



ประกาศหน่วยงานบริหารความเสี่ยง

ที่ 002/2567

เรื่อง นโยบายการบริหารความเสี่ยงองค์กร

(ฉบับแก้ไข ประจำปี 2567)

.....

อ้างอิงจากการประชุมคณะกรรมการบริษัท ครั้งที่ 2/2567 เมื่อวันที่ 26 มีนาคม พ.ศ. 2567 ได้พิจารณาและมีมติอนุมัติการทบทวนและปรับปรุงนโยบายการบริหารความเสี่ยงองค์กร (ฉบับแก้ไข ประจำปี 2567) โดยให้ยกเลิก “นโยบายการบริหารความเสี่ยงองค์กร (ฉบับแก้ไขครั้งที่ 1 พ.ศ. 2564) และให้ใช้นโยบายนี้แทน

ดังนั้นเพื่อเป็นมาตรฐาน กำหนดแนวทาง หลักเกณฑ์ แนวปฏิบัติ บังคับใช้กับพนักงานผู้มีหน้าที่เกี่ยวข้องทั้งโดยตรง และทางอ้อม จึงประกาศให้ทราบโดยทั่วกัน โดยให้มีผลบังคับใช้นับตั้งแต่วันที่ได้รับอนุมัติเป็นต้นไป

ประกาศ ณ วันที่ 27 มีนาคม 2567

深田裕司

(นายยูจิ ฟุคาคะ)

ประธานเจ้าหน้าที่บริหาร

บริษัท ไอรา แอนด์ ไอฟูล จำกัด (มหาชน)



AIRA & AIFUL Public Company Limited

90 CW Tower, 33rd, 34th Floor, unit B3301-2, B3401-2, Ratchadapisek Road, Huai Khwang Sub-district, Huai Khwang District, Bangkok 10310
Registration Number: 0107557000489

**นโยบายการบริหารความเสี่ยงองค์กร
บริษัท ไอรา แอนด์ ไอฟูล จำกัด (มหาชน)
(ฉบับทบทวน ปี 2567)**



นโยบายการบริหารความเสี่ยงองค์กร
(Enterprise Risk Management Policy)
(ฉบับทบทวน ปี 2567)

ก. เหตุผลในการออกนโยบาย

บริษัท ไออาร์ แอนด์ ไอฟูล จำกัด (มหาชน) “บริษัท” เป็นผู้ให้บริการด้านสินเชื่อส่วนบุคคลด้วยวิสัยทัศน์ของบริษัทที่จะเป็นบริษัทสินเชื่อส่วนบุคคลที่เติบโตเร็วที่สุดในประเทศไทยควบคู่ไปกับการเติบโตอย่างมีประสิทธิภาพ และส่งเสริมการมีส่วนร่วมกับสังคมผ่านกิจกรรมของบริษัทด้วยความจริงจังตามค่านิยมองค์กร

จากการดำเนินงานในปัจจุบันของบริษัทที่เติบโตขึ้น และเผชิญกับการเปลี่ยนแปลงอยู่ตลอดเวลา ทั้งจากปัจจัยภายนอก ไม่ว่าจะเป็นการเปลี่ยนแปลงด้านสถานะเศรษฐกิจ การเมือง ตลอดจนการพัฒนาของเทคโนโลยีสารสนเทศ และสถานะการทำธุรกรรมในตลาดภายนอก รวมตลอดถึงปัจจัยภายใน เช่น การเปลี่ยนแปลง ปรับปรุงการดำเนินงานตามสถานะการเปลี่ยนแปลง การพัฒนากลยุทธ์เพื่อพัฒนาแผนการดำเนินงานของบริษัท การปรับโครงสร้างองค์กร และการบริหารจัดการข้อมูลของบริษัท เป็นต้น ซึ่งการเปลี่ยนแปลงและพัฒนาจากปัจจัยดังกล่าว อาจก่อให้เกิดความเสี่ยงต่อการดำเนินธุรกิจขององค์กร

บริษัทตระหนักถึงความสำคัญของการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นกับองค์กรดังกล่าว เพื่อให้เกิดความเชื่อมั่นและก้าวไปสู่การควบคุม กำกับดูแลที่มีประสิทธิภาพ นอกจากนี้ยังเป็นการสร้างความตระหนักรู้ถึงการบริหารความเสี่ยง การดำเนินงานบนพื้นฐานการบริหารความเสี่ยงที่ดี ลดอุปสรรค ป้องกันความเสียหายของทรัพยากรต่างๆ อันอาจเกิดจากความเสี่ยง เป็นต้น ทั้งนี้เพื่อให้พนักงานของบริษัทตระหนัก และให้ถือเป็นความรับผิดชอบของพนักงานโดยทั่วกัน

ด้วยเหตุนี้ บริษัทจึงให้ความสำคัญกับการบริหารความเสี่ยงและการจัดการความเสี่ยงโดยสนับสนุนให้บุคลากรทุกหน่วยงานทั่วทั้งบริษัท ได้มีส่วนร่วมในการคิด วิเคราะห์ และคาดการณ์ถึงเหตุการณ์หรือความเสี่ยงที่อาจจะเกิดขึ้น รวมทั้งการระบุแนวทางในการจัดการกับความเสี่ยงดังกล่าว ให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้ เพื่อช่วยให้องค์กรบรรลุวัตถุประสงค์ และเป้าหมายในการสร้างผลตอบแทนสูงสุด สร้างความเชื่อมั่นต่อผู้ถือหุ้นและผู้มีส่วนได้เสียในระยะยาว ตามกรอบวิสัยทัศน์และพันธกิจขององค์กร ภายใต้หลักบรรษัทภิบาลและจรรยาบรรณธุรกิจ เพื่อให้บริษัทเติบโตอย่างยั่งยืนต่อไป

ข. วัตถุประสงค์

1) เพื่อนำระบบการบริหารความเสี่ยงมาปฏิบัติใช้ในแนวทางเดียวกันทั่วทั้งองค์กร และกำหนดให้การบริหารความเสี่ยงเป็นส่วนหนึ่งในการตัดสินใจ การกำหนดกลยุทธ์ แผนงาน และการดำเนินงานของบริษัท

2) เพื่อกำหนดแนวทางการบริหารจัดการความเสี่ยงที่เหลืออยู่ ให้อยู่ในระดับที่ยอมรับได้ขององค์กร โดยพิจารณามาตรการที่จะลดโอกาส และ/หรือ ผลกระทบจากความเสี่ยงที่อาจจะเกิดขึ้นได้อย่างมีประสิทธิภาพ เพื่อให้สามารถบรรลุวัตถุประสงค์ขององค์กรที่กำหนดไว้ ทั้งในระดับองค์กร และในระดับหน่วยงาน



3) เพื่อให้คณะผู้บริหาร และคณะกรรมการบริหารความเสี่ยง ได้รับทราบข้อมูลความเสี่ยงที่สำคัญ แนวโน้มของความเสี่ยง และความเสี่ยงในภาพรวม ตลอดจนกำกับดูแลความเสี่ยงของบริษัทได้อย่างมีประสิทธิภาพและประสิทธิผล

4) เพื่อให้ทุกส่วนงานมีหน้าที่ระบุ ประเมิน และบริหารจัดการความเสี่ยงที่สำคัญๆ อย่างสม่ำเสมอ โดยคำนึงถึงระดับความเสี่ยงที่ยอมรับได้ และความสามารถในการปฏิบัติได้จริงด้วยต้นทุนที่เหมาะสม

5) เพื่อให้มีการสื่อสารและถ่ายทอดความรู้การบริหารความเสี่ยง ให้พนักงานได้อย่างสม่ำเสมอ และพัฒนาพนักงานให้มีความเข้าใจ มีความตระหนักถึงการเป็นเจ้าของความเสี่ยง ตลอดจนมีการบริหารความเสี่ยงร่วมกันภายใต้งานที่รับผิดชอบ

ค. ขอบเขตการใช้บังคับ

นโยบายนี้ใช้บังคับกับการบริหารจัดการความเสี่ยง การจัดลำดับความเสี่ยง กระบวนการจัดการความเสี่ยง และงานอื่นที่เกี่ยวข้องโดยตรงกับการบริหารความเสี่ยงองค์กร เพื่อให้การดำเนินงานของบริษัทเป็นไปอย่างมีประสิทธิภาพ และบรรลุวัตถุประสงค์สูงสุด

หน่วยงานบริหารความเสี่ยง มีหน้าที่รับผิดชอบโดยตรง เพื่อให้เกิดการปฏิบัติตามนโยบายนี้อย่างเคร่งครัด โดยคำนึงถึงผลกระทบเกี่ยวกับการประกอบธุรกิจของบริษัท ภายใต้การบริหารจัดการ ความเสี่ยงที่มีประสิทธิภาพ เพื่อหลีกเลี่ยงความสูญเสีย ความเสียหาย และผลกระทบอันอาจเกิดขึ้นกับการดำเนินงานของบริษัท โดยอาจเกิดจากความเสียหายในการดำเนินธุรกิจของบริษัทต่อไป

หมวดที่ 1

บททั่วไป

ข้อ 1. คำนิยาม

“บริษัท” หมายถึง บริษัท ไอรา แอนด์ อีฟูล จำกัด (มหาชน)

“พนักงาน” หมายถึง พนักงานของบริษัท ไอรา แอนด์ อีฟูล จำกัด (มหาชน) ทุกคน และทุกระดับชั้น

“ความเสี่ยง (Risk)” หมายถึง โอกาส หรือเหตุการณ์ที่มีความไม่แน่นอน หรือสิ่งที่ทำให้แผนงานหรือการดำเนินการของบริษัทในปัจจุบัน ไม่บรรลุวัตถุประสงค์ เป้าหมายที่กำหนดไว้ โดยก่อให้เกิดผลกระทบหรือความเสียหายต่อบริษัท ทั้งในแง่ผลกระทบที่เป็นตัวเงิน และ/หรือ ผลกระทบที่ไม่ใช่ตัวเงิน เช่น ภาพลักษณ์ และชื่อเสียงของบริษัท

“การบริหารความเสี่ยงองค์กร (Enterprise Risk Management)” หมายถึง กระบวนการที่ปฏิบัติโดยคณะกรรมการ ผู้บริหาร และพนักงานทุกคนในบริษัท โดยกระบวนการบริหารความเสี่ยงออกแบบเพื่อให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อบริษัท และสามารถจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ เพื่อความมั่นใจว่า การดำเนินงานของบริษัทจะเป็นไปโดยบรรลุวัตถุประสงค์ที่บริษัทกำหนดอย่างมีประสิทธิภาพ

“หน่วยงานบริหารความเสี่ยง” หมายถึง หน่วยงานที่มีหน้าที่โดยตรงในการกำกับดูแล กำหนดหลักเกณฑ์ บริหารจัดการความเสี่ยง ประสานงานกับหน่วยงานอื่น ตลอดจนดำเนินการอื่นที่เกี่ยวข้อง เพื่อให้เป็นไปตามนโยบายนี้

“คณะกรรมการบริหารความเสี่ยง” หมายถึง คณะกรรมการบริหารความเสี่ยงของ บริษัท ไอรา แอนด์ อีฟูล จำกัด (มหาชน) ซึ่งแต่งตั้งขึ้นโดยคณะกรรมการบริษัท และมีหน้าที่พิจารณา กำกับดูแล และบริหารความเสี่ยงโดยรายงานต่อคณะกรรมการบริษัท หรือคณะกรรมการอื่นตามที่ได้รับมอบหมาย และตามความเหมาะสม

ข้อ 2. นโยบายหลักในการบริหารความเสี่ยงองค์กร

2.1 กำหนดให้มั่นนโยบายในการบริหารความเสี่ยงองค์กร โดยให้เป็นความรับผิดชอบของพนักงานในทุกระดับชั้นที่ต้องตระหนักถึงความเสี่ยงที่มีในการปฏิบัติงานในหน่วยงานของตนและองค์กรโดยให้ความสำคัญในการบริหารความเสี่ยงด้านต่างๆ ให้อยู่ในระดับที่เพียงพอและเหมาะสม

2.2 กำหนดให้มีกระบวนการบริหารความเสี่ยงที่เป็นไปตามมาตรฐานที่ดีตามแนวปฏิบัติสากล เพื่อให้เกิดกระบวนการบริหารความเสี่ยงที่มีประสิทธิภาพ เกิดการพัฒนาและมีการปฏิบัติงานด้านการบริหารความเสี่ยงทั่วทั้งองค์กรในทิศทางเดียวกัน โดยนำระบบการบริหารความเสี่ยงมาเป็นส่วนหนึ่งในการตัดสินใจ การวางแผนกลยุทธ์ แผนงาน และการดำเนินงาน รวมถึงการมุ่งเน้นให้บรรลุวัตถุประสงค์ เป้าหมาย วิสัยทัศน์ พันธกิจ กลยุทธ์ที่กำหนดไว้ เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นและส่งผลกระทบกับการดำเนินงานของบริษัท เพื่อสร้างความเป็นเลิศในการปฏิบัติงานและสร้างความเชื่อมั่นของผู้เกี่ยวข้อง



2.3 กำหนดให้มีแนวทางป้องกันและบรรเทาความเสี่ยงจากการดำเนินงาน เพื่อป้องกัน และ/หรือหลีกเลี่ยงความเสียหาย และ/หรือ ความสูญเสียที่อาจเกิดขึ้น รวมถึงการติดตาม และประเมินผลการบริหารความเสี่ยงอย่างสม่ำเสมอ

2.4 สนับสนุนให้มีการนำระบบเทคโนโลยีสารสนเทศที่ทันสมัยมาใช้ในกระบวนการบริหารความเสี่ยงตามความเหมาะสม

2.5 สนับสนุนให้บุคลากรทุกระดับชั้น สามารถเข้าถึงแหล่งข้อมูลข่าวสารการบริหารความเสี่ยงได้อย่างทั่วถึง

2.6 สนับสนุนให้มีการจัดระบบการรายงานการบริหารความเสี่ยงให้ผู้บริหารระดับสูง คณะกรรมการบริหารความเสี่ยง คณะกรรมการบริษัท และ/หรือ คณะกรรมการอื่น (ถ้ามี) อย่างมีประสิทธิภาพ

ข้อ 3. หน้าที่และความรับผิดชอบหน่วยงานบริหารความเสี่ยง

3.1 ให้องค์กรบริหารความเสี่ยง รับผิดชอบการบริหารความเสี่ยงองค์กร ให้เป็นไปตามเกณฑ์ที่บริษัทกำหนด

3.2 ให้องค์กรบริหารความเสี่ยง กำหนดให้มีแนวนโยบายและเกณฑ์การบริหารความเสี่ยง โดยแนวนโยบายหลักเกณฑ์ หรือข้อกำหนดต่างๆ เกี่ยวกับการบริหารความเสี่ยงที่ได้รับอนุมัติตามขั้นตอน ที่ถูกต้องมาปฏิบัติ รวมถึงประเมินและควบคุมติดตามการบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

3.3 ในการดำเนินงานบริหารความเสี่ยงนั้น ให้องค์กรบริหารความเสี่ยง กำหนดแนวทางในการระบุความเสี่ยง และประเมินระดับของความเสี่ยง ให้เป็นไปตามเกณฑ์ที่กำหนดไว้ และสร้างมาตรการในการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ รวมถึงติดตามผลและรายงานสถานะความเสี่ยง ตลอดจนทบทวนความเพียงพอและควมมีประสิทธิภาพของมาตรการจัดการความเสี่ยงอย่างต่อเนื่อง เพื่อให้มั่นใจว่ากรณีที่เกิดเหตุขึ้นจะสามารถจัดการความเสี่ยงได้ทันท่วงที

3.4 ให้องค์กรบริหารความเสี่ยง รายงานสถานะความเสี่ยงที่สำคัญต่อผู้บริหารระดับสูง และคณะกรรมการที่เกี่ยวข้องตามระยะเวลาที่กำหนด และรายงานต่อหน่วยงานควบคุม หรือกำกับดูแล ตามกำหนด

3.5 ให้องค์กรบริหารความเสี่ยง กำหนดแนวทางในการสร้างเสริมความรู้เกี่ยวกับความเสี่ยง ตลอดจนสร้างเสริมวัฒนธรรมการทำงาน หรือการบริหารงานบนพื้นฐานของการบริหารความเสี่ยง ให้แก่ผู้บริหารและพนักงานอย่างต่อเนื่อง

ข้อ 4. ให้ผู้อำนวยการหน่วยงานบริหารความเสี่ยงหรือผู้อำนวยการฝ่ายที่ได้รับมอบหมายจากประธานเจ้าหน้าที่บริหาร เป็นผู้รักษาการและควบคุมการปฏิบัติตามนโยบายนี้ในอันที่จะตรวจสอบ และพิจารณา กฎ ระเบียบ ข้อบังคับ คู่มือ และ/หรือแนวปฏิบัติใดที่หน่วยงานที่เกี่ยวข้องจัดทำขึ้น ทั้งนี้เพื่อให้การปฏิบัติตามนโยบายนี้สำเร็จลุล่วงไป โดยนำเสนอขออนุมัติต่อผู้มีอำนาจอนุมัติตามนโยบายการมอบหมายอำนาจหน้าที่ของบริษัท (Delegation of Authority)

ข้อ 5. กฎ ระเบียบ ข้อบังคับ คู่มือ แนวปฏิบัติ และ/หรือ ข้อกำหนดใดที่ได้บังคับใช้ก่อนนโยบายนี้ให้ใช้บังคับโดยอนุโลมเพียงเท่าที่ไม่ขัดต่อนโยบายนี้

หมวดที่ 2

ระดับของความเสียหาย

ข้อ 6. หน่วยงานบริหารความเสี่ยง ต้องจัดให้มีการบริหารความเสี่ยง โดยครอบคลุม

- ก) การระบุความเสี่ยง
- ข) การประเมินความเสี่ยง
- ค) การกำหนดแผนการบริหารความเสี่ยง
- ง) การติดตามและจัดการความเสี่ยงที่สำคัญ

ข้อ 7. เพื่อให้เกิดความมั่นใจว่าสามารถบริหารความเสี่ยงได้อย่างมีประสิทธิภาพ ให้หน่วยงานบริหารความเสี่ยง กำหนดกรอบการบริหารความเสี่ยงครอบคลุมความเสี่ยงที่สำคัญ โดยแบ่งออกเป็น 3 ระดับ ดังนี้

7.1 ความเสี่ยงในระดับกลยุทธ์ (Strategic Risk)

7.2 ความเสี่ยงในระดับธุรกิจ (Business Risk) ความเสี่ยงที่สำคัญที่จัดอยู่ในความเสี่ยงในระดับธุรกิจ อาทิเช่น

- ก) ความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ข) ความเสี่ยงจากการหยุดชะงักของธุรกิจ
- ค) ความเสี่ยงจากการลงทุน
- ง) ความเสี่ยงจากการไม่ปฏิบัติตามกฎ ระเบียบ และข้อบังคับ

7.3 ความเสี่ยงระดับกระบวนการปฏิบัติงาน (Process Risk)

หมวดที่ 3

กระบวนการบริหารความเสี่ยงองค์กร

ข้อ 8. กำหนดให้มีกระบวนการบริหารความเสี่ยง เพื่อให้ขั้นตอนและวิธีการในการบริหารความเสี่ยงเป็นไปอย่างมีระบบ และดำเนินไปในทิศทางเดียวกันทั่วทั้งบริษัท โดยมีขั้นตอนสำคัญของกระบวนการบริหารความเสี่ยงองค์กรดังที่ได้กำหนดไว้นี้ เป็นอย่างน้อย

8.1 วิเคราะห์ หรือประเมินสภาพแวดล้อมภายในองค์กร (Internal Environment) ซึ่งเป็นพื้นฐานที่สำคัญ สำหรับการวางกรอบการบริหารความเสี่ยง ซึ่งมีอิทธิพลต่อการกำหนดกลยุทธ์และเป้าหมายขององค์กร การกำหนดกิจกรรม การบ่งชี้ ประเมินและจัดการความเสี่ยง

อนึ่ง สภาพแวดล้อมภายในองค์กร ให้หมายความรวมถึง ปัจจัยต่างๆ ที่นอกเหนือจากทรัพยากรของบริษัทด้วย เช่น จริยธรรม วิธีการทำงานของพนักงานและผู้บริหาร จำนวนบุคลากร รูปแบบการจัดการของฝ่ายบริหาร วิธีการมอบหมายอำนาจหน้าที่และความรับผิดชอบที่ส่งผลให้เกิดการสร้างจิตสำนึกการตระหนักและรับรู้เรื่อง ความเสี่ยงและการควบคุม แก่พนักงานทุกคนในบริษัท

8.2 กำหนดวัตถุประสงค์ (Objective Setting) โดยให้มีการกำหนดวัตถุประสงค์ทางธุรกิจที่ชัดเจน เพื่อให้มั่นใจว่าวัตถุประสงค์ที่กำหนดนั้น มีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ โดยการบริหารจัดการให้อยู่ในกรอบของ Risk Appetite และ Risk Tolerance

8.3 การบ่งชี้เหตุการณ์ (Event Identification) โดยพิจารณาปัจจัยความเสี่ยงทุกด้านที่อาจเกิดขึ้น เช่น ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านการเงิน ความเสี่ยงด้านการจัดการบุคลากร ความเสี่ยงด้านการปฏิบัติงาน ความเสี่ยงด้านกฎหมายและหน่วยงานกำกับดูแล ความเสี่ยงด้านภาษีอากร ความเสี่ยงด้านระบบงาน ความเสี่ยงด้านผลกระทบต่อสิ่งแวดล้อม โดยพิจารณาความสัมพันธ์ระหว่างเหตุการณ์ที่อาจเกิดขึ้น และส่งผลกระทบต่อ รวมถึงแหล่งที่มา หรือเหตุแห่งการเกิดความเสี่ยงทั้งจากสภาพแวดล้อมภายในและภายนอก

อนึ่ง การระบุเหตุการณ์อาจดำเนินการโดยการสัมภาษณ์ผู้บริหารระดับสูงหรือฝ่ายจัดการที่รับผิดชอบในแผนงานหรือการดำเนินการนั้น และรวบรวมประเด็นความเสี่ยงสำคัญที่ได้รับความสนใจหรือเป็นประเด็นที่กังวล เพื่อนำมาจัดทำภาพรวมความเสี่ยงขององค์กร (Corporate Risk Profile)

8.4 การประเมินความเสี่ยง (Risk Assessment) โดยมีกระบวนการประกอบด้วย 2 กระบวนการหลัก ดังนี้

8.4.1 การวิเคราะห์ความเสี่ยง จะพิจารณาสาเหตุและแหล่งที่มาของความเสี่ยง ผลกระทบที่ตามมาทั้งในทางบวกและทางลบ รวมทั้งโอกาสที่อาจเกิดขึ้นของผลกระทบที่อาจตามมาดังกล่าว โดยต้องระบุถึงปัจจัยที่มีผลกระทบต่อผลกระทบและโอกาสที่จะเกิดขึ้นทุกด้าน และพิจารณาถึงมาตรการจัดการความเสี่ยงที่ดำเนินการอยู่ ณ ปัจจุบัน รวมถึงประสิทธิผลของมาตรการดังกล่าวด้วย

8.4.2 การประเมินความเสี่ยง การประเมินความเสี่ยงจะเปรียบเทียบระหว่างระดับของความเสี่ยงที่ได้จากการวิเคราะห์ความเสี่ยง เปรียบเทียบกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) รวมถึงมาตรการจัดการความเสี่ยงในทันทีที่ระดับของความเสี่ยงไม่อยู่ในระดับที่ยอมรับได้

8.5 การตอบสนองความเสี่ยง (Risk Response) โดยให้มีการกำหนดแผนจัดการความเสี่ยง และนำเสนอแผนจัดการความเสี่ยงที่จะดำเนินการต่อผู้บริหาร คณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการบริษัท แล้วแต่กรณี เพื่อพิจารณา และขออนุมัติจัดสรรทรัพยากรที่จำเป็นต้องใช้ดำเนินการ (ถ้ามี) ทั้งนี้ การคัดเลือกแนวทางในการจัดการความเสี่ยงที่เหมาะสมที่สุดจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ (Risk Appetite) กับต้นทุนที่เกิดขึ้นเปรียบเทียบกับประโยชน์ที่จะได้รับ และต้องพิจารณา ข้อกฎหมาย ข้อกำหนดที่เกี่ยวข้อง และความรับผิดชอบต่อผู้มีส่วนได้ส่วนเสีย เป็นอย่างน้อย ประกอบด้วย เพื่อประกอบการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

8.6 กิจกรรมการควบคุม (Control Activities) กำหนดให้มีการควบคุมตามนโยบายนี้ โดยจัดให้ ระเบียบข้อกำหนด กระบวนการปฏิบัติงาน หรือแนวทางการปฏิบัติ หรือคำสั่งประการอื่นที่ชัดเจน เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยงให้อยู่ในระดับที่สามารถยอมรับได้ เพื่อป้องกันไม่ให้เกิดผลกระทบต่อเป้าหมายของบริษัท ทั้งนี้ ขึ้นต่อนวัตถุประสงค์ และเทคนิคการนำไปปฏิบัติ ให้นำเสนอต่อผู้บริหาร คณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการบริษัท แล้วแต่กรณี โดยอาจพิจารณาการควบคุมตามวัตถุประสงค์ที่ได้กำหนดไว้ ดังนี้

8.6.1 การควบคุมเพื่อการป้องกัน (Preventive Control) เพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก

8.6.2 การควบคุมเพื่อให้อัตราตรวจพบ (Detective Control) เพื่อให้ค้นพบข้อผิดพลาดที่เกิดขึ้นแล้ว

8.6.3 การควบคุมโดยการชี้แนะ (Directive Control) เพื่อส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ

8.6.4 การควบคุมเพื่อการแก้ไข (Corrective Control) เพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นและป้องกันไม่ให้เกิดขึ้นซ้ำอีกในอนาคต

ทั้งนี้ การดำเนินกิจกรรมการควบคุม ต้องพิจารณาถึงความคุ้มค่าในด้านค่าใช้จ่ายและต้นทุนเพื่อเปรียบเทียบกับประโยชน์ที่คาดว่าจะได้รับ ทั้งกิจกรรม วิธีการดำเนินงาน ขั้นตอน กระบวนการกำหนดบุคลากร เพื่อรับผิดชอบการควบคุมเพื่อพิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน และการพิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยงในอนาคต และกำหนดระยะเวลาแล้วเสร็จของกิจกรรมการควบคุม ประกอบการพิจารณาด้วย

8.7 ข้อมูลและการติดต่อสื่อสารสารสนเทศ (Information and Communication) กำหนดให้มีการใช้ข้อมูลและการติดต่อสื่อสารสารสนเทศ เพื่อบ่งชี้ ประเมิน และจัดการความเสี่ยง ข้อมูลสารสนเทศที่เกี่ยวข้องทั้งจากแหล่งข้อมูลภายในและภายนอก ควรได้รับการบันทึกและสื่อสารไปยังบุคลากรอย่าง เหมาะสม เพื่อให้สามารถปฏิบัติตามหน้าที่และความรับผิดชอบได้อย่างมีประสิทธิภาพ รวมถึงการรายงานการบริหารจัดการความเสี่ยง เพื่อให้รับทราบถึงความเสี่ยงที่เกิดขึ้น และผลของการบริหารจัดการความเสี่ยงด้วย

ทั้งนี้ ในการบริหารความเสี่ยงควรใช้ทั้งข้อมูลในอดีต และปัจจุบัน เพื่อแสดงแนวโน้มของเหตุการณ์และคาดการณ์การปฏิบัติงานในอนาคต และเพื่อประโยชน์ในการพิจารณาความเสี่ยงที่เกิดขึ้น ใน กระบวนการ สายงาน หรือหน่วยงาน เพื่อให้บริษัทสามารถปรับเปลี่ยนกิจกรรมการควบคุมตามความจำเป็นเพื่อให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้

8.8 การติดตาม (Monitoring) เพื่อการควบคุมความคืบหน้าในการบริหารความเสี่ยง การดูแลติดตามแนวโน้มของความเสียหายหลัก รวมถึงการเกิดเหตุการณ์ ผิดปกติอย่างต่อเนื่อง โดยมีวัตถุประสงค์หลักเพื่อให้มั่นใจว่า

8.8.1 หน่วยงานที่เป็นเจ้าของความเสี่ยง (Risk Owner) มีการติดตามประเมินสถานการณ์ วิเคราะห์และบริหารความเสี่ยงที่อยู่ภายใต้ความรับผิดชอบของตนอย่างสม่ำเสมอและเหมาะสม

8.8.2 ความเสี่ยงที่มีผลกระทบสำคัญต่อการบรรลุวัตถุประสงค์ของบริษัท ได้รับ การรายงานถึงความคืบหน้าในการบริหารความเสี่ยง และแนวโน้มของความเสี่ยงต่อผู้บริหารที่รับผิดชอบ

8.8.3 ระบบการควบคุมภายในที่วางไว้มีความเพียงพอ เหมาะสม มีประสิทธิผล และมีการนำมาปฏิบัติใช้จริงเพื่อป้องกัน หรือลดความเสี่ยงที่อาจเกิดขึ้น รวมทั้งมีการปรับปรุงแก้ไข การควบคุมอยู่เสมอเพื่อให้สอดคล้องกับสถานการณ์หรือความเสี่ยงที่เปลี่ยนไป

หน่วยงานบริหารความเสี่ยง มีหน้าที่ประสานงานให้มีการจัดการรับผิดชอบต่อความเสี่ยง รายงาน สถานะความเสี่ยง รวมถึงกระบวนการบริหารความเสี่ยงให้ผู้บริหาร คณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการบริษัท แล้วแต่กรณี หรือคณะกรรมการอื่นตามที่เห็นสมควร เพื่อพิจารณาต่อไป

หมวดที่ 4

การจัดประเภทของความเสี่ยง

ข้อ 9. บริษัทจัดให้มีการจำแนกประเภทความเสี่ยง โดยแบ่งประเภทความเสี่ยงออกเป็น 4 ประเภทเป็นอย่างน้อย ได้แก่

9.1 ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) อันเกี่ยวข้องกับการกำหนดแผนกลยุทธ์แผนการดำเนินงาน และรวมถึงการนำแผนไปปฏิบัติอย่างไม่เหมาะสม ตลอดจนการเปลี่ยนแปลงจากปัจจัยภายนอกและปัจจัยภายใน อันส่งผลกระทบต่อข้อกำหนดกลยุทธ์หรือการดำเนินงานเพื่อให้บรรลุวัตถุประสงค์หลัก เป้าหมาย และแนวทางการดำเนินงานของบริษัท

9.2 ความเสี่ยงด้านปฏิบัติการ (Operational Risk) ความเสี่ยงที่จะเกิดความเสียหายต่าง ๆ อันเนื่องมาจากความไม่เพียงพอหรือความบกพร่องของกระบวนการควบคุมภายใน บุคลากร ระบบงาน หรือจากเหตุการณ์ภายนอก รวมถึงความเสี่ยงที่เกิดจากการริเริ่มความเปลี่ยนแปลง (change initiatives) เช่น การออกผลิตภัณฑ์และบริการทางการเงินรูปแบบใหม่ การเข้าสู่ตลาดใหม่ การปรับเปลี่ยน กระบวนการ ระบบงาน หรือการขยาย ขอบเขตการดำเนินงานที่อยู่ห่างไกลจากสำนักงานใหญ่ เป็นต้น และความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอก (Third party dependency)

9.3 ความเสี่ยงที่เกี่ยวข้องกับการบริหารจัดการทางการเงิน (Financial Risk) ซึ่งอาจเกิดจากปัจจัยภายใน เกี่ยวด้วยการบริหารจัดการด้านสภาพคล่อง ด้านเครดิต ด้านเงินลงทุน หรืออาจเกิดจากปัจจัยภายนอกเกี่ยวข้องการเปลี่ยนแปลงของอัตราดอกเบี้ย อัตราแลกเปลี่ยน หรือความเสี่ยงที่คู่สัญญาไม่สามารถปฏิบัติตามภาระผูกพันที่ตกลงไว้ เป็นต้น ซึ่งอาจส่งผลกระทบต่อการทำงาน รวมถึงส่งผลให้เกิดความเสียหายต่อบริษัท

9.4 ความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามกฎระเบียบ และข้อบังคับที่เกี่ยวข้อง ของหน่วยงานกำกับดูแล (Compliance Risk) รวมทั้งความเสี่ยงที่เกี่ยวกับกฎหมายและกฎเกณฑ์ต่างๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัท เช่น ธนาคารแห่งประเทศไทย สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ เป็นต้น ทั้งนี้ให้หมายความรวมถึง ผลกระทบต่อชื่อเสียง และภาพลักษณ์ของบริษัท อันเกิดจากการที่ไม่สามารถปฏิบัติตามนโยบายและวิธีการปฏิบัติงานที่หน่วยงานกำกับดูแลด้วย

หมวดที่ 5

เกณฑ์ความเสี่ยง

ข้อ 10. ให้กำหนดเกณฑ์ความเสี่ยงที่ใช้ในการประเมินความเสี่ยงโดยสะท้อนถึงคุณค่า ชื่อเสียง วัตถุประสงค์ และทรัพยากรของบริษัท โดยสอดคล้องกับหลักเกณฑ์ ข้อกำหนดทางกฎหมาย หรือข้อบังคับของหน่วยงานกำกับดูแลหรือหน่วยงานที่เป็นสมาชิกอยู่ในปัจจุบัน และสอดคล้องกับนโยบายนี้

ข้อ 11. ปัจจัยที่นำมาพิจารณา เพื่อประกอบการกำหนดเกณฑ์ความเสี่ยงอย่างน้อย ให้พิจารณาครอบคลุม ดังนี้

11.1 ลักษณะและประเภทของผลกระทบที่สามารถเกิดขึ้น และแนวทางในการประเมินผลกระทบ

11.2 แนวทางในการระบุโอกาสในการเกิดความเสี่ยง



- 11.3 กรอบเวลาของโอกาส และผลกระทบที่เกิดขึ้น
- 11.4 แนวทางในการกำหนดระดับความเสี่ยง
- 11.5 ระดับของความเสี่ยงที่สามารถยอมรับได้
- 11.6 ระดับของความเสี่ยงที่จะต้องจัดการ

ข้อ 12. ให้กำหนดโอกาสที่จะเกิดความเสี่ยง (Likelihood) และระดับของความเสียหาย โดยแบ่งเป็น 5 ระดับ ดังนี้

- 12.1 ความเสี่ยงระดับ 5 หมายถึง โอกาสที่จะเกิดความเสี่ยง ค่อนข้างแน่นอน
- 12.2 ความเสี่ยงระดับ 4 หมายถึง โอกาสที่จะเกิดความเสี่ยง น่าจะเกิด
- 12.3 ความเสี่ยงระดับ 3 หมายถึง โอกาสที่จะเกิดความเสี่ยง เป็นไปได้ที่จะเกิด
- 12.4 ความเสี่ยงระดับ 2 หมายถึง โอกาสที่จะเกิดความเสี่ยง ไม่น่าจะเกิด
- 12.5 ความเสี่ยงระดับ 1 หมายถึง โอกาสที่จะเกิดความเสี่ยง ยากที่จะเกิด

ข้อ 13. ให้กำหนดระดับของผลกระทบจากความเสี่ยง (Risk Impact) และความเสียหายจากความเสี่ยง ครอบคลุมการบริหารความเสี่ยงทั้งองค์กร โดยคำนึงถึงผลกระทบอย่างน้อย 5 ด้าน ดังนี้

- 13.1 ผลกระทบด้านการเงิน
- 13.2 ผลกระทบด้านชื่อเสียงและภาพลักษณ์ของบริษัท
- 13.3 ผลกระทบต่อการไม่ปฏิบัติตามกฎหมาย กฎ ระเบียบ ข้อบังคับของหน่วยงานกำกับดูแลและของบริษัท
- 13.4 ผลกระทบต่อบุคลากรสำคัญของบริษัท
- 13.5 ผลกระทบต่อความล่าช้าในการดำเนินงานในโครงการสำคัญของบริษัท ตลอดจนผลกระทบที่สืบเนื่องจากการบริหารงานที่ไม่เป็นไปตามเป้าหมาย

ทั้งนี้ แต่ละด้านให้กำหนดระดับความรุนแรง โดยแบ่งออกเป็น 5 ระดับ แต่ละระดับกำหนดนิยามไว้ ดังนี้

- ก) ระดับ 5 หมายถึง วิกฤติ
- ข) ระดับ 4 หมายถึง มีนัยสำคัญ
- ค) ระดับ 3 หมายถึง ปานกลาง
- ง) ระดับ 2 หมายถึง น้อย
- จ) ระดับ 1 หมายถึง ไม่เป็นนัยสำคัญ

ข้อ 14. กำหนดให้มีเครื่องมือที่ใช้สำหรับการรายงานระดับความเสี่ยงที่ได้รับการประเมิน โดยแสดงเป็นแผนภาพ แสดงการจัดลำดับความเสี่ยงว่า ความเสี่ยงที่ได้รับการประเมินอยู่ในกลุ่มประเภทความเสี่ยงสูง ค่อนข้างสูง ปานกลาง หรือต่ำ

ให้หน่วยงานบริหารความเสี่ยง วิเคราะห์ สรุปผลการประเมิน และจัดลำดับความสำคัญของประเด็นความเสี่ยง และนำเสนอผลการประเมิน ประเด็นความเสี่ยง และมาตรการต่างๆ ที่กำหนดให้ต้องจัดการดูแลเพิ่มเติมเพื่อให้ผู้บริหาคณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการบริษัท แล้วแต่กรณี หรือคณะกรรมการอื่นตามที่เห็นสมควร เพื่อทราบและพิจารณาคัดเลือกประเด็นความเสี่ยงสำคัญที่ต้องจัดการ รวมถึงการกำหนดหน่วยงานที่รับผิดชอบ เพื่อบริหารจัดการความเสี่ยงเพิ่มเติมจากที่มีในปัจจุบัน

หมวดที่ 6

แนวทางในการจัดการความเสี่ยง

ข้อ 15. แนวทางในการจัดการความเสี่ยง ให้คำนึงถึงวิธีการที่กำหนดไว้ในข้อนี้ เป็นอย่างน้อย

15.1 การหลีกเลี่ยง (Avoid) เป็นการดำเนินการเพื่อหลีกเลี่ยงเหตุการณ์ที่ก่อให้เกิดความเสี่ยงในกรณีที่ความเสี่ยงมีความรุนแรงสูง ไม่สามารถหาวิธีลดหรือจัดการให้อยู่ในระดับที่ยอมรับได้

15.2 การร่วมจัดการ (Share) เป็นการร่วมหรือถ่ายโอนความเสี่ยงทั้งหมดหรือบางส่วนไปยังบุคคลหรือหน่วยงานภายนอก ให้ช่วยแบกรับภาระความเสี่ยงแทน เช่น การซื้อกรมธรรม์ประกันภัย

15.3 การลด (Reduce) เป็นการลดมาตรการจัดการ เพื่อลดโอกาสการเกิดเหตุการณ์ความเสี่ยง หรือลดผลกระทบที่อาจเกิดขึ้นให้อยู่ในระดับที่ยอมรับได้ เช่น การเตรียมแผนฉุกเฉิน (Contingency plan)

15.4 การยอมรับ (Accept) ความเสี่ยงที่เหลือในปัจจุบันอยู่ในระดับที่ยอมรับได้โดยไม่ต้องดำเนินการใด เพื่อลดโอกาส หรือผลกระทบที่อาจเกิดขึ้นอีก เมื่อมีความเสี่ยงที่ใช้ต้นทุนสูงในมาตรการจัดการซึ่งอาจไม่คุ้มกับประโยชน์ที่ได้รับ

หมวดที่ 7

การทบทวนนโยบายบริหารความเสี่ยง

ข้อ 16. ให้นำหน่วยงานบริหารความเสี่ยง วิเคราะห์ ติดตามการเปลี่ยนแปลงของสภาพแวดล้อมทั้งภายในและภายนอก และทำการทบทวนนโยบายนี้อย่างน้อยหนึ่งครั้งต่อปี

ให้หน่วยงานบริหารความเสี่ยงมีหน้าที่ วิเคราะห์ ติดตามการเปลี่ยนแปลงของสภาพแวดล้อมที่เกี่ยวข้อง รวมถึงการเปลี่ยนแปลงของความเสี่ยงที่อาจเกิดขึ้น ซึ่งอาจส่งผลให้ต้องมีการทบทวน การบริหารจัดการความเสี่ยง และ/หรือการจัดลำดับความสำคัญ เพื่อนำไปทบทวนและปรับปรุงแผนการดำเนินการบริหารความเสี่ยง ให้มีประสิทธิภาพโดยให้คำนึงถึงความสำคัญของการทบทวนและปรับปรุงแผนการดำเนินการ เพื่ออาจเสนอขอพิจารณาแก้ไขเปลี่ยนแปลงโดยเร่งด่วน โดยไม่จำเป็นต้องรอให้ถึงกำหนดการทบทวนแผนการดำเนินงาน หรือนโยบาย ตามกำหนดในวรรคแรก

ข้อ 17 บันทึกการแก้ไข

ประวัติแก้ไข/ปรับปรุงเนื้อหา

แก้ไขครั้งที่	วันที่อนุมัติใช้	เนื้อหาที่แก้ไข/ปรับปรุง	หน้าที่
1	16 ธันวาคม 2564	แก้ไข “แผนบริหารความเสี่ยง” เป็น “หน่วยงานบริหารความเสี่ยง”	2,3,4,5, 7,9,10
		แก้ไขและเพิ่มเติมหมวดที่ 4 การจัดการประเภทของความเสี่ยง ข้อที่ 9.2 ความเสี่ยงด้านปฏิบัติการ (Operational Risk)	8



แก้ไขครั้งที่	วันที่อนุมัติใช้	เนื้อหาที่แก้ไข/ปรับปรุง	หน้าที่
2	26 มีนาคม 2567	แก้ไขและเพิ่มเติมหมวดที่ 1 บททั่วไป ได้แก่ - ข้อที่ 1 คำนิยาม - ข้อที่ 2 นโยบายหลักในการบริหารความเสี่ยงองค์กร ข้อที่ 2.6” - ข้อที่ 3 หน้าที่และความรับผิดชอบหน่วยงานบริหารความเสี่ยง - ข้อที่ 4 ภารกิจและการควบคุมการปฏิบัติตามนโยบายนี้	3-4
		แก้ไขและเพิ่มเติมหมวดที่ 2 ระดับความเสี่ยง ในหัวข้อที่ 7.2 ความเสี่ยงในระดับธุรกิจ (Business Risk)	5
		แก้ไขและเพิ่มเติมหมวดที่ 3 กระบวนการบริหารความเสี่ยงองค์กร ได้แก่ - ข้อที่ 8.5 การตอบสนองความเสี่ยง (Risk Response) - ข้อที่ 8.6 กิจกรรมการควบคุม (Control Activities) - วรรคสุดท้ายของหมวดที่ 3	6-7
		แก้ไขและเพิ่มเติมหมวดที่ 4 การจัดประเภทของความเสี่ยง ได้แก่ - ข้อที่ 9.2 ความเสี่ยงด้านปฏิบัติการ (Operational Risk) - ข้อที่ 9.4 ความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามกฎระเบียบ และข้อบังคับที่เกี่ยวข้อง ของหน่วยงานกำกับดูแล(Compliance Risk)	8
		แก้ไขและเพิ่มเติมหมวดที่ 5 เกณฑ์ความเสี่ยง ในวรรคสุดท้าย	9
		แก้ไขและเพิ่มเติมหมวดที่ 6 แนวทางในการจัดการความเสี่ยงข้อที่ 15.4 การยอมรับ (Accept)	10

บริษัท ไอรา แอนด์ อีฟูล จำกัด (มหาชน)

วันที่ 26 มีนาคม 2567