บริษัท เอสทีพี แอนด์ ไอ จำกัด (มหาชน)
นโยบายบริหารความเสี่ยง

(ได้ผ่านการพิจารณาอนุมัติจากคณะกรรมการบริษัท เมื่อการประชุมคณะกรรมการ ครั้งที่ 3/2568
วันที่ 14 มีนาคม 2568)

นโยบายบริหารความเสี่ยง ของบริษัท เอสทีพี แอนด์ ไอ จำกัด (มหาชน)

1. หลักการและเหตุผล

บริษัท เอสทีพี แอนด์ ไอ จำกัด (มหาชน) มีความมุ่งหวังที่จะดำเนินธุรกิจอย่างต่อเนื่องและยั่งยืน เพื่อเพิ่มคุณค่าให้กับผู้มีส่วนได้เสีย ซึ่งหมายรวมถึงผู้ถือหุ้น ลูกค้า คู่ค้า พนักงานทั้งหมด รัฐบาล และประชาชนทั่วไป จึงตระหนักถึงความสำคัญของการบริหารความเสี่ยง ซึ่งถือเป็นกลไกสำคัญที่ช่วยวางแผนและกำหนดโครงสร้างบริษัท เป้าหมายกลยุทธ์และการดำเนินงานให้สอดคล้องกับวัตถุประสงค์ที่บริษัทกำหนดไว้ ได้อย่างมีประสิทธิภาพและประสิทธิผล ทั้งนี้บริษัทฯได้กำหนดนโยบายบริหารความเสี่ยงตามแนวคิดของ COSO Enterprise & Risk Management – Integrating with Strategy and Performance (2017)[1] ขึ้นมาเป็นเครื่องมือเพื่อจัดให้มีกระบวนการที่จะสามารถระบุความเสี่ยงซึ่งครอบคลุมถึงความเสี่ยง ให้สามารถบ่งชี้รวมทั้งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้โดยกำหนดให้คณะกรรมการ ผู้บริหาร และพนักงานทุกคนในบริษัท มีส่วนร่วมในการบริหารความเสี่ยงและมีการทบทวนนโยบายและกระบวนการปฏิบัติให้มีความเหมาะสมอยู่เสมอ

2. วัตถุประสงค์

2.1 เพื่อกำหนดให้การบริหารความเสี่ยงเป็นส่วนหนึ่งในการตัดสินใจในการกำหนดยุทธศาสตร์ แผนงาน และการดำเนินงานด้านต่าง ๆ ของบริษัท

2.2 เพื่อระบุความเสี่ยงและกำหนดแนวทางการจัดการความเสี่ยงที่เหลืออยู่ให้อยู่ในระดับที่ยอมรับได้ โดยพิจารณามาตรการที่จะลดโอกาสและ/หรือผลกระทบจากความเสี่ยงที่อาจจะเกิดขึ้นได้อย่างมี ประสิทธิภาพ เพื่อบรรลุเป้าหมายที่กำหนดไว้ทั้งในระดับองค์กร และในระดับหน่วยงาน

เพื่อสื่อสารและสร้างวัฒนธรรมองค์กรให้กรรมการและผู้บริหาร ได้รับทราบและตระหนักถึงข้อมูลความเสี่ยงที่สำคัญ แนวโน้มของความเสี่ยง และความเสี่ยงในภาพรวม เพื่อเป็นการตัดสินใจรวมถึงการกำกับดูแลความเสี่ยงได้อย่างมีประสิทธิภาพและมีประสิทธิผล

3. ขอบเขต

นโยบายการบริหารความเสี่ยงให้มีผลครอบคลุมบริษัทและบริษัทย่อย

[1] COSO Enterprise & Risk Management กรอบการบริหารความเสี่ยงองค์กร แนวคิดการบริหารความเสี่ยงองค์กรตามแนวคิดใหม่ โดยได้ให้ความสำคัญถึงการเชื่อมโยงการบริหารความเสี่ยงองค์กรเข้ากับการวางแผนเชิงกลยุทธ์เพื่อเพิ่ม มูลค่าให้องค์กร

4. คำนิยาม

ความเสี่ยง (Risk) คือ โอกาส หรือ เหตุการณ์ที่ไม่แน่นอนต่างๆ หรือสิ่งที่ทำให้แผนงานหรือการดำเนินการอยู่ ณ ปัจจุบันไม่บรรลุวัตถุประสงค์หรือเป้าหมายที่กำหนดไว้ โดยก่อให้เกิดผลกระทบเชิงลบ เป็นตัวเงินและ/หรือ ผลกระทบต่อภาพลักษณ์และชื่อเสียงของบริษัท

ปัจจัยเสี่ยง (Risk Factor) คือ สิ่งที่เป็นต้นเหตุหรือสิ่งที่เป็นแหล่งที่มาของความเสี่ยงและเหตุการณ์ที่จะทำให้ไม่บรรลุวัตถุประสงค์หรือเป้าหมายที่กำหนดไว้ โดยในแต่ละปัจจัยจะมีการกำหนดสาเหตุที่แท้จริงของปัจจัยต่างๆ ที่สามารถอธิบายได้ว่าสาเหตุปัจจัยเสี่ยงดังกล่าวส่งผลให้เกิดความเสี่ยงใดๆ และสามารถหามาตรการจัดการเพื่อลดความเสี่ยงที่จะเกิดขึ้นได้

การบริหารความเสี่ยง (Risk Management) คือ กระบวนการที่ปฏิบัติโดยคณะกรรมการ ผู้บริหาร และพนักงานทุกคน เพื่อช่วยในการกำหนดกลยุทธ์และดำเนินงาน โดยกระบวนการบริหารความเสี่ยงได้รับการออกแบบเพื่อให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อบริษัท และสามารถจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) คือ ระดับความเสี่ยงที่จัดทำการประเมินผลการบริหารความเสี่ยงและได้รับอนุมัติจากคณะกรรมการบริษัทแล้วว่าสามารถยอมรับได้ในระดับองค์กร โดยความเสี่ยงใดที่ได้รับการวิเคราะห์และประเมินแล้วพบว่าอาจมีผลกระทบต่อบริษัทเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ให้หน่วยงานเจ้าของความเสี่ยงนั้นๆ จัดทำแผนบริหารความเสี่ยง (Action Plan) นำเสนอและรายงานขออนุมัติต่อคณะกรรมการที่เกี่ยวข้องตามลำดับ

แหล่งที่มาของการเกิดความเสี่ยง เกิดจากปัจจัย 2 ปัจจัย คือ

1) ปัจจัยภายใน เช่น วัตถุประสงค์ขององค์กร นโยบายและกลยุทธ์ การดำเนินงาน กระบวนการทำงาน, โครงสร้างองค์กร วัฒนธรรมองค์กร และเทคโนโลยีสารสนเทศ เป็นต้น
2) ปัจจัยภายนอก เช่น นโยบายของรัฐ สภาวะเศรษฐกิจ/สังคมการเมือง การแข่งขัน โรคระบาด และภัยธรรมชาติต่างๆ เป็นต้น

การประเมินความเสี่ยง (Risk Assessment) คือ กระบวนการในการระบุระดับความรุนแรง และการจัดลำดับความสำคัญของปัจจัยเสี่ยง โดยประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) ที่จะเกิดขึ้น

5. หน้าที่และความรับผิดชอบ

1. กำหนดนโยบายบริหารความเสี่ยง กรอบการบริหารความเสี่ยงองค์กร และกรอบการบริหารจัดการผู้มีส่วนได้ส่วนเสียขององค์กร และพิจารณาปัจจัยความเสี่ยงที่สำคัญอันอาจเกิดขึ้น
2. กำหนดเกณฑ์วัดความเสี่ยงและเพดานความเสี่ยงที่บริษัทฯ จะยอมรับได้
3. กำหนดมาตรการที่จะใช้ในการจัดการความเสี่ยงให้เหมาะสมต่อสภาวการณ์
4. การกำกับดูแลบริหารความเสี่ยงของบริษัทในภาพรวม และให้ข้อเสนอแนะต่อความเสี่ยงที่สำคัญอย่างเป็นอิสระ ติดตามและสอบทานนโยบายและการปฏิบัติตามหลักการบริหารความเสี่ยงของบริษัทและบริษัทย่อย ให้มั่นใจว่าดำเนินการตรวจสอบบนฐานความเสี่ยง (Risk based Audit) และมีการจัดการความเสี่ยงที่เหมาะสมขององค์กร
5. ทบทวนความเพียงพอของนโยบาย, กระบวนการปฏิบัติงานและระบบการบริหารความเสี่ยง โดยรวมถึงความมีประสิทธิผลของระบบ, ความเหมาะสม, ให้สอดคล้องกับกลยุทธ์และเป้าหมายทางธุรกิจ รวมถึงสภาวการณ์ที่เปลี่ยนแปลงไป
6. จัดให้มีคณะทำงานบริหารความเสี่ยงตามความจำเป็น โดยสนับสนุนคณะทำงานบริหารความเสี่ยงในด้านบุคลากร งบประมาณและทรัพยากรอื่นที่จำเป็นให้สอดคล้องกับขอบเขตความรับผิดชอบ
7. พิจารณารายงานผลการบริหารความเสี่ยงองค์กรและให้ข้อคิดเห็นในความเสี่ยงที่อาจจะเกิดขึ้นต่อคณะกรรมการบริษัทอย่างสม่ำเสมอ รวมทั้งแนวทางการกำหนดมาตรการควบคุม หรือบรรเทา (Mitigation Plan) รวมถึงสิ่งที่ต้องดำเนินการปรับปรุงแก้ไขเพื่อให้สอดคล้องกับนโยบายและกลยุทธ์ที่กำหนด

6. ประเภทความเสี่ยง

6.1 ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) เป็นความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ หรือปัจจัยต่าง ๆ ที่นำไปปฏิบัติอย่างไม่เหมาะสมหรือไม่สอดคล้องกับนโยบาย เป้าหมาย กลยุทธ์โครงสร้างองค์กร ปัจจัยภายใน และสภาพแวดล้อมภายนอก ส่งผลให้ไม่บรรลุตามวัตถุประสงค์และเป้าหมายที่บริษัทฯ กำหนดไว้ ครอบคลุมถึง ความเสี่ยงจากการผันผวนของรายได้ ความเสี่ยงจากการผันผวนของราคาวัตถุดิบ และความไม่เพียงพอของปริมาณแรงงาน ซึ่งปัจจัยดังกล่าวส่งผลกระทบต่อการกำหนดกลยุทธ์ด้านการแข่งขัน และแนวทางดำเนินงานขององค์กร

6.2 ความเสี่ยงด้านการเงิน (Financial Risk) เป็นความเสี่ยงที่เกี่ยวกับนโยบายและขั้นตอนการบริหารจัดการด้านการเงินและการลงทุน ซึ่งส่งผลกระทบต่อผลการดำเนินงานและงบการเงินของบริษัทฯ ครอบคลุมถึงความเสี่ยงที่ผลประกอบการไม่เป็นไปตามเป้าหมายที่กำหนด รวมถึงความเสี่ยงจากการขาดสภาพคล่อง ด้านเครดิต ด้านเงินลงทุน หรือการเปลี่ยนแปลงของอัตราแลกเปลี่ยน และอัตราดอกเบี้ย อีกทั้งความเสี่ยงที่คู่สัญญาไม่ปฏิบัติตามภาระผูกพันที่ตกลงไว้อันจะส่งผลเสียหายต่อองค์กรได้

6.3 ความเสี่ยงด้านการปฏิบัติการ (Operational Risk) เป็นความเสี่ยงที่เกิดจากกระบวนการปฏิบัติงาน ระบบงาน หรือจากเหตุการณ์ภายนอก ที่ส่งผลต่อประสิทธิภาพและประสิทธิผลในการดำเนินงาน ครอบคลุมถึงความเสี่ยงที่เกิดจากข้อบกพร่องของกระบวนการปฏิบัติงานอันจะส่งผลให้กิจกรรมต่างๆ ภายในองค์กรไม่มีประสิทธิภาพ รวมทั้งความเสี่ยงที่เกี่ยวข้องกับการบริหารจัดการข้อมูลด้านเทคโนโลยีสารสนเทศ และข้อมูลความรู้ต่างๆ เพื่อให้การปฏิบัติงานบรรลุเป้าหมายที่กำหนด

6.4 ความเสี่ยงที่เกี่ยวข้องกับกฎระเบียบ (Compliance Risk) เป็นความเสี่ยงที่เกิดขึ้นจากการไม่ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ ประกาศคำสั่ง หลักเกณฑ์ และแนวปฏิบัติทั้งของบริษัทฯ และของหน่วยงานภายนอก รวมถึงการที่กฎระเบียบที่ถูกกำหนดขึ้นไม่ชัดเจน ต้องใช้ดุลยพินิจหรือการตีความ ซึ่งจะมีผลต่อการถูกฟ้องร้องหรือร้องเรียน ครอบคลุมถึงความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติตามกฎระเบียบ ข้อบังคับของหน่วยงานกำกับดูแล และความเสี่ยงที่เกี่ยวกับกฎหมายต่างๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัท

6.5 ความเสี่ยงด้านไซเบอร์ (Cyber Risk) เป็นความเสี่ยงที่เกี่ยวข้องกับเรื่องความปลอดภัยทางด้านไซเบอร์ที่เกิดจากการเปลี่ยนแปลงทางเทคโนโลยีสารสนเทศ รวมทั้งการเปลี่ยนแปลงเทคโนโลยีดิจิตัล (Digital Transformation) ซึ่งมีผลกระทบต่อการดำเนินงานของบริษัท และให้หมายรวมถึงระบบเทคโนโลยีสารสนเทศที่องค์กรใช้ในการดำเนินกิจกรรมทางธุรกิจที่สำคัญ

6.6 ความเสี่ยงในองค์กร (Organization Risk) เช่น การควบรวมกิจการ (Merger & Acquisition) การจัดการด้านการตลาดลูกค้าร่วมกัน การบริหารจัดการบุคคลากร รวมถึงการเลิกจ้างงานอย่างถูกต้อง เป็นต้น

6.7 ความเสี่ยงจากปัจจัยภายนอก (External Risk) เช่น ผลกระทบจากสงคราม รูปแบบการขนส่งที่เปลี่ยนแปลง การเมืองที่เปลี่ยนแปลง ภัยพิบัติน้ำท่วม ไฟไหม้ โรคภัยต่างๆ สภาพอากาศที่เปลี่ยนแปลงไป เป็นต้น

6.8 ความเสี่ยงด้านการทุจริตคอร์รัปชัน (Corruption Risk) เป็นความเสี่ยงที่เกิดจากการกระทำใดๆ เพื่อแสวงหาผลประโยชน์โดยมิชอบด้วยกฎหมาย โดยการให้หรือรับสินบน ไม่ว่าจะเป็นเงิน สิ่งของ การช่วยเหลือทางการเมือง การบริจาคเพื่อการกุศล ค่าบริการต้อนรับหรือค่าใช้จ่ายอื่นๆ โดยการเสนอให้สัญญาว่าจะให้ ให้คำมั่น เรียกร้อง ให้หรือรับซึ่งเงิน หรือประโยชน์อื่นใดที่ไม่เหมาะสมแก่เจ้าหน้าที่รัฐ หน่วยงานรัฐ เอกชนหรือผู้มีหน้าที่ไม่ว่าโดยทางตรงหรือทางอ้อม เพื่อให้หน่วยงานหรือบุคคลดังกล่าวกระทำหรือยกเว้นการปฏิบัติหน้าที่โดยมิชอบ

<u>แนวทางในการบริหารความเสี่ยง มีขั้นตอนดังต่อไปนี้</u>

1) ระบุความเสี่ยงทุกประเภทที่อาจจะมีผลกระทบต่อการดำเนินธุรกิจ การเงิน ข้อบังคับและกฎหมายที่เกี่ยวข้อง
2) วิเคราะห์และประเมินความเสี่ยง โดยพิจารณาทั้งโอกาสเกิดเหตุการณ์ และผลกระทบที่อาจเกิดขึ้น

3) กำหนดมาตรการและแผนปฏิบัติงานเพื่อจัดการความเสี่ยง โดยอาจเป็นการยอมรับความเสี่ยงนั้น (acceptance) การลดความเสี่ยง (reduction) การหลีกเลี่ยงความเสี่ยง (avoidance) หรือการร่วมรับความเสี่ยง (sharing)
4) กำหนดมาตรการควบคุมให้เป็นไปตามแผนปฏิบัติงานในทุกระดับขององค์กร ได้แก่ระดับกลุ่มบริษัท สายงาน ฝ่ายงาน แผนก หรือกระบวนการ ที่มีความเหมาะสมกับความเสี่ยง และลักษณะเฉพาะขององค์กร เช่น สภาพแวดล้อม ความซับซ้อนของงาน ลักษณะงาน ขอบเขต การดำเนินงาน เป็นต้น
5) ติดตามและทบทวนผลการควบคุม เพื่อให้มั่นใจได้ว่ามาตรการควบคุมยังดำเนินไปอย่างครบถ้วนและเหมาะสม