นโยบายการบริหารความเสี่ยง

(Risk Management Policy)

มีผลบังคับใช้ตั้งแต่ วันที่ 19 พฤษภาคม 2568

นโยบายการบริหารความเสี่ยง (Risk Management Policy)

หลักการและเหตุผล

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

การบริหารความเสี่ยงขององค์กรที่มีประสิทธิภาพ จะทำให้บริษัทฯสามารถดำเนินธุรกิจอย่างต่อเนื่อง บริหารจัดการผลกระทบเชิงลบของความเสี่ยงให้เกิดน้อยที่สุด และช่วยให้บริษัทฯสามารถระบุโอกาสในการเติบโตและแข่งขัน เพื่อให้บรรลุเป้าหมายในการดำเนินงานและเติบโตอย่างยั่งยืน โดยบริษัทฯได้นำกรอบด้านการบริหารความเสี่ยงขององค์กร (Enterprise Risk Management) ตามกรอบการบริหารความความเสี่ยงของ COSO-ERM 2017 และการควบคุมภายในตามมาตรฐานสากลของ The Committee of Sponsoring Organizations of the Treadway Commission (COSO) มาเป็นเครื่องมือในการพัฒนาการบริหารความเสี่ยงของบริษัทฯให้มีประสิทธิภาพและประสิทธิผลมากขึ้น

วัตถุประสงค์

1. เพื่อกำหนดกรอบและแนวทางการบริหารความเสี่ยงขององค์กร
2. เพื่อให้มั่นใจว่ามีการกำหนดหน้าที่ความรับผิดชอบในการควบคุมความเสี่ยงที่ได้ระบุไว้อย่างเหมาะสม ทั้งในระดับกรรมการ ผู้บริหาร และพนักงาน

ขอบเขต

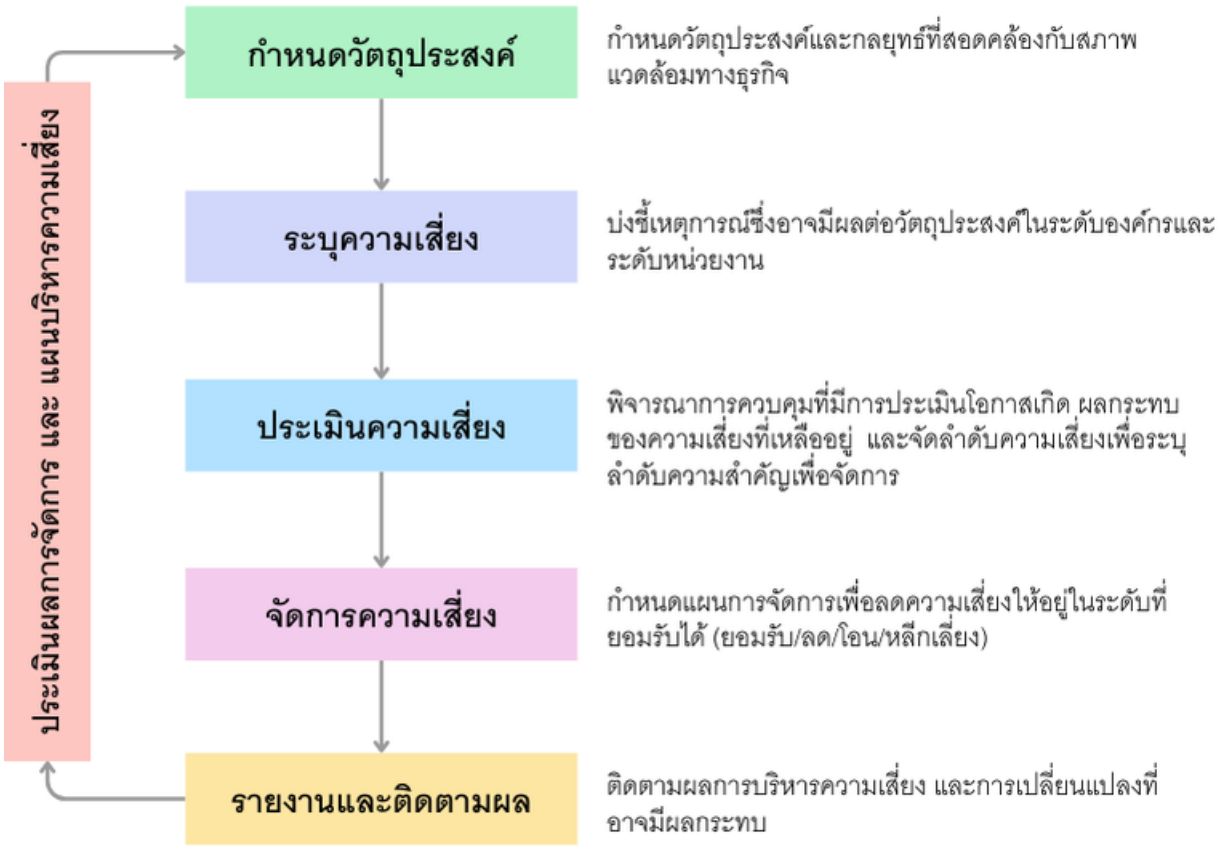
นโยบายฉบับนี้ให้มีผลบังคับใช้กับทุกการดำเนินงาน รวมถึงผู้เกี่ยวข้องทุกระดับตั้งแต่กรรมการ ผู้บริหาร พนักงานของบริษัทและบริษัทย่อย

คำนิยาม

- **ความเสี่ยง** หมายถึง เหตุการณ์หรือสถานการ์ความไม่แน่นอน ที่อาจเกิดขึ้นและมีผลกระทบต่อการบรรลุวัตถุประสงค์และเป้าหมาย

- **การบริหารความเสี่ยงขององค์กร** (Enterprise Risk Management) หมายถึง การกำหนดนโยบาย โครงสร้าง หรือขั้นตอนกระบวนการ วิธีการ เพื่อให้คณะกรรมการ ผู้บริหาร และพนักงานปฏิบัติงานต่างๆ ทั้งในระดับการกำหนดกลยุทธ์และปฏิบัติงานโดยทั่วไป กระบวนการบริหารความเสี่ยงจะช่วยให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้น ประเมินผลกระทบต่อองค์กร และกำหนดวิธีจัดการกับความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ เพื่อให้เกิดความเชื่อมั่นในระดับหนึ่งว่าการดำเนินงานจะบรรลุตามวัตถุประสงค์หรือเป้าหมายที่กำหนดไว้
- **โอกาส** (Likelihood) หมายถึง โอกาสหรือความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้น
- **ผลกระทบ** (Impact) หมายถึง ผลที่ตามมาหรือผลของความเสี่ยง โดยความเสี่ยงหนึ่งอาจมีผลกระทบที่เป็นไปได้หลากหลายทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน ผลกระทบของความเสี่ยงอาจเป็นผลเชิงบวกหรือเชิงลบ ต่อกลยุทธ์หรือวัตถุประสงค์ทางธุรกิจขององค์กร
- **ระดับความเสี่ยงที่ยอมรับได้** (Risk Appetite) หมายถึง ระดับความเสี่ยงโดยรวมที่องค์กรยอมรับได้เมื่อเกิดเหตุการณ์ความเสี่ยงขึ้น ซึ่งเป็นปัจจัยสำคัญในการประเมินทางเลือกสำหรับการดำเนินธุรกิจและการกำหนดกลยุทธ์เพื่อบรรลุตามวัตถุประสงค์หรือเป้าหมายที่กำหนดไว้

กระบวนการบริหารความเสี่ยง



บริษัทฯกำหนดกระบวนการบริหารความเสี่ยง โดยแบ่งออกเป็น 5 ขั้นตอน มีรายละเอียดดังนี้

1. **การกำหนดวัตถุประสงค์** คือการที่สายธุรกิจและหน่วยงานทุกระดับต้องกำหนดวัตถุประสงค์หรือเป้าหมายการดำเนินงานที่สอดคล้องกับวิสัยทัศน์ พันธกิจ กลยุทธ์ และเป้าหมายโดยรวมของบริษัทฯ โดยต้องมีความชัดเจน สามารถวัดผล ประเมินผลได้

2. **การระบุประเด็นความเสี่ยง** คือการระบุเหตุการณ์ความเสี่ยงหรือความไม่แน่นอนที่อาจเกิดขึ้น ที่ส่งผลกระทบต่อการบรรลุวัตถุประสงค์ของธุรกิจ โดยกำหนดให้มีการบริหารความเสี่ยงอย่างน้อย 2 ระดับ คือ 1) ระดับบริษัท 2) ระดับหน่วยงาน/กระบวนการ/โครงการ (ตามความเหมาะสม)

   ประเภทความเสี่ยงแบ่งออกเป็น 5 ด้าน ดังนี้

   (1) **ความเสี่ยงด้านกลยุทธ์** (Strategic Risk) หมายถึง ความเสี่ยงที่เกิดจากการกำหนดกลยุทธ์ หรือนโยบายการบริหารงานที่ทำให้องค์กรอาจไม่สามารถบรรลุวัตถุประสงค์และเพิ่มมูลค่าได้ เช่น นโยบายไม่สอดคล้องกับความต้องการของผู้มีส่วนได้เสีย โครงสร้างองค์กรอาจทำให้เป็นการปรับเปลี่ยนกลยุทธ์ แผนดำเนินงานอาจไม่เหมาะสมหรือไม่สอดคล้องกับปัจจัยและสภาพแวดล้อมต่างๆ ที่เกิดการเปลี่ยนแปลงไป เช่น ความผันผวนของเศรษฐกิจ ความรุนแรงของการแข่งขัน การเปลี่ยนแปลงของคู่ค้าทางธุรกิจ เป็นต้น

   (2) **ความเสี่ยงด้านการเงิน** (Financial Risk) หมายถึง ความเสี่ยงที่มีปัจจัยส่งผลกระทบทางด้านการเงินของบริษัท เช่น แผนการลงทุนไม่มีความชัดเจนเพียงพอที่จะนำไปใช้ในการวิเคราะห์เพื่อคาดการณ์ด้านการเงินได้ สภาพคล่องทางการเงิน อัตราแลกเปลี่ยน อัตราดอกเบี้ย การไม่มีแหล่งรายได้ใหม่ เป็นต้น

   (3) **ความเสี่ยงด้านการปฏิบัติงาน** (Operational Risk) หมายถึง ความเสี่ยงที่จะเกิดความเสียหายต่างๆ อันเนื่องมาจากความไม่เพียงพอหรือความบกพร่องของกระบวนการภายใน บุคลากร และระบบงานของบริษัท รวมถึงจากเหตุการณ์ภายนอก เช่น โครงการล่าช้า การใช้อุปกรณ์หรือเครื่องมือที่ไม่มีประสิทธิภาพเพียงพอ การติดตามการบริหารสัญญาผิดพลาด บุคลากรไม่มีแรงจูงใจในการปฏิบัติงาน การร้องเรียนจากชุมชนรอบข้าง เป็นต้น

   (4) **ความเสี่ยงด้านการปฏิบัติตามกฎหมาย กฎระเบียบ** (Compliance Risk) หมายถึง ความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หรือมาตรฐานที่เกี่ยวข้องกับการดำเนินงาน หรือกฎหมายที่มีอยู่ไม่เหมาะสมเป็นอุปสรรคต่อการปฏิบัติงาน นโยบายและวิธีการปฏิบัติงานที่องค์กรกำหนดขึ้นไม่สามารถปฏิบัติได้ เช่น ความสับสนในการเลือกกฎหมายหรือระเบียบที่จะบังคับใช้เนื่องจากกฎหมายหรือระเบียบมีหลายฉบับที่สามารถอ้างถึง และบังคับใช้ในกรณีหนึ่งๆ การดำเนินงาดที่ขัดต่อกฎหมาย/ระเบียบที่เกี่ยวข้องโดยขาดความระมัดระวัง

อาจทำให้ผู้ปฏิบัติงานไม่ได้ปฏิบัติตามกฎหมาย/ระเบียบจากหน่วยงานกำกับดูแลภายนอก ตลอดจนระเบียบภายในขององค์กรเอง

(5) **ความเสี่ยงด้านระบบสารสนเทศและเทคโนโลยีสารสนเทศ** (Information System and Information Technology Risk) หมายถึง ความเสี่ยงที่เกิดจากความเป็นไปได้ที่จะเกิดเหตุการณ์ที่คาดหวังหรือไม่คาดหวัง อันเนื่องมาจากการนำเทคโนโลยีสารสนเทศมาใช้ ซึ่งมีผลกระทบถึงระบบงาน โดยแบ่งออกเป็น 3 ประเภทดังนี้

- ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์หรืออุปกรณ์เครือข่าย ชำรุด/เสื่อมสภาพตามอายุการใช้งาน
- ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของซอฟต์แวร์ต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ
- ความเสี่ยงด้านสารสนเทศ (Information Risk) หมายถึง ความเสี่ยงที่ผู้ใช้ในองค์กรเข้าสู่ระบบสารสนเทศหรือใช้ข้อมูลต่างๆ ขององค์กรได้เกินกว่าสิทธิ์การเข้าถึงข้อมูลที่กำหนดไว้ หรือการถูกผู้ไม่หวังดี (Hacker) ขโมยข้อมูลหรือสร้างความเสียหายต่อระบบคอมพิวเตอร์และข้อมูลสารสนเทศได้

อย่างไรก็ดี เนื่องจากบริษัทให้ความสำคัญกับการบริหารความเสี่ยงเพื่อการดำเนินธุรกิจให้เติบโตอย่างยั่งยืน กระบวนการบริหารความเสี่ยงจะต้องไม่จำกัดเพียงเพื่อบรรลุวัตถุประสงค์หรือเป้าหมายเชิงเศรษฐกิจ ผู้ที่เกี่ยวข้องทุกฝ่ายจะต้องพิจารณาความเสี่ยงในหลากหลายมิติ โดยจะต้องพิจารณาให้ครอบคลุมถึงมิติสิ่งแวดล้อม, สังคม/ชุมชน และการกำกับดูแล ซึ่งรวมถึงความเสี่ยงที่อาจจะเกิดการทุจริตคอร์รัปชั่น และการละเมิดสิทธิมนุษยชนในกระบวนการทำงานของบริษัทฯ ด้วย

3. **การประเมินความเสี่ยง** คือการประเมินความมีนัยสำคัญของประเด็นความเสี่ยง โดยพิจารณาจากโอกาสที่อาจจะเกิด (Likelihood) และผลกระทบของความเสี่ยง (Impact) โดยผู้ที่เกี่ยวข้องมีหน้าที่ประเมินความเสี่ยงในแต่ละประเด็นที่ระบุในเบื้องต้น โดยเกณฑ์ที่ใช้ในการประเมินความเสี่ยงควรสะท้อนถึงคุณค่า วัตถุประสงค์ และทรัพยากรของบริษัทฯ โดยใช้ตารางการวิเคราะห์ความเสี่ยง(Risk Matrix) ดังภาพ

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

ระดับ	แทนด้วย	ความหมาย
สูงมาก		ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ ต้องมีการจัดการความเสี่ยงอย่างเร่งด่วน (จัดการทันที) เพื่อให้อยู่ในระดับที่ยอมรับได้
สูง		ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ ต้องมีการจัดการความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
ปานกลาง		ระดับความเสี่ยงที่ยอมรับได้ แต่ต้องมีการควบคุมการดำเนินการอย่างสม่ำเสมอและต่อเนื่อง เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ไม่สามารถยอมรับได้
ต่ำ		ระดับความเสี่ยงที่ยอมรับได้ โดยไม่ต้องมีการควบคุมหรือการจัดการความเสี่ยงเพิ่มเติม แต่ต้องติดตามอย่างสม่ำเสมอ

หมายเหตุ บริษัทฯ กำหนดหลักเกณฑ์การพิจารณาความเสี่ยงในกรณีพิเศษ กล่าวคือความเสี่ยงใดที่ประเมินแล้ว ระดับคะแนนในส่วนของผลกระทบ (Impact) ตามเกณฑ์เท่ากับ 4 แม้ว่าระดับคะแนนในส่วนของโอกาสเกิด (Likelihood) จะเป็นค่าใด ซึ่งไม่ส่งผลให้ระดับความเสี่ยงนั้นอยู่ในระดับความเสี่ยงที่ไม่สามารถยอมรับได้ตามตารางอธิบายข้างต้น หน่วยงานหรือบริษัทเจ้าของความเสี่ยงยังคงต้องกำหนดมาตรการจัดการเพื่อลดระดับของผลกระทบ (Impact) ของความเสี่ยงดังกล่าวให้น้อยกว่า 4 เสมอ

4. **การจัดการความเสี่ยง** คือการตอบสนองต่อความเสี่ยงโดยการกำหนดมาตราการจัดการ เพื่อให้สามารถจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (Risk Appetite) ให้คำนึงถึงต้นทุนและผลประโยชน์ที่จะได้รับจากการดำเนินการนั้นๆ และต้องประเมินด้วยว่าปัจจุบันการจัดการความเสี่ยงเพียงพอหรือไม่ทั้งประสิทธิภาพในการลดโอกาสเกิด (Likelihood) และผลกระทบ (Impact) ที่อาจเกิดขึ้นจากความเสี่ยงต่างๆ หากความเสี่ยงใดยังไม่มีการจัดการหรือการจัดการปัจจุบันไม่เพียงพอที่จะทำให้ความเสี่ยงให้อยู่ระดับที่ยอมรับได้ ให้กำหนดมาตรการจัดการเพิ่มเติมเพื่อจัดการความเสี่ยง โดยมาตรการจัดการเพิ่มเติมดังกล่าวจะต้องสามารถลดโอกาสเกิด (Likelihood) หรือผลกระทบ (Impact) ที่อาจเกิดขึ้นสอดคล้องสำหรับความเสี่ยงนั้นๆ

5. **การติดตามและรายงานผล** คือการติดตามและรายงานผลการบริหารความเสี่ยงต่อผู้บริหารระดับสูง คณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการบริษัท (แล้วแต่กรณี) เพื่อติดตามให้มั่นใจได้อย่างสมเหตุสมผลว่า มาตรการจัดการความเสี่ยงที่กำหนดไว้สามารถดำเนินไปได้อย่างมีประสิทธิภาพเหมาะสมหรือควรปรับเปลี่ยน โดยบริษัทกำหนดให้มีการติดตามและรายงานผลการบริหารความเสี่ยงต่อคณะกรรมการบริษัทฯ อย่างน้อยปีละ 2 ครั้ง เพื่อติดตามสถานะของความเสี่ยงขององค์กรว่า ความเสี่ยงใดอยู่ในระดับที่ยอมรับได้ ความเสี่ยงใดอยู่ในระหว่างดำเนินการ หรือมีความเสี่ยงใดเกิดใหม่เพิ่มขึ้น

หน้าที่ความรับผิดชอบ

1. คณะกรรมการบริษัท (Board of Director) อนุมัตินโยบายบริหารความเสี่ยง และการกำกับดูแลการบริหารความเสี่ยงในภาพรวมขององค์กร
2. คณะกรรมการบริหารความเสี่ยง (Risk Management Committee) รับผิดชอบในการ
    - พิจารณาทบทวนนโยบายการบริหารความเสี่ยง ก่อนเสนอให้คณะกรรมการบริษัทอนุมัติ
    - กำกับดูแล สนับสนุน ให้บริษัทฯมีกระบวนการบริหารความเสี่ยงอย่างต่อเนื่องทั่วทั้งองค์กร
    - ติดตามให้ฝ่ายจัดการมีการจัดทำและดำเนินการตามแผนบริหารความเสี่ยง พร้อมทั้งให้ความเห็นและคำแนะนำการปรับปรุง เพื่อจัดการความเสี่ยงอย่างเหมาะสม
3. คณะกรรมการตรวจสอบ (Audit Committee) สนับสนุนคณะกรรมการบริษัทในการปฏิบัติหน้าที่ด้านการบริหารความเสี่ยง โดยการสอบทานให้มั่นใจได้อย่างสมเหตุสมผลว่าระบบการบริหารความเสี่ยงของบริษัทฯ มีความเหมาะสม มีประสิทธิภาพและประสิทธิผล
4. ผู้บริหารระดับสูงมีหน้าที่สำคัญในการดำเนินกระบวนการบริหารความเสี่ยงให้เกิดขึ้นในองค์กร โดยสร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับการบริหารความเสี่ยง ติดตามผลการดำเนินงานและจัดสรรทรัพยากรเพื่อการบริหารความเสี่ยงของบริษัทฯเป็นไปอย่างมีประสิทธิภาพ ประสิทธิผล และต่อเนื่อง

พร้อมทั้งรายงานผลการบริหารความเสี่ยงต่อคณะกรรมการบริหารความเสี่ยงและคณะกรรมการบริษัทอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าบริษัทฯ สามารถจัดการกับความเสี่ยง และจะสามารถบรรลุเป้าหมายทางธุรกิจได้อย่างยั่งยืน

5. คณะทำงาน Risk and Compliance Management มีหน้าที่ติดตามสนับสนุนการบริหารความเสี่ยงของผู้บริหารระดับสูงและคณะกรรมการบริษัท โดยรับผิดชอบดำเนินการในเรื่องต่างๆ ดังนี้
   - ทบทวนนโยบายการบริหารความเสี่ยงขององค์กร เสนอแนวทางพัฒนากระบวนการ/หลักเกณฑ์การบริหารความเสี่ยง เพื่อให้คณะกรรมการบริหารความเสี่ยงเห็นชอบ ก่อนเสนอคณะกรรมการบริษัทพิจารณาอนุมัติ
   - ทบทวนประเด็นความเสี่ยงและแนวทางการจัดการความเสี่ยงที่สำคัญ ตามที่บริษัทหรือหน่วยงานเจ้าของความเสี่ยงได้ประเมินไว้
   - สื่อสารกระบวนการ/หลักเกณฑ์การบริหารความเสี่ยงที่บริษัทกำหนด เพื่อให้เกิดการนำไปปฏิบัติเป็นแนวทางเดียวกันทั่วทั้งองค์กร
   - ติดตามสนับสนุนให้เกิดการบริหารจัดการความเสี่ยงอย่างต่อเนื่อง
6. ผู้บริหารและพนักงานทุกระดับ มีหน้าที่รับผิดชอบในการปฏิบัติตามนโยบายฉบับนี้
7. ผู้ตรวจสอบภายใน (Internal Audit) มีหน้าที่รับผิดชอบในการสอบทานประสิทธิภาพ/ประสิทธิผลของการบริหารความเสี่ยงและการควบคุมภายในผ่านการตรวจสอบภายในประจำปี ซึ่งเป็นการตรวจสอบกระบวนการทางธุรกิจที่สำคัญตามปัจจัยเสี่ยง (Risk based Audit) รวมทั้งติดตามการปรับปรุงแก้ไขข้อบกพร่องที่ตรวจพบรายงานต่อคณะกรรมการตรวจสอบทราบ