นโยบายบริหารความเสี่ยง

บริษัท แรบบิท โฮลดิ้งส์ จำกัด (มหาชน)

เวอร์ชั่น .:	5
วันที่บังคับใช้ :	11 มีนาคม 2569
อนุมัติโดย :	คณะกรรมการบริษัท

สารบัญ

ลำดับการแก้ไข	3
วัตถุประสงค์	4
ขอบเขตของนโยบาย	4
ข้อยกเว้นของการไม่ปฏิบัติตามนโยบาย	4
กฎหมาย ข้อบังคับ นโยบาย และขั้นตอนที่เกี่ยวข้อง	4
วันที่มีผลบังคับใช้และรอบระยะเวลาในการทบทวน	4
คำศัพท์และคำนิยาม	5
ภาพรวมทั่วไป	7
กรอบการบริหารความเสี่ยง	8
บทบาทและความรับผิดชอบ	10
ระดับความเสี่ยงที่ยอมรับได้	17
เครื่องมือและแนวทางการบริหารจัดการความเสี่ยง	17

ลำดับการปรับปรุงแก้ไข

ลำดับ.	สรุปการเปลี่ยนแปลงที่สำคัญ	วันที่อนุมัติ
1	• การเพิ่มสารบัญ หน้าที่ 2 • การเพิ่มลำดับการแก้ไขในหน้า 3 • การเพิ่มหัวข้อย่อยที่สำคัญ เช่น วัตถุประสงค์ ขอบเขตนโนบาย ข้อยกเว้นของการไม่ปฏิบัติตามนโยบาย กฎหมาย ระเบียบ และขั้นตอนที่เกี่ยวข้อง วันที่มีผลบังคับใช้ และความถี่ของการตรวจสอบ คำจำกัดความ ลักษณะทั่วไป บทบาทและความรับผิดชอบ กรอบการจัดการความเสี่ยง การยอมรับความเสี่ยง เครื่องมือและวิธีการจัดการความเสี่ยง • กรอบความเสี่ยงที่ปรับปรุงใหม่ (จาก COSO ERM 2004 เป็น COSO ERM 2017) เพื่อให้สอดคล้องกับแนวทางปฏิบัติปัจจุบัน	14 ก.พ. 2565 คณะกรรมการบริษัท
2	• ปรับปรุงถ้อยคำและรูปแบบเอกสาร เนื่องจากการเปลี่ยนชื่อบริษัทฯ และแก้ไขข้อความที่ไม่ถูกต้อง (ถ้ามี)	14 ก.พ. 2566 คณะกรรมการบริษัท
3	• ปรับปรุงบทบาทและความรับผิดชอบ • ปรับปรุงคำศัพท์และตัวย่อให้สอดคล้องกับบทบาทและความรับผิดชอบ • ปรับปรุงถ้อยคำของรายละเอียดระดับความเสี่ยงที่ยอมรับได้ เพื่อความเข้าใจที่ชัดเจน	14 ก.พ. 2567 คณะกรรมการบริษัท
4	• ปรับปรุงวัตถุประสงค์ และข้อยกเว้นของการไม่ปฏิบัติตามนโยบาย • ปรับปรุงถ้อยคำเพื่อความเข้าใจที่ชัดเจน	10 มี.ค. 2568 คณะกรรมการบริษัท

นโยบายบริหารความเสี่ยง

วัตถุประสงค์

วัตถุประสงค์โดยรวมของนโยบาย คือ เพื่อสร้างกรอบการบริหารความเสี่ยงขององค์กร (Enterprise Risk Management : ERM) ที่เหมาะสมและเพียงพอ ซึ่งช่วยให้องค์กรสามารถกำหนดบทบาทและความรับผิดชอบ ส่งเสริมความรับผิดชอบ และจัดการความเสี่ยงขององค์กรได้อย่างมีประสิทธิภาพ ดังนี้

1) ตระหนักว่าความเสี่ยงได้รับการพิจารณาในทุกกิจกรรม ตั้งแต่การกำหนดวัตถุประสงค์และกลยุทธ์ การตัดสินใจ และการดำเนินงานประจำวัน
2) ส่งเสริมความสม่ำเสมอของระเบียบวิธีการประเมินและกระบวนการบริหารความเสี่ยง
3) ตระหนักถึงความสำคัญของการติดตาม ตรวจสอบ สื่อสาร และรายงานความเสี่ยงอย่างถูกต้องและทันท่วงที รวมถึงมีกลไกแจ้งเตือนล่วงหน้าเพื่อการบริหารความเสี่ยงอย่างมีประสิทธิภาพ

ขอบเขตของนโยบาย

นโยบายนี้ใช้กับ บริษัท แรบบิท โฮลดิ้งส์ จำกัด (มหาชน) และบริษัทย่อย

ข้อยกเว้นของการไม่ปฏิบัติตามนโยบาย

ในกรณีที่ฝ่ายบริหารเห็นว่า ประเด็นใดของนโยบายไม่เหมาะสมต่อการนำไปใช้ จะต้องนำเรื่องดังกล่าวเสนอต่อคณะกรรมการบริษัทเพื่อพิจารณาก่อนที่กลุ่มบริษัทจะมีข้อผูกพันใด ๆ

กฎหมาย ข้อบังคับ นโยบาย และขั้นตอนที่เกี่ยวข้อง

1) Personal Data Protection Act, 2562 (2019) and further amendment
2) The Enterprise Risk Management Integrated Framework (COSO ERM 2017)

วันที่มีผลบังคับใช้และรอบระยะเวลาในการทบทวน

นโยบายนี้มีผลบังคับใช้ตั้งแต่วันที่คณะกรรมการบริษัทอนุมัติ โดยต้องได้รับการทบทวนเป็นประจำทุกปีหรือเมื่อจำเป็นต้องแก้ไขที่สำคัญ โดยการแก้ไขหรือทบทวนนโยบายนี้ต้องได้รับอนุมัติจากคณะกรรมการบริษัทก่อนประกาศใช้

คำศัพท์และคำนิยาม

คำศัพท์และคำนิยาม	ความหมาย
AC	คณะกรรมการตรวจสอบ
BOD	คณะกรรมการบริษัท
กรอบความเสี่ยงของธุรกิจ	**กรอบความเสี่ยงของธุรกิจ** สามารถนำไปใช้กับทุกแผนกเพื่อระบุความเสี่ยง โดยมีความเสี่ยงหลัก 4 ประเภท ดังนี้ ▪ **ความเสี่ยงเชิงกลยุทธ์ (Strategic Risk)** หมายถึง ความเป็นไปได้ที่เหตุการณ์ใด ๆ จะส่งผลกระทบต่อกลยุทธ์หรือรูปแบบธุรกิจของบริษัทฯ ความเสี่ยงเชิงกลยุทธ์ คือ ความเสี่ยงที่เกิดจากการไม่สามารถบรรลุวัตถุประสงค์ทางธุรกิจได้ ▪ **ความเสี่ยงด้านปฏิบัติการ (Operational Risk)** หมายถึง ความเสี่ยงที่บริษัทฯ ต้องเผชิญในการดำเนินงานประจำวัน เช่น ความล้มเหลวในกระบวนการผลิต การละเมิดความปลอดภัย การทุจริต การบริหารจัดการที่ผิดพลาด หรือภัยธรรมชาติ ▪ **ความเสี่ยงทางการเงิน (Financial Risk)** หมายถึง ความเสี่ยงที่เกี่ยวข้องกับด้านการเงิน เช่น ธุรกรรมทางการเงิน และการกู้ยืมของบริษัทฯ ที่อาจมีความเสี่ยงต่อการผิดนัดชำระหนี้ ▪ **ความเสี่ยงด้านการปฏิบัติตามกฎหมาย (Compliance Risk)** หมายถึง ความเป็นไปได้ที่บริษัทฯ อาจเผชิญกับบทลงโทษทางกฎหมาย การสูญเสียทางการเงิน หรือความเสียหายที่เกิดจากการไม่ปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้อง
การบริหารความเสี่ยง (Enterprise Risk Management – ERM)	คณะกรรมการบริหารความเสี่ยง สนับสนุนให้บริษัทฯ ปฏิบัติตามกรอบ The Enterprise Risk Management Integrated Framework (COSO ERM 2017)
ความเสี่ยงที่เกิดขึ้นใหม่	ความเสี่ยงที่ไม่เคยเกิดขึ้นมาก่อน ซึ่งอาจส่งผลกระทบต่อความสามารถในการบรรลุวัตถุประสงค์ทางกลยุทธ์ขององค์กร
การบริหารความเสี่ยงขององค์กร (ERM)	วัฒนธรรม ความรู้ความสามารถ และแนวปฏิบัติที่บูรณาการร่วมกับการกำหนดกลยุทธ์และผลการปฏิบัติงาน ซึ่งองค์กรใช้ในการบริหารความเสี่ยงเกี่ยวกับการสร้างคุณค่า การรักษาคุณค่า และการทำให้คุณค่าเกิดขึ้นจริง

คำศัพท์และคำนิยาม	ความหมาย
EXCOM	คณะกรรมการบริหาร
ผลกระทบ	ความรุนแรงของเหตุการณ์ที่มีความเสี่ยงหรือการคาดการณ์ว่าเหตุการณ์ความเสี่ยงดังกล่าวจะก่อให้เกิดความเสียหายในด้านต่าง ๆ เช่น การเงิน กฎหมาย นโยบายหรือข้อบังคับ ความล่าช้า หรือการหยุดชะงักในการดำเนินงาน ความเสียหายต่อภาพลักษณ์และชื่อเสียงของบริษัทฯ เป็นต้น
ความเสี่ยงสืบเนื่อง	ความเสี่ยงขององค์กร ซึ่งผู้บริหารยังไม่ได้ดำเนินการใด ๆ เพื่อที่จะลดความรุนแรงของความเสี่ยงนั้น
ตัวชี้วัดความเสี่ยง (KRIs)	เครื่องมือที่ใช้ติดตามความเคลื่อนไหวของความเสี่ยง ซึ่งจะบ่งบอกสัญญาณเตือนภัยความเสี่ยงล่วงหน้า (Early Signal)
โอกาส	ความถี่หรือความน่าจะเป็นที่เหตุการณ์ความเสี่ยงจะเกิดขึ้น
ความเสี่ยงที่คงเหลือ	ความเสี่ยงที่เหลืออยู่หลังจากที่ผู้บริหารได้ดำเนินการใด ๆ เพื่อที่จะลดความรุนแรงของความเสี่ยง
ความเสี่ยง	ความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้นและส่งผลกระทบต่อการบรรลุกลยุทธ์และวัตถุประสงค์ทางธุรกิจ โดยพิจารณาจากผลกระทบและโอกาสที่จะเกิดขึ้น
ระดับความเสี่ยงที่ยอมรับได้	ความเสี่ยงที่บริษัทฯ จะยอมรับได้และจะถูกบริหารจัดการโดยฝ่ายบริหารและหน่วยงานเจ้าของความเสี่ยง ทบทวนโดยทีมบริหารความเสี่ยง ประเมินโดยคณะกรรมการบริหาร (EXCOM) และอนุมัติโดยคณะกรรมการบริษัท (BOD)
วัฒนธรรมด้านความเสี่ยง	คุณค่า ความเชื่อ ความรู้ ทัศนคติ และความเข้าใจที่มีร่วมกันของผู้บริหารและพนักงานทุกระดับในองค์กรเกี่ยวกับความเสี่ยงที่ส่งผลต่อการตัดสินใจขององค์กร
ระดับความเสี่ยง	สถานะความเสี่ยงได้รับการประเมินจากความน่าจะเป็น และผลกระทบของแต่ละปัจจัยความเสี่ยง โดยมีสถานะความเสี่ยง 3 ระดับ คือ สูง กลาง และต่ำ

คำศัพท์และคำนิยาม	ความหมาย
การบริหารความเสี่ยง	กระบวนการที่คณะกรรมการ ผู้บริหาร และพนักงานทุกคนในบริษัทฯ ดำเนินการเพื่อช่วยในการกำหนดกลยุทธ์และการดำเนินงาน การบริหารความเสี่ยงมีไว้เพื่อระบุเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อบริษัทฯ เพื่อให้บริษัทฯ สามารถบริหารความเสี่ยงในระดับที่ยอมรับได้ และมีความเชื่อมั่นอย่างสมเหตุสมผลในการบรรลุวัตถุประสงค์
ลักษณะความเสี่ยง	มุมมองแบบองค์รวมต่อความเสี่ยงในระดับองค์กรหรือธุรกิจ ช่วยให้ผู้บริหารประเมินระดับความรุนแรงและความเชื่อมโยงของความเสี่ยงที่ส่งผลกระทบซึ่งกันและกัน การวิเคราะห์เชิงลึกนี้ช่วยให้สามารถคาดการณ์ผลกระทบที่อาจเกิดขึ้นต่อผลการดำเนินงาน และปรับกลยุทธ์ให้สอดคล้องกับเป้าหมายทางธุรกิจได้อย่างมีประสิทธิภาพ
การตอบสนองต่อความเสี่ยง	แนวทางที่ฝ่ายบริหารกำหนดและดำเนินการ การหลีกเลี่ยง การยอมรับ การลด และการโอนความเสี่ยง เป็นต้น โดยพิจารณาการตอบสนองความเสี่ยงดังกล่าวให้สอดคล้องกับช่วงความเสี่ยง (Risk Tolerance) และระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)
การยอมรับความเสี่ยง	ระดับความแปรปรวนที่ยอมรับได้เมื่อเทียบกับการบรรลุวัตถุประสงค์ที่กำหนด โดยวัดระดับความเสี่ยงที่สอดคล้องกับที่การประเมินวัตถุประสงค์ที่เกี่ยวข้อง

ภาพรวมทั่วไป

บริษัทฯ ให้ความสำคัญอย่างยิ่งกับการบริหารความเสี่ยง เนื่องจากการบริหารความเสี่ยงที่เหมาะสมจะช่วยให้บริษัทฯ บรรลุวัตถุประสงค์ทางธุรกิจและเติบโตอย่างยั่งยืน บริษัทฯ ได้จัดสรรทรัพยากรที่จำเป็นและเพียงพอเพื่อรองรับการบริหารความเสี่ยงในระดับที่ยอมรับได้ภายใต้กรอบนโยบายนี้ กรรมการ ผู้บริหาร และพนักงานทุกระดับ มีหน้าที่รับผิดชอบในการบริหารจัดการความเสี่ยงให้สอดคล้องกับนโยบายและกรอบการบริหารความเสี่ยงของบริษัทฯ

กรอบการบริหารความเสี่ยง

คณะกรรมการบริษัทได้ให้ความเห็นชอบต่อกรอบการบริหารความเสี่ยง ตามแนวทาง COSO ERM 2017 ซึ่งสอดคล้องกับระดับความเสี่ยงเชิงกลยุทธ์ที่เพิ่มขึ้นอันเป็นผลมาจากการเปลี่ยนแปลงทางเศรษฐกิจในปัจจุบัน โดยมีการบูรณาการเข้ากับกลยุทธ์และผลการดำเนินงาน เพื่อช่วยให้บริษัทฯ สามารถสร้าง ดำเนินการ และบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ

กรอบการบริหารความเสี่ยง ประกอบด้วย 5 องค์ประกอบหลัก และ 20 หลักการบริหารความเสี่ยงตามแนวทาง COSO ERM 2017 ซึ่งถูกนำไปใช้เป็นส่วนหนึ่งของกระบวนการดำเนินธุรกิจปกติ โดยครอบคลุมการกำกับดูแลและวัฒนธรรมองค์กร (Governance and Culture) การกำหนดกลยุทธ์และวัตถุประสงค์ (Strategy and Objective Setting) ผลการดำเนินงาน (Performance) การทบทวนและปรับปรุง (Review and Revision) และการสื่อสารและการรายงานข้อมูล (Information Communication and Reporting) โดยรายละเอียดดังต่อไปนี้

1) **การกำกับดูแล และวัฒนธรรม (Governance and Culture) (5 หลักการ)**
   การกำกับดูแล (Governance) กำหนดทิศทางและการให้ความสำคัญขององค์กร (Organization's tone) สร้างเสริมความตระหนักในด้านความสำคัญ และกำหนดความรับผิดชอบในการกำกับดูแลด้านการบริหารความเสี่ยงองค์กร

   วัฒนธรรมองค์กร (Culture) สะท้อนถึงคุณค่าด้านจริยธรรม พฤติกรรมที่พึงประสงค์ และความเข้าใจในเรื่องความเสี่ยงขององค์กร ทั้งนี้ การกำกับดูแลและวัฒนธรรมองค์กรครอบคลุมประเด็นต่อไปนี้

   - ควบคุมดูแลความเสี่ยงโดยคณะกรรมการ (Exercise Board Risk Oversight)
   - จัดตั้งโครงสร้างดำเนินการ (Establish Operating Structure)
   - กำหนดวัฒนธรรมที่พึงประสงค์ (Define Desired Culture)
   - แสดงให้เห็นถึงการยึดมั่นต่อคุณค่าหลัก (Demonstrate Commitment to Core Values)
   - ดึงดูด พัฒนา และรักษาบุคคลที่มีความสามารถ (Attract Develop and Retain Capable Individuals)

2) **กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy and Objective Setting) (4 หลักการ)**
   การบริหารความเสี่ยงองค์กร (Enterprise Risk Management) กลยุทธ์ (Strategy) และการกำหนดวัตถุประสงค์ (Objective Setting) ทำงานร่วมกันอย่างเป็นระบบในกระบวนการวางแผนเชิงกลยุทธ์ โดยมีการกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)

ให้สอดคล้องกับกลยุทธ์ โดยเชื่อมโยงกับกลยุทธ์ขององค์กร ซึ่งมีการระบุ ประเมิน และตอบสนองความเสี่ยงต่างๆ โดยอ้างอิงวัตถุประสงค์ทางธุรกิจขององค์กร

กลยุทธ์และการกำหนดวัตถุประสงค์ ประกอบด้วยหลักการที่สำคัญ ดังต่อไปนี้

- วิเคราะห์บริบททางธุรกิจ (Analyze Business Context)
- กำหนดระดับความเสี่ยงที่ยอมรับได้ (Define Risk Appetite)
- ประเมินกลยุทธ์ทางเลือก (Evaluate Alternative Strategies)
- กำหนดวัตถุประสงค์ทางธุรกิจ (Formulate Business Objectives)

3) ผลการปฏิบัติงาน (Performance) (5 หลักการ)

องค์กรควรระบุและประเมินความเสี่ยงที่อาจส่งผลกระทบต่อการบรรลุกลยุทธ์และวัตถุประสงค์ขององค์กร ซึ่งมีการจัดลำดับความสำคัญของความเสี่ยง (Risk Prioritization) โดยพิจารณาความรุนแรงของความเสี่ยง (Severity) เปรียบเทียบกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) กำหนดวิธีการตอบสนองความเสี่ยง (Risk Responses) และพิจารณาภาพรวมความเสี่ยงขององค์กร (Portfolio View of Risk) ทั้งนี้ ผลของการประเมินความเสี่ยงจะต้องรายงานต่อผู้มีส่วนได้เสียที่สำคัญที่เกี่ยวข้องกับกระบวนการบริหารความเสี่ยง

ผลการปฏิบัติงานประกอบด้วยหลักการที่สำคัญ ดังต่อไปนี้

- ระบุความเสี่ยง (Identify Risk)
- ประเมินความรุนแรงของความเสี่ยง (Assess Severity of Risks)
- จัดลำดับความสำคัญของความเสี่ยง (Prioritize Risks)
- นำวิธีการตอบสนองความเสี่ยงไปปฏิบัติ (Implement Risk Responses)
- พัฒนาภาพรวมความเสี่ยง (Develop Portfolio View)

4) การสอบทานและการแก้ไขปรับปรุง (Review and Revision) (3 หลักการ)

องค์กรสามารถพิจารณาผลการดำเนินงานด้านการบริหารความเสี่ยงองค์กร ผ่านการสอบทานผลการปฏิบัติงานขององค์กรในแง่ของการเปลี่ยนแปลงที่สำคัญ และการแก้ไขปรับปรุงที่จำเป็น

การสอบทานและการแก้ไขปรับปรุงประกอบด้วยหลักการที่สำคัญ ดังต่อไปนี้

- ประเมินการเปลี่ยนแปลงที่สำคัญ (Assess Substantial Change)
- สอบทานความเสี่ยงและผลการปฏิบัติงาน (Review Risk and Performance)
- พยายามปรับปรุงการบริหารความเสี่ยงขององค์กรอย่างต่อเนื่อง (Pursue Improvement in Enterprise Risk Management)

5) **สารสนเทศ การสื่อสาร และการรายงาน (Information Communication and Reporting) (3 หลักการ)**

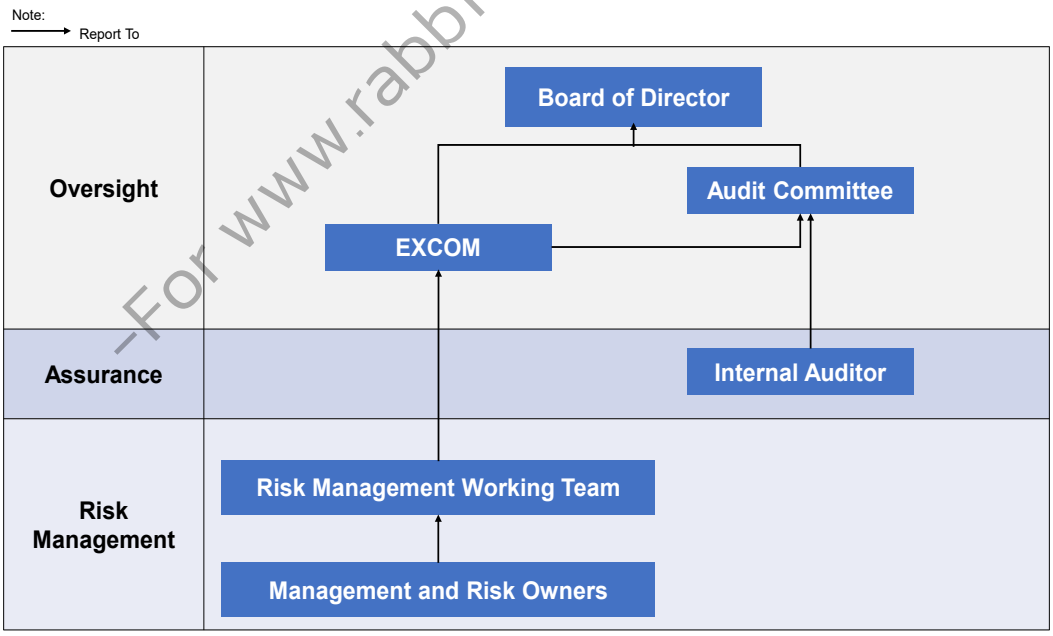
การบริหารความเสี่ยงขององค์กรต้องมีกระบวนการรับและแลกเปลี่ยนข้อมูลที่สำคัญอย่างต่อเนื่อง ทั้งข้อมูลภายในและภายนอกองค์กร มีความสำคัญและจำเป็นสำหรับการบริหารความเสี่ยงองค์กร

สารสนเทศ การสื่อสาร และการรายงานประกอบด้วยหลักการที่สำคัญ ดังต่อไปนี้

- ใช้ประโยชน์จากสารสนเทศและเทคโนโลยี (Leverage Information and Technology)
- สื่อสารสารสนเทศด้านความเสี่ยง (Communicate Risk Information)
- รายงานความเสี่ยง วัฒนธรรมและผลการปฏิบัติงาน (Report on Risk Culture and Performance)

บทบาทและความรับผิดชอบ

การจัดตั้งโครงสร้างความเสี่ยงอย่างเป็นทางการช่วยให้กำหนดความรับผิดชอบ บทบาท และหน้าที่ของผู้ที่เกี่ยวข้องในกระบวนการบริหารความเสี่ยงทั่วทั้งบริษัทฯ ได้อย่างชัดเจน นอกจากนี้ ยังช่วยกำหนดอำนาจการตัดสินใจด้านความเสี่ยง และสร้างระบบการสื่อสารและรายงานข้อมูลความเสี่ยงให้มีประสิทธิภาพมากขึ้น



รูป (1) – โครงสร้างการบริหารความเสี่ยงองค์กร

1. คณะกรรมการบริษัท (The Company Board of Directors, BOD)

1.1. ธรรมาภิบาลและวัฒนธรรมองค์กร (Governance and Culture)

- กำหนดแนวทางและค่านิยมขององค์กรให้สอดคล้องกับวัฒนธรรมด้านความเสี่ยงที่ต้องการ รวมถึงวิสัยทัศน์ พันธกิจ และค่านิยมองค์กร
- อนุมัติและทบทวนนโยบายบริหารความเสี่ยง
- ประเมินความเหมาะสมของกรอบการบริหารความเสี่ยง
- ส่งเสริมวัฒนธรรมองค์กร โดยสื่อสารให้พนักงานทุกคนตระหนักถึงความสำคัญของการบริหารความเสี่ยง และนำไปประยุกต์ใช้ในทุกแผนก
- มอบหมายให้คณะกรรมการบริหาร รับผิดชอบการบริหารความเสี่ยงขององค์กรโดยรวม การประเมินความเสี่ยง และโครงสร้างการบริหารความเสี่ยงขององค์กร

1.2. กลยุทธ์และการกำหนดเป้าหมาย (Strategic and Objective-Setting)

- กำหนดกลยุทธ์และเป้าหมายทางธุรกิจขององค์กร รวมถึงทำความเข้าใจความเสี่ยงที่เกี่ยวข้องกับกลยุทธ์
- อนุมัติและทบทวนระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และระดับความเบี่ยนเบนของความเสี่ยงที่องค์กรยอมรับได้ (Risk Tolerance)
- กำกับดูแลและให้คำแนะนำแก่ฝ่ายบริหารในการกำหนดกลยุทธ์และเป้าหมายทางธุรกิจให้สอดคล้องกับความเสี่ยง วิสัยทัศน์ พันธกิจ และวัฒนธรรมองค์กร

1.3. การประเมินผลการปฏิบัติงาน (Risk Assessment)

- อนุมัติแนวทางการบริหารความเสี่ยงของบริษัทฯ ซึ่งรวมถึงการประเมินความเสี่ยง การตอบสนองความเสี่ยง และแผนการลดความเสี่ยงตามที่ฝ่ายบริหารเสนอ
- กำกับดูแล และติดตามให้มีการบริหารจัดการความเสี่ยงอย่างเหมาะสม

1.4. การทบทวนและปรับปรุง (Review and Revision)

- หารือกับฝ่ายบริหารเพื่อตรวจสอบความเสี่ยงที่สำคัญ ซึ่งส่งผลต่อการดำเนินงานของบริษัทฯ รวมถึงการเปลี่ยนแปลงในบริบททางธุรกิจที่อาจกระทบต่อวิสัยทัศน์ พันธกิจ ค่านิยม กลยุทธ์ และเป้าหมายขององค์กร

1.5. การสื่อสารและรายงานข้อมูลความเสี่ยง (Risk Information Communication and Reporting)

- เน้นย้ำการบริหารความเสี่ยงโดยรายงานให้คณะกรรมการบริหารรับทราบอย่างน้อยปีละ 1 ครั้ง
- ส่งเสริมการรายงานความเสี่ยงที่สำคัญอย่างสม่ำเสมอ เพื่อสนับสนุนการตัดสินใจอย่างมีประสิทธิภาพ พร้อมให้คำแนะนำเกี่ยวกับแนวทางการรับมือและแผนดำเนินการที่เหมาะสม
- พิจารณาอนุมัติรายงานความเสี่ยงและสถานะ KRI ของบริษัทฯ

2. คณะกรรมการตรวจสอบ (Audit Committee)

- เพื่อประเมินความเพียงพอของนโยบายการบริหารความเสี่ยง ระบบการควบคุมภายใน และระบบการตรวจสอบภายใน
- ส่งเสริมให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการบริหารองค์กร โดยกำหนดให้มีการพิจารณาความเสี่ยงเป็นวาระสำคัญอย่างน้อยปีละหนึ่งครั้ง
- ให้คำแนะนำและพิจารณารายงานการตรวจสอบจากฝ่ายตรวจสอบภายในเป็นประจำ เพื่อเสริมสร้างประสิทธิภาพและความน่าเชื่อถือของระบบควบคุมภายใน
- ให้คำแนะนำเกี่ยวกับนโยบายและคู่มือบริหารความเสี่ยงขององค์กร รวมถึงแผนตรวจสอบภายใน ผลการตรวจสอบ การทุจริต และข้อบกพร่องในระบบควบคุมภายใน พร้อมนำเสนอต่อคณะกรรมการบริษัท
- สนับสนุนให้มีการพัฒนาและปรับปรุงกระบวนการบริหารความเสี่ยงอย่างต่อเนื่อง เพื่อให้สอดคล้องกับสถานการณ์และความท้าทายที่เปลี่ยนแปลง
- พิจารณารายงานจากคณะกรรมการบริหารเกี่ยวกับผลการดำเนินงานด้านการบริหารความเสี่ยง พร้อมทบทวนและตั้งคำถามต่อการประเมินความเสี่ยงของฝ่ายบริหารตามความเหมาะสม

3. คณะกรรมการบริหาร (EXCOM)

3.1. ธรรมาภิบาลและวัฒนธรรมองค์กร (Governance and Culture)

- กำหนดให้มีคณะทำงานบริหารความเสี่ยง โดยมีผู้บริหารและผู้ประสานงานด้านความเสี่ยงจากทุกแผนก เพื่อเสริมสร้างการบริหารความเสี่ยงให้มีประสิทธิภาพและสอดคล้องกับเป้าหมายขององค์กร
- กำกับดูแล และติดตามการบริหารความเสี่ยงขององค์กร เพื่อให้แน่ใจว่ามีการดำเนินงานที่เหมาะสม และเป็นไปตามมาตรฐานที่กำหนด
- ส่งเสริมและรักษาวัฒนธรรมการบริหารความเสี่ยงให้เป็นส่วนหนึ่งขององค์กรอย่างต่อเนื่อง

- ทบทวนและปรับปรุงนโยบายและแนวปฏิบัติด้านการบริหารความเสี่ยง ให้สอดคล้องกับแนวทางมาตรฐานสากล เช่น ERM COSO
- อนุมัติและทบทวนคู่มือการจัดการบริหารความเสี่ยง

3.2. กลยุทธ์และการกำหนดเป้าหมาย (Strategic and Objective-Setting)

- เพื่อกำหนดแนวทางในการพิจารณาความเสี่ยงในการกำหนดกลยุทธ์และวัตถุประสงค์ทางธุรกิจโดยฝ่ายบริหาร
- เพื่อกำกับดูแลและให้ฝ่ายบริหารรับผิดชอบในการระบุและจัดการความเสี่ยงต่อการบรรลุวัตถุประสงค์
- เพื่อประเมินความยอมรับความเสี่ยงและความอดทนต่อความเสี่ยงที่บริษัทฯ จะยอมรับในการบรรลุวัตถุประสงค์ทางธุรกิจ

3.3. การประเมินผลการปฏิบัติงาน (Risk Assessment)

- กำกับดูแลการบริหารความเสี่ยงขององค์กร ประเมินความเสี่ยง และวางโครงสร้างการจัดการความเสี่ยงขององค์กร

3.4. การทบทวนและปรับปรุง (Review and Revision)

- ตรวจสอบและปรับปรุงการประเมินความเสี่ยงขององค์กร โดยแก้ไขเมื่อมีความเสี่ยงสำคัญเกิดขึ้นระหว่างปี เพื่อให้แน่ใจว่าความเสี่ยงอยู่ในระดับที่เหมาะสมและยอมรับได้ตามนโยบายของบริษัทฯ
- ติดตามความคืบหน้าของแผนบริหารความเสี่ยงและตัวชี้วัดความเสี่ยงที่สำคัญ

3.5. การสื่อสารและรายงานข้อมูลความเสี่ยง (Risk Information Communication and Reporting)

- รายงานผลการจัดการบริหารความเสี่ยงให้แก่คณะกรรมการบริษัท และคณะกรรมการตรวจสอบรับทราบ อย่างน้อยปีละ 1 ครั้ง
- รายงานความเสี่ยงสำคัญต่อคณะกรรมการบริษัท และคณะกรรมการตรวจสอบอย่างทันท่วงที
- รายงานข้อมูลหรือประเด็นที่เกี่ยวข้องกับความเสี่ยงขององค์กรต่อคณะกรรมการตรวจสอบอย่างสม่ำเสมอ
- พิจารณาและทบทวนการเปิดเผยข้อมูลเกี่ยวกับการบริหารความเสี่ยงขององค์กรในรายงานประจำปี (แบบ 56-1 One Report)

4. **ฝ่ายตรวจสอบภายใน (Internal Audit)**

- จัดทำแผนตรวจสอบภายในโดยคำนึงถึงความเสี่ยงขององค์กรและความเสี่ยงจากการทุจริต
- ดำเนินการตรวจสอบภายในเพื่อประเมินความเพียงพอ และประสิทธิผลของกระบวนการจัดการความเสี่ยง และแผนปฏิบัติการ รวมถึงให้คำแนะนำที่เหมาะสมแก่ฝ่ายบริหารและหน่วยงานเจ้าของความเสี่ยง
- ทำงานร่วมกับทีมบริหารความเสี่ยงของบริษัทฯ เพื่อร่วมพิจารณาและติดตามความเสี่ยงอย่างต่อเนื่อง

5. **คณะทำงานบริหารความเสี่ยง (Risk Management Working Team)**

ทีมบริหารความเสี่ยงประกอบด้วยตัวแทนจากฝ่ายงานต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัทฯ

5.1. ธรรมาภิบาลและวัฒนธรรมองค์กร (Governance and Culture)

- การเตรียมพร้อม และปรับปรุง กรอบการบริหารความเสี่ยง นโยบาย ขั้นตอนปฏิบัติ และคู่มือ เสนอต่อคณะกรรมการบริษัท คณะกรรมการบริหาร และประธานเจ้าหน้าที่บริหารตามลำดับ เพื่อพิจารณาและแจ้งให้ฝ่ายบริหารและหน่วยงานเจ้าของความเสี่ยงทราบ

5.2. กลยุทธ์และการกำหนดเป้าหมาย (Strategic and Objective-Setting)

- เพื่อให้คำแนะนำและสนับสนุนในการดำเนินการตามนโยบายการจัดการความเสี่ยงในการกำหนดกลยุทธ์และวัตถุประสงค์แก่ผู้บริหารและหน่วยงานเจ้าของความเสี่ยง

5.3. การประเมินผลการปฏิบัติงาน (Risk Assessment)

- ดำเนินกิจกรรมการบริหารความเสี่ยงให้เป็นไปตามกรอบการบริหารความเสี่ยงที่ได้รับอนุมัติ
- เพื่อให้คำแนะนำและอำนวยความสะดวกในกระบวนการประเมินความเสี่ยงแก่ฝ่ายบริหารและหน่วยงานเจ้าของความเสี่ยง

5.4. การทบทวนและปรับปรุง (Review and Revision)

- เพื่อตรวจสอบและให้ความมั่นใจว่ามีการทบทวนและปรับปรุงผลการประเมินความเสี่ยงในกรณีที่มีการเปลี่ยนแปลงที่สำคัญหรือความเสี่ยงหลักเกิดขึ้น
- เพื่อติดตามความคืบหน้าของแผนการบรรเทาความเสี่ยง
- เพื่อทบทวนและปรับปรุงประสิทธิภาพและประโยชน์ของกระบวนการจัดการความเสี่ยงที่มีอยู่

5.5. การสื่อสารและรายงานข้อมูลความเสี่ยง (Risk Information Communication and Reporting)

- รายงานผลการจัดการบริหารความเสี่ยงและตัวชี้วัด (KRI) ให้คณะกรรมการบริษัทรับทราบอย่างน้อยไตรมาสละ 1 ครั้ง และรายงานต่อคณะกรรมการบริหาร และคณะกรรมการตรวจสอบ อย่างน้อยปีละ 1 ครั้ง
- ประสานงานร่วมกับฝ่ายตรวจสอบภายในและแผนกที่เกี่ยวข้อง เพื่อสื่อสารและติดตามประเด็นความเสี่ยงขององค์กร
- พิจารณาและทบทวนการเปิดเผยข้อมูลเกี่ยวกับการบริหารความเสี่ยงขององค์กรในรายงานประจำปี (แบบ 56-1 One Report)

6. ฝ่ายบริหาร และหน่วยงานเจ้าของความเสี่ยง (Management and Risk Owners)

ฝ่ายบริหารและหน่วยงานเจ้าของความเสี่ยง เป็นผู้รับผิดชอบกระบวนการต่าง ๆ ซึ่งรวมถึงหัวหน้าฝ่าย ปฏิบัติการ ผู้บริหาร และพนักงาน

6.1. ธรรมาภิบาลและวัฒนธรรมองค์กร (Governance and Culture)

- ส่งเสริมและสนับสนุนวัฒนธรรมการบริหารความเสี่ยงภายในองค์กร
- มีส่วนร่วมในการติดตามและประเมินความเสี่ยงที่เกี่ยวข้อง
- ปฏิบัติตามนโยบายและแนวทางการบริหารความเสี่ยงของบริษัทฯ

6.2. กลยุทธ์และการกำหนดเป้าหมาย (Strategic and Objective-Setting)

- เพื่อกำหนดกลยุทธ์และวัตถุประสงค์ทางธุรกิจที่สอดคล้องกับภารกิจ วิสัยทัศน์ และกลยุทธ์ขององค์กร
- กำหนดขอบเขตความเสี่ยงที่ยอมรับได้ให้เหมาะสมกับกลยุทธ์และเป้าหมายทางธุรกิจ

6.3. การประเมินผลการปฏิบัติงาน (Risk Assessment)

- เพื่อระบุเหตุการณ์ความเสี่ยงภายในและภายนอกที่มีผลกระทบต่อทั้งระดับกระบวนการและระดับบริษัท และจัดเตรียมข้อมูลความเสี่ยง รวมถึงความเสี่ยงตามลักษณะของธุรกิจและความเสี่ยงที่เกิดขึ้นใหม่
- ดำเนินการประเมินความเสี่ยงและกำหนดลำดับความสำคัญของความเสี่ยง
- เลือกและดำเนินการตอบสนองความเสี่ยงที่เหมาะสม เพื่อจัดการความเสี่ยงแต่ละเรื่องให้สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้

6.4. การทบทวนและปรับปรุง (Review and Revision)

- ระบุ ติดตาม และพิจารณาความเสี่ยงทั้งภายในและภายนอกที่ส่งผลกระทบต่อระดับกระบวนการและระดับบริษัท รวมถึงการเปลี่ยนแปลงที่สำคัญหรือความเสี่ยงเชิงกลยุทธ์ที่เกิดขึ้นระหว่างปี พร้อมปรับปรุงข้อมูลด้านความเสี่ยงให้เป็นปัจจุบัน
- ดำเนินการตามแผนลดความเสี่ยงและรายงานผลการดำเนินงาน
- เพื่อดำเนินการปรับปรุงกระบวนการบริหารความเสี่ยงอย่างสม่ำเสมอ
- เพื่อประเมินระดับความรุนแรงของการปรับปรุงข้อมูลความเสี่ยง

6.5. การสื่อสารและรายงานข้อมูลความเสี่ยง (Risk Information Communication and Reporting)

- มีการระบุ ติดตาม และปรับปรุงสถานะของ KRIs ให้กับคณะทำงานบริหารความเสี่ยงทุกไตรมาส เพื่อใช้เครื่องมือและวิธีการที่เหมาะสมในการสนับสนุนกระบวนการประเมินความเสี่ยง (ERM)

การรายงานความเสี่ยง	ผู้รับผิดชอบ	รอบเวลา	ผู้รับทราบการรายงาน
1. รายงานผลประเมินความเสี่ยงและความคืบหน้าของการดำเนินการ	- คณะทำงานบริหารความเสี่ยง - คณะกรรมการบริษัท	ไตรมาสละ 1 ครั้ง และ ประจำปี 1 ครั้ง	คณะกรรมการบริหาร คณะกรรมการตรวจสอบ / คณะกรรมการบริษัท
2. รายงานผลการติดตามตัวชี้วัดความเสี่ยง (KRIs)	- คณะทำงานบริหารความเสี่ยง - คณะกรรมการบริษัท	ไตรมาสละ 1 ครั้ง และ ประจำปี 1 ครั้ง	คณะกรรมการบริหาร คณะกรรมการตรวจสอบ / คณะกรรมการบริษัท
3. รายงานผลประเมินความเสี่ยงและความคืบหน้าของการดำเนินการ	- ฝ่ายบริหาร - หน่วยงานเจ้าของความเสี่ยง	ไตรมาสละ 1 ครั้ง	คณะทำงานบริหารความเสี่ยง
4. รายงานการประเมินความเสี่ยงและการควบคุม (RCSA Report)	- ฝ่ายบริหาร - หน่วยงานเจ้าของความเสี่ยง	ไตรมาสละ 1 ครั้ง	ฝ่ายตรวจสอบภายใน / คณะทำงานบริหารความเสี่ยง
5. รายงานการบริหารความต่อเนื่องทางธุรกิจ	- ฝ่ายบริหาร - หน่วยงานเจ้าของความเสี่ยง	ไตรมาสละ 1 ครั้ง	ฝ่ายตรวจสอบภายใน / คณะทำงานบริหารความเสี่ยง

ระดับความเสี่ยงที่ยอมรับได้

บริษัทฯ กำหนดระดับความเสี่ยงที่ยอมรับได้ เพื่อแสดงระดับความเสี่ยงหรือระดับความเสียหายที่สามารถยอมรับได้ การยอมรับความเสี่ยงจะถูกรวบรวมโดยฝ่ายบริหารและหน่วยงานเจ้าของความเสี่ยง ตรวจสอบโดยคณะทำงานบริหารความเสี่ยง ประเมินโดยคณะกรรมการบริหาร และอนุมัติโดยคณะกรรมการบริษัท

เครื่องมือและแนวทางการบริหารจัดการความเสี่ยง

เครื่องมือและแนวทางการบริหารจัดการความเสี่ยงได้รับการออกแบบและจัดทำขึ้นเพื่อให้มีประสิทธิภาพและประสิทธิผล ในการระบุ ประเมิน ติดตาม ควบคุม และรายงานความเสี่ยง โดยมีรายละเอียดดังต่อไปนี้

1. **การประเมินตนเองด้านความเสี่ยงและการควบคุม (RCSA)**

   RCSA เตรียมพร้อมสำหรับการระบุความเสี่ยง การประเมิน และประสิทธิภาพการควบคุมภายในเพื่อให้แน่ใจถึงประสิทธิผลของการจัดการความเสี่ยงและการควบคุม

2. **ตัวชี้วัดความเสี่ยง (KRIs) รายงานผลการติดตาม**

   KRI เป็นเครื่องมือแจ้งเตือนล่วงหน้าเพื่อติดตามแนวโน้มความเสี่ยงของบริษัทฯ นอกจากนี้ ยังช่วยแจ้งเตือนผู้บริหารเกี่ยวกับการเปลี่ยนแปลงระดับความเสี่ยงที่สำคัญเพื่อใช้ในการควบคุมและตรวจสอบ

3. **การบริหารจัดการความต่อเนื่องของธุรกิจ**

   โครงสร้างการบริหารความต่อเนื่องทางธุรกิจของบริษัทฯ ประกอบด้วย บทบาท หน้าที่ โครงสร้างและกระบวนการต่าง ๆ เพื่อให้มั่นใจว่าในกรณีที่เกิดการหยุดชะงักของธุรกิจ กิจกรรมของบริษัทฯ จะสามารถดำเนินการต่อไปได้และกลับสู่ภาวะปกติได้อย่างทันท่วงที

นายคีรี กาญจนพาสน์
ประธานคณะกรรมการ
บริษัท แรบบิท โฮสดิ้งส์ จำกัด (มหาชน)