นโยบายการบริหารความเสี่ยง

(Risk Management Policy)

มีผลบังคับใช้ตั้งแต่วันที่ 16 สิงหาคม 2566 เป็นต้นไป

สารบัญ

นโยบายการบริหารความเสี่ยง

หลักการและเหตุผล

บริษัท พรีไซซ คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทย่อย (“บริษัทฯ”) ตระหนักถึงความสำคัญของการบริหารความเสี่ยงขององค์กร ซึ่งเป็นส่วนหนึ่งของการกำกับดูแลกิจการที่ดี และเป็นการช่วยเพิ่มความยืดหยุ่น (Resilience) และความสามารถในการปรับตัว (Agility) ขององค์กรต่อการเปลี่ยนแปลงที่เกิดขึ้นอยู่ตลอดเวลา ไม่ว่าจะเป็นจากปัจจัยภายนอก เช่น การเมือง สภาวะเศรษฐกิจ หรือนวัตกรรมเทคโนโลยี ปัจจัยภายใน เช่น โครงสร้างองค์กร กระบวนการทำงาน หรือความพร้อมของบุคลากร เป็นต้น

การบริหารความเสี่ยงขององค์กรที่มีประสิทธิภาพจะทำให้บริษัทฯ สามารถดำเนินธุรกิจอย่างต่อเนื่อง บริหารจัดการผลกระทบเชิงลบของความเสี่ยงให้น้อยที่สุด และช่วยให้บริษัทฯสามารถระบุโอกาสในการเติบโตและแข่งขันเพื่อให้สามารถบรรลุเป้าหมายในการดำเนินงานและเติบโตอย่างยั่งยืน โดยบริษัทฯได้นำกรอบด้านการควบคุมภายในตามมาตรฐานสากลของ The Committee of Sponsoring Organizations of the Treadway Commission (COSO) และหลักการบริหารความเสี่ยงขององค์กร (Enterprise Risk Management) ตามกรอบการบริหารความความเสี่ยงของ COSO-ERM 2017 มาเป็นเครื่องมือในการพัฒนาการบริหารความเสี่ยงของบริษัทฯให้มีประสิทธิภาพและประสิทธิผลมากขึ้น

วัตถุประสงค์

1. เพื่อกำหนดกรอบและแนวทางการบริหารความเสี่ยงขององค์กร
2. เพื่อให้มั่นใจว่ามีการกำหนดหน้าที่ความรับผิดชอบในการควบคุมความเสี่ยงที่ได้ระบุไว้อย่างเหมาะสม ทั้งในระดับกรรมการ ผู้บริหารและพนักงาน

ขอบเขต

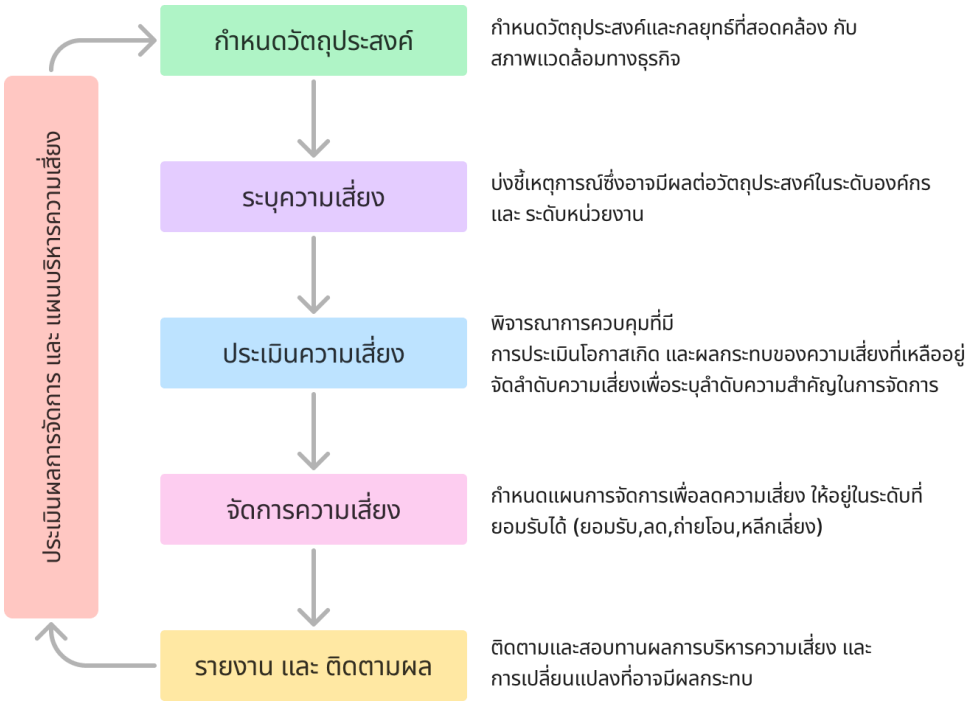
นโยบายฉบับนี้ให้มีผลบังคับใช้กับทุกการดำเนินงานรวมถึงกรรมการ ผู้บริหาร และพนักงานทุกคนของบริษัทฯ

คำนิยาม

- **ความเสี่ยง** หมายถึง เหตุการณ์หรือสถานการ์ความไม่แน่นอน ที่อาจเกิดขึ้นและมีผลกระทบในเชิงลบต่อการบรรลุวัตถุประสงค์และเป้าหมาย

- **การบริหารความเสี่ยงขององค์กร** (Enterprise Risk Management) หมายถึง การกำหนดนโยบาย โครงสร้าง หรือกระบวนการ เพื่อให้คณะกรรมการ ผู้บริหาร และบุคลากร นำไปปฏิบัติในการกำหนดกลยุทธ์และปฏิบัติงานทั่วทั้งองค์กร โดยกระบวนการบริหารความเสี่ยงจะช่วยให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้น ประเมินผลกระทบต่อองค์กร และกำหนดวิธีจัดการกับความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ เพื่อให้เกิดความเชื่อมั่นในระดับหนึ่งว่าการดำเนินการจะบรรลุตามวัตถุประสงค์/เป้าหมายที่กำหนดไว้
- **โอกาส** (Likelihood) หมายถึง โอกาสหรือความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้น
- **ผลกระทบ** (Impact) หมายถึง ผลที่ตามมาหรือผลของความเสี่ยง ความเสี่ยงหนึ่งอาจมีผลกระทบที่เป็นไปได้หลากหลายทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน ผลกระทบของความเสี่ยงอาจเป็นผลเชิงบวกหรือเชิงลบ ต่อกลยุทธ์หรือวัตถุประสงค์ทางธุรกิจขององค์กร
- **ระดับความเสี่ยงที่ยอมรับได้** (Risk Appetite) หมายถึง ระดับความเสี่ยงโดยรวมที่องค์กรยอมรับได้ เมื่อเกิดเหตุการณ์ความเสี่ยงขึ้นแล้ว ซึ่งเป็นปัจจัยสำคัญในการประเมินทางเลือกสำหรับการดำเนินธุรกิจและกำหนดกลยุทธ์ของบริษัทฯ เพื่อบรรลุตามวัตถุประสงค์/เป้าหมายที่กำหนดไว้

กระบวนการบริหารความเสี่ยง



บริษัทฯกำหนดกระบวนการบริหารความเสี่ยง โดยแบ่งออกเป็น 5 ขั้นตอน มีรายละเอียดดังนี้

1. **การกำหนดวัตถุประสงค์** สายธุรกิจและหน่วยงานต้องกำหนดวัตถุประสงค์และเป้าหมายการดำเนินงานที่สอดคล้องกับวิสัยทัศน์ พันธกิจ กลยุทธ์ และเป้าหมายโดยรวมของบริษัทฯ โดยต้องมีความชัดเจน สามารถวัดหรือประเมินผลได้
2. **การระบุความเสี่ยง** ระบุเหตุการณ์ความเสี่ยงหรือความไม่แน่นอนที่อาจเกิดขึ้น ที่ส่งผลกระทบต่อการบรรลุวัตถุประสงค์ของธุรกิจ ความเสี่ยงมีทั้งหมด 2 ระดับ คือระดับบริษัท และหน่วยงาน

   ประเภทความเสี่ยงแบ่งออกเป็น 5 ด้าน ดังนี้

   (1) **ความเสี่ยงด้านกลยุทธ์** (Strategic Risk) หมายถึง ความเสี่ยงที่เกิดจากการกำหนดกลยุทธ์ หรือนโยบายการบริหารงาน ที่ทำให้องค์กรไม่สามารถบรรลุวัตถุประสงค์และเพิ่มมูลค่าให้องค์กรได้ เช่น นโยบายไม่สอดคล้องกับความต้องการของผู้มีส่วนได้เสีย โครงสร้างองค์กรที่ปรับเปลี่ยน กลยุทธ์ แผนดำเนินงานอาจไม่เหมาะสมหรือไม่สอดคล้องกับปัจจัยและสภาพแวดล้อมต่างๆ ที่เกิดการเปลี่ยนแปลงไป เช่น ความผันผวนของเศรษฐกิจ ความรุนแรงของการแข่งขัน การเปลี่ยนแปลงของคู่ค้าทางธุรกิจ เป็นต้น

   (2) **ความเสี่ยงด้านการเงิน** (Financial Risk) หมายถึง ความเสี่ยงที่มีปัจจัยส่งผลกระทบทางด้านการเงินของบริษัท เช่น แผนการลงทุนไม่มีความชัดเจนเพียงพอที่จะนำไปใช้ในการวิเคราะห์เพื่อคาดการณ์ด้านการเงินได้ สภาพคล่องทางการเงิน อัตราแลกเปลี่ยน ดอกเบี้ย ไม่มีแหล่งรายได้ใหม่ เป็นต้น

   (3) **ความเสี่ยงด้านการปฏิบัติงาน** (Operational Risk) หมายถึง ความเสี่ยงที่จะเกิดความเสียหายต่างๆ อันเนื่องมาจากความไม่เพียงพอ หรือ ความบกพร่องของกระบวนการภายใน บุคลากร และระบบงานของบริษัท หรือจากเหตุการณ์ภายนอก เช่น โครงการล่าช้า ขาดอุปกรณ์หรือเครื่องมือที่มีประสิทธิภาพ ขาดการติดตามการบริหารสัญญา บุคลากรขาดแรงจูงใจในการปฏิบัติงาน การร้องเรียนจากชุมชนรอบข้าง เป็นต้น

   (4) **ความเสี่ยงด้านการปฏิบัติตามกฎหมาย กฎระเบียบ** (Compliance Risk) หมายถึง ความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หรือมาตรฐานที่เกี่ยวข้องกับการดำเนินงาน หรือกฎหมายที่มีอยู่ไม่เหมาะสมเป็นอุปสรรคต่อการปฏิบัติงาน นโยบายและวิธีการปฏิบัติงานที่องค์กรกำหนดขึ้นไม่สามารถปฏิบัติได้ เช่น ความสับสนในการเลือกกฎหมายหรือระเบียบที่จะบังคับใช้ เนื่องจากกฎหมายหรือระเบียบมีหลายฉบับที่สามารถอ้างถึง และบังคับใช้ในกรณีหนึ่งๆ การดำเนินการที่ขัดต่อกฎหมายหรือระเบียบที่เกี่ยวข้อง โดยขาดความระมัดระวังที่อาจทำให้องค์กรไม่ได้ปฏิบัติตามกฎหมาย

หรือ ระเบียบจากหน่วยงานกำกับดูแลภายนอก ตลอดจนระเบียบภายในขององค์กรเอง จนเกิดการทุจริตในองค์กร, ข้อพิพาททางกฎหมายกับลูกค้า/คู่ค้า เป็นต้น

(5) **ความเสี่ยงด้านระบบสารสนเทศและเทคโนโลยีสารสนเทศ** (Information System and Information Technology Risk) หมายถึง ความเสี่ยงที่เกิดจากความเป็นไปได้ที่จะเกิดเหตุการณ์ที่คาดหวังหรือไม่คาดหวัง อันเนื่องมาจากการนำเทคโนโลยีสารสนเทศมาใช้ ซึ่งมีผลกระทบถึงระบบงานและการปฏิบัติงาน โดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน ระบบงาน เหตุการณ์ภายนอก หรือคน (พนักงาน บุคคลภายนอก หรือลูกค้า) ซึ่งส่งผลกระทบต่อการดำเนินงาน โดยแบ่งออกเป็น 3 ประเภทดังนี้

I. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์หรืออุปกรณ์เครือข่ายชำรุด หรือเสื่อมสภาพตามอายุการใช้งาน

II. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ซึ่งอาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

III. ความเสี่ยงด้านสารสนเทศ (Information Risk) หมายถึง ความเสี่ยงที่ผู้ใช้ในองค์กรเข้าสู่ระบบสารสนเทศหรือใช้ข้อมูลต่างๆ ขององค์กรได้เกินกว่าสิทธิ์การเข้าถึงข้อมูลที่กำหนดไว้ หรือการถูกผู้ไม่หวังดี (Hacker) ขโมยข้อมูลหรือสร้างความเสียหายต่อระบบและข้อมูลสารสนเทศได้ หรือการถูกคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ ซึ่งอาจเกิดจากผู้ใช้งานใช้เครือข่ายขององค์กรเข้าถึงข้อมูลภายนอกที่มีไวรัส

3. **การประเมินความเสี่ยง** ประเมินความเสี่ยงที่อาจจะเกิดขึ้น โดยพิจารณาจากโอกาสที่อาจจะเกิด (Likelihood) และผลกระทบของความเสี่ยง (Impact) โดยหน่วยงานทุกระดับมีหน้าที่ประเมินความเสี่ยงในแต่ละด้านที่ระบุไว้เบื้องต้น เกณฑ์ที่ใช้ในการประเมินความเสี่ยงควรสะท้อนถึงคุณค่า วัตถุประสงค์และทรัพยากรขององค์กร ในการประเมินความเสี่ยงบริษัทฯ โดยบริษัทฯใช้ตารางการวิเคราะห์ความเสี่ยง (Risk Matrix) ดังภาพ

ตารางการวิเคราะห์ความเสี่ยง (Risk Matrix)					
โอกาสเกิด / ผลกระทบ	1 น้อยมาก	2 น้อย	3 ปานกลาง	4 สูง	5 สูงมาก
5 สูงมาก	ปานกลาง	สูง	สูง	สูงมาก	สูงมาก
4 สูง	ปานกลาง	ปานกลาง	สูง	สูงมาก	สูงมาก
3 ปานกลาง	ต่ำ	ปานกลาง	สูง	สูง	สูง
2 น้อย	ต่ำ	ปานกลาง	ปานกลาง	ปานกลาง	สูง
1 น้อยมาก	ต่ำ	ต่ำ	ต่ำ	ปานกลาง	ปานกลาง

ระดับความเสี่ยง	ระดับคะแนน	แทนด้วย	ความหมาย
สูงมาก	16 - 25		ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ ต้องมีการจัดการความเสี่ยงอย่างเร่งด่วน (จัดการทันที) เพื่อให้อยู่ในระดับที่ยอมรับได้
สูง	9 - 15		ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ ต้องมีการจัดการความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
ปานกลาง	4 – 8		ระดับความเสี่ยงที่ยอมรับได้ แต่ต้องมีการควบคุมการดำเนินการอย่างสม่ำเสมอและต่อเนื่อง เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ไม่สามารถยอมรับได้
ต่ำ	1 - 3		ระดับความเสี่ยงที่ยอมรับได้ โดยไม่ต้องมีการควบคุมหรือการจัดการความเสี่ยงเพิ่มเติม แต่ต้องติดตามอย่างสม่ำเสมอ

หมายเหตุ บริษัทฯกำหนดหลักเกณฑ์การพิจารณาความเสี่ยงในกรณีพิเศษ กล่าวคือความเสี่ยงใดที่ประเมินแล้ว ระดับคะแนนในส่วนของผลกระทบ (Impact) ตามเกณฑ์เท่ากับ 5 แม้ว่าระดับคะแนนในส่วนของโอกาสเกิด (Likelihood) จะเป็นค่าใด ซึ่งไม่ส่งผลให้ระดับความเสี่ยงนั้นอยู่ในระดับความเสี่ยงที่ไม่สามารถยอมรับได้ตามตารางอธิบายข้างต้น หน่วยงานหรือบริษัทเจ้าของความเสี่ยงก็ยังคงต้องกำหนดมาตรการจัดการเพื่อลดระดับคะแนนในส่วนของผลกระทบของความเสี่ยงดังกล่าวให้น้อยกว่า 5 เสมอ

4. **การจัดการความเสี่ยง** ตอบสนองต่อความเสี่ยง กำหนดมาตราการจัดการเพื่อให้สามารถจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (Risk Appetite) โดยคำนึงถึงต้นทุนและผลประโยชน์ที่จะได้รับจากการดำเนินการนั้นๆ และต้องประเมินว่าปัจจุบันการจัดการความเสี่ยงเพียงพอหรือไม่ ทั้งประสิทธิภาพในการลดโอกาสเกิดความเสี่ยง และผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงต่างๆ หากไม่มีการจัดการความเสี่ยง หรือการจัดการในปัจจุบันไม่เพียงพอ
5. **รายงานและติดตามผล** ติดตามและรายงานผลเพื่อมั่นใจได้ว่าการจัดการความเสี่ยงมีประสิทธิภาพและเหมาะสม หรือควรปรับเปลี่ยน หากแผนนั้นไม่มีประสิทธิภาพเพียงพอ โดยกำหนดข้อมูลที่ต้องติดตาม และความถี่ในการสอบทาน และควรกำหนดให้มีการประเมินความเสี่ยงอย่างน้อยปีละ 2 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อประเมินว่าความเสี่ยงใดอยู่ในระดับที่ยอมรับได้แล้วหรือมีความเสี่ยงใหม่เพิ่มขึ้น

หน้าที่ความรับผิดชอบ

1. คณะกรรมการบริษัท (Board of Director) มีหน้าที่ความรับผิดชอบโดยรวมในการกำกับดูแลบริหารความเสี่ยงขององค์กร
2. คณะกรรมการบริหาร (Executive Committee) มีหน้าที่ความรับผิดชอบในการพิจารณาและสอบทานการบริหารความเสี่ยงและระบบควบคุมภายในของบริษัท
3. คณะกรรมการตรวจสอบ (Audit Committee) ช่วยสนับสนุนคณะกรรมการบริษัทในการปฏิบัติหน้าที่ด้านการบริหารความเสี่ยง โดยสอบทานให้มั่นใจว่าระบบการบริหารความเสี่ยงมีความเหมาะสม และมีประสิทธิผล
4. ฝ่ายจัดการมีความรับผิดชอบในการดำเนินการตามนโยบายฉบับนี้ และกำกับดูแลให้มีการปฏิบัติตามอย่างต่อเนื่อง ผ่านหน่วยงาน Risk, Compliance, Remediation and Resiliency Management
5. คณะทำงานบริหารความเสี่ยง ซึ่งแต่งตั้งโดยคณะกรรมการบริหาร (Executive Committee) มีหน้าที่ทำให้เชื่อมั่นได้ว่าความเสี่ยงที่สำคัญ ได้รับการระบุและประเมินอย่างสม่ำเสมอ รวมทั้งได้มีการกำหนดมาตรการจัดการความเสี่ยงที่มีประสิทธิผลไว้ โดยรับผิดชอบในเรื่องต่างๆ ดังนี้

- จัดทำนโยบายการบริหารความเสี่ยง กลยุทธ์และหลักเกณฑ์ในการบริหารความเสี่ยง เพื่อเสนอให้คณะกรรมการบริหาร และ/หรือ คณะกรรมการบริษัทพิจารณา
- สอบทานความเสี่ยงและแนวทางการจัดการความเสี่ยงของบริษัทฯ ตามที่หน่วยงาน เจ้าของความเสี่ยงได้ประเมินไว้ รวมทั้งให้ข้อเสนอแนะเพื่อปรับปรุงแก้ไข
- กำกับดูแลความมีประสิทธิผลของกระบวนการบริหารความเสี่ยงของบริษัทฯ โดยการติดตามและสอบทานอย่างต่อเนื่อง
- รายงานผลการบริหารความเสี่ยงต่อคณะกรรมการบริหาร คณะกรรมการตรวจสอบ และ/หรือ คณะกรรมการบริษัทพิจารณา
- สอบทานนโยบาย กรอบและกระบวนการบริหารความเสี่ยงเป็นประจำทุกปี

6. ผู้ตรวจสอบภายในมีหน้าที่ความรับผิดชอบในการสอบทานประสิทธิผลของการควบคุมภายในและการบริหารความเสี่ยงผ่านการตรวจสอบภายในประจำปี ซึ่งเป็นการตรวจสอบกระบวนการทางธุรกิจที่สำคัญตามปัจจัยเสี่ยง รวมทั้งติดตามการปรับปรุงแก้ไขข้อบกพร่องที่ตรวจพบโดยรายงานผลให้คณะกรรมการตรวจสอบได้รับทราบ