสี่ยง ซึ่งเข้าใจความเสี่ยงที่เกี่ยวข้องกับหน่วยงานตนเองมากที่สุดเป็นผู้จัดทำแผนจัดการ/บริหารความเสี่ยงโดยวิเคราะห์หาวิธีการจัดการกับความเสี่ยงที่คาดว่าจะเกิดขึ้น วิธีการใดวิธีการหนึ่งหรือหลายวิธีรวมกันเพื่อลดโอกาสที่จะเกิดขึ้น และ/หรือลดความรุนแรงของผลกระทบให้อยู่ในระดับที่หน่วยงานยอมรับได้ และจัดทำเป็นแผนจัดการ/บริหารความเสี่ยงของหน่วยงานตนเอง

วิธีการจัดการความเสี่ยง

1. วิเคราะห์หาวิธีการจัดการกับความเสี่ยงที่คาดว่าจะเกิดขึ้น โดยมีแนวทางในการจัดการ/บริหารความเสี่ยงได้ 4 วิธี (4 T) ดังนี้

(1) การควบคุม/ ลด (treat) คือ การควบคุมความเสี่ยงหรือหาวิธีการบริหารความเสี่ยง เช่น ใช้เทคนิควิชาการทางวิศวกรรมหรือการกำหนดแผนฉุกเฉิน หรือการปรับปรุงแก้ไขกระบวนการดำเนินงาน เป็นต้น

(2) การโอนย้าย (transfer) คือ การถ่ายโอนความเสี่ยงหรือโอนย้ายความเสี่ยงให้ผู้อื่นรับผิดชอบ เช่น การทำประกันภัย หรือจ้างบุคคลภายนอกเป็นผู้ดำเนินการแทน เป็นต้น

(3) การหลีกเลี่ยง / กำจัด (terminate) คือ การกำจัดความเสี่ยงหรือหลีกเลี่ยงไม่ยอมรับความเสี่ยงนั้นเลย เช่น การเปลี่ยนวัตถุประสงค์หรือหยุดทำกิจกรรม เป็นต้น

(4) การยอมรับ (Take) เนื่องจากองค์กรอาจมีระบบควบคุมที่มีประสิทธิภาพหรือมีเงินทุนเพียงพอที่จะรองรับผลกระทบที่อาจเกิดขึ้นหรือระดับความเสี่ยงเหลืออยู่ในระดับที่ยอมรับได้ หรือการยอมรับให้มีความเสี่ยงเนื่องจากค่าใช้จ่ายในการบริหารความเสี่ยง โดยการสร้างระบบควบคุมอาจมีมูลค่าสูงกว่าผลลัพธ์ที่ได้ แต่ควรมีมาตรการติดตามและควบคุมดูแล

ทั้งนี้ การเลือกวิธีการจัดการความเสี่ยง ต้องพิจารณาเปรียบเทียบต้นทุนในการจัดการ/บริหารความเสี่ยงและความเสี่ยงภัยที่เกิดขึ้นด้วย

2. จัดทำแผนจัดการ/บริหารความเสี่ยงเพิ่มเติมโดยมีขั้นตอน ดังนี้

(1) ระบุวิธีการ มาตรการที่เป็นทางเลือกจากวิธีการจัดการความเสี่ยง (4 T) เพื่อให้ความเสี่ยงคงเหลืออยู่ในระดับที่ยอมรับได้ และสอดคล้องกับวัตถุประสงค์ที่กำหนดไว้

(2) ศึกษาเปรียบเทียบความเป็นไปได้และค่าใช้จ่ายของแต่ละทางเลือกตาม ข้อ (1) โดยคำนึงถึงความคุ้มค่าในการลงทุน ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงินโดยต้นทุนในการดำเนินการต้องไม่สูงกว่าความเสียหายที่คาดว่าจะเกิดขึ้น

(3) เลือกวิธีการที่ดีที่สุด โดยกำหนดผู้รับผิดชอบ/ ระยะเวลา/ งบประมาณพร้อมกำหนดแผนปฏิบัติการ



ขั้นตอนที่ 5 กิจกรรมการควบคุม (Control Activities)

กิจกรรมการควบคุม หมายถึง นโยบายและแนวทางการปฏิบัติงานในการควบคุมที่ฝ่ายบริหารกำหนดขึ้นเพื่อให้มั่นใจว่าแผนจัดการ/บริหารความเสี่ยงที่กำหนดขึ้นอย่างมีประสิทธิภาพมีการกำหนดผู้รับผิดชอบและระยะเวลาในการดำเนินงานได้อย่างชัดเจน และกิจกรรมการควบคุมนั้นก็เป็นวิธีการหนึ่งในการจัดการ/บริหารความเสี่ยง

ตัวอย่าง กิจกรรมการควบคุม

1. การควบคุมโดยการจัดทำนโยบายและวิธีปฏิบัติงาน
2. การสอบทานและการกำกับดูแลการปฏิบัติงาน
3. ระบบงานคอมพิวเตอร์และการควบคุมด้านคอมพิวเตอร์
4. การควบคุมทางกายภาพ
5. ดัชนีตัวชี้วัดผลการดำเนินงาน
6. การแบ่งแยกหน้าที่ความรับผิดชอบงาน

กิจกรรมการควบคุมที่จะเกิดประโยชน์มากที่สุดควรจะแทรกอยู่ในกระบวนการสามารถป้องกันและลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยต้นทุนในการดำเนินการต้องไม่สูงกว่าความเสียหายที่คาดว่าจะเกิดขึ้น

การกำหนดกิจกรรมการควบคุมอย่างชัดเจนจะทำให้แผนการจัดการบริหารความเสี่ยงเพิ่มเติมที่ได้จัดทำไว้บรรลุวัตถุประสงค์โดยจัดทำนโยบายและวิธีปฏิบัติเพิ่มเติม กำหนดผู้รับผิดชอบและระยะเวลาแล้วเสร็จอย่างชัดเจน ในบางกรณีอาจจัดทำกระบวนการควบคุมภายในเพิ่มเติมกำหนดผู้รับผิดชอบและระยะเวลาแล้วเสร็จอย่างชัดเจน ในบางกรณีอาจจัดทำกระบวนการควบคุมภายในเพิ่มเติม เช่น การสอบทาน การกำกับดูแล การแบ่งแยกหน้าที่งานเพิ่ม เป็นต้น

กิจกรรมการควบคุม เป็นองค์ประกอบหนึ่งของระบบการควบคุมภายในในลักษณะการเสนอแนะ (Suggestive Control) เพื่อปรับปรุงและพัฒนาระบบการดำเนินงานและระบบการควบคุมภายในให้เหมาะสมกับสถานการณ์ที่หน่วยงานต้องจัดทำให้มีขึ้นเพื่อลดความเสี่ยง และทำให้เกิดความคุ้มค่าตลอดจนให้ฝ่ายบริหารเกิดความมั่นใจในประสิทธิผลของระบบการควบคุมภายในที่มีอยู่

ขั้นตอนที่ 6 การติดตามและประเมินผล (Monitoring & Evaluation)

การติดตามและประเมินผล หมายถึง กระบวนการควบคุมคุณภาพการปฏิบัติงานและประเมินผล แผนการจัดการ/บริหารความเสี่ยงเพิ่มเติม หรือกิจกรรมการควบคุมที่วางไว้อย่างต่อเนื่องและสม่ำเสมอ โดยการติดตามในระหว่างการปฏิบัติงานและการประเมินผลเป็นครั้งคราวตามระยะเวลา เพื่อให้มั่นใจว่าการจัดการ/การบริหารความเสี่ยงมีประสิทธิภาพและประสิทธิผล จึงต้องมีรายงานความก้าวหน้า ปัญหา อุปสรรคของการจัดการ/บริหารความเสี่ยงเพื่อใช้เป็นแนวทางในการทบทวนหรือปรับปรุงแผนการจัดการ/บริหารความเสี่ยงต่อไป



รายงานที่ต้องจัดทำและขั้นตอนการรายงาน มีดังนี้

- แผนบริหารความเสี่ยง ซึ่งประกอบด้วย
 - 1) รายงานปัจจัยความเสี่ยงระดับความเสี่ยง
 - 2) การควบคุมที่มีอยู่การจัดการความเสี่ยงที่เหลือ
 - 3) หน่วยงาน/ ผู้รับผิดชอบความเสี่ยงหลังการควบคุม
- รายงานต่อผู้บริหารระดับสูงหรือคณะกรรมการบริษัท ซึ่งประกอบด้วย
 - 1) ความเสี่ยงที่คลาดเคลื่อนเกินกว่าที่ยอมรับได้
 - 2) ความเสี่ยงสูงสุด 5 ระดับ
 - 3) เหตุการณ์ที่แม้จะมีโอกาสต่ำ แต่จะมีผลต่อ
 - ความปลอดภัยต่อพนักงานหรือบุคคลอื่น
 - การกระทำผิดกฎหมาย
 - ผลเสียหายสำคัญต่อทรัพย์สิน การด้อยค่าของทรัพย์สิน
 - ชื่อเสียงของหน่วยงาน
 - การจัดทำงบและรายงานทางการเงินไม่เหมาะสม