Thai Institute of Directors

แนวปฏิบัติที่ดี สำหรับคณะกรรมการ ด้านการบริหารความเสี่ยง

Guideline on Board's Oversight
Role in Risk Management

สารบัญ

© 2022 Thai Institute of Directors Association. All rights reserved.

Thai IOD and the officers, authors and editors of Thai IOD make no representation or warranty as to the accuracy, completeness or legality of any of the information contained herein. The material is for general information only and is not intended as advice on any of the matters discussed. Each recipient should consult their professional advisers for advice in relation to a specific matter affecting them.

By accepting this material, each recipient agrees that Thai IOD and the officers, authors and editors of Thai IOD shall not have any liability for any information contained in, or for any omission from, this material.

In addition, by accepting this material, the recipient agrees to utilize the information contained herein solely for the purpose of personal use for professional development purpose.

Copyright in this material is strictly reserved. Any distribution or reproduction of any part of this material without the prior written permission of Thai IOD, the copyright owners is strictly prohibited.

บทนำ

การดำเนินธุรกิจในปัจจุบันมีความยากลำบากอย่างยิ่ง เพราะอยู่ท่ามกลางสภาพแวดล้อมที่เต็มไปด้วยความไม่แน่นอนและการเปลี่ยนแปลงที่อาจเกิดขึ้นอย่างฉับพลัน (Disruption) ซึ่งไม่มีผู้ใดคาดเดาได้อย่างแม่นยำ เช่น การเปลี่ยนแปลงของเทคโนโลยี การเกิดโรคระบาด การเกิดภัยธรรมชาติ การเปลี่ยนแปลงผู้บริหาร การแข่งขัน การออกกฎเกณฑ์ใหม่ๆ การกีดกันทางการค้า ฯลฯ

บริษัทที่จะอยู่ได้อย่างยั่งยืนในโลกยุคใหม่นี้ ต้องเป็นบริษัทที่มีพื้นฐานแข็งแกร่งและมีความยืดหยุ่นต่อการปรับเปลี่ยนกลยุทธ์และการบริหารภายใต้กฎระเบียบต่างๆ ที่กำกับบริษัทอยู่ รวมถึงต้องมีคณะกรรมการและฝ่ายจัดการที่มีศักยภาพในการขับเคลื่อนองค์กรเพื่อตอบสนองความคาดหวังของผู้มีส่วนได้ส่วนเสียกลุ่มต่างๆ ได้อย่างรอบด้าน ตลอดจนสามารถรับมือกับ “ปัจจัยเสี่ยง” ต่างๆ ที่องค์กรเผชิญอยู่ได้อย่างเหมาะสม

ในการกำกับดูแลให้กลไกการบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิภาพนั้น คณะกรรมการจะต้องมีความเข้าใจใน “ความเสี่ยงสำคัญ” (Key Risks) ต่างๆ ขององค์กร ตลอดจน “กระบวนการ” ในการบริหารจัดการความเสี่ยงเหล่านั้น (เริ่มตั้งแต่การระบุ การประเมิน การจัดการ ไปจนถึงการรายงานความเสี่ยง) โดยคณะกรรมการมีหน้าที่ติดตามการดำเนินงานของฝ่ายจัดการตามกระบวนการข้างต้น เพื่อให้มั่นใจว่าความเสี่ยงสำคัญๆ ขององค์กรได้รับการควบคุม หรือถูกบริหารจัดการให้อยู่ในระดับที่ยอมรับได้ ทั้งนี้ คณะกรรมการอาจพิจารณาแต่งตั้ง “คณะกรรมการบริหารความเสี่ยง” (Risk Management Committee) ขึ้นมาเป็นการเฉพาะ เพื่อช่วยแบ่งเบาภาระหน้าที่ในการกำกับดูแลเรื่องดังกล่าวก็ได้

ด้วยเหตุนี้ สถาบันกรรมการบริษัทไทย (IOD) จึงได้จัดทำแนวปฏิบัติที่ดีฉบับนี้ขึ้น เพื่อให้คณะกรรมการ ฝ่ายจัดการ ตลอดจนส่วนงานที่เกี่ยวข้องได้ตระหนักถึงความสำคัญ และเข้าใจถึงองค์ประกอบ บทบาทหน้าที่ และแนวทางในการเพิ่มพูนประสิทธิภาพของระบบบริหารความเสี่ยงที่มีอยู่ในปัจจุบัน เพื่อช่วยให้องค์กรสามารถดำรงอยู่และเจริญเติบโตได้อย่างยั่งยืนต่อไป

• สถาบันกรรมการบริษัทไทย (IOD) •

รายนามคณะทำงานพิจารณาแนวปฏิบัติที่ดีด้าน ESG สำหรับคณะกรรมการ ประจำปี 2564

1. นายกุลเวช	**เจนวัฒนวิทย์**	กรรมการผู้อำนวยการ สถาบันกรรมการบริษัทไทย (ประธานคณะทำงาน)
2. นายรพี	**สุจริตกุล**	อดีตที่ปรึกษา สถาบันกรรมการบริษัทไทย (ที่ปรึกษาคณะทำงาน)
3. นายวีรศักดิ์	**โฆสิตไพศาล**	กรรมการ สถาบันกรรมการบริษัทไทย
4. ผู้แทนจากตลาดหลักทรัพย์แห่งประเทศไทย		
นางสินีนาฏ	แจ่มศรี	ผู้อำนวยการฝ่ายพัฒนาบรรษัทภิบาล
นายพรชัย	ถาวรานนท์	รองผู้อำนวยการฝ่ายพัฒนาบรรษัทภิบาล
นายสุรพล	บุพโกสุม	รองผู้อำนวยการฝ่ายพัฒนาบรรษัทภิบาล
5. ผู้แทนจากกองทุนบำเหน็จบำนาญข้าราชการ		
นายศุภวิท	โชติวิท	ผู้อำนวยการอาวุโสและผู้บริหารฝ่ายวิเคราะห์การลงทุน
6. ผู้แทนจากสมาคมบริษัทจัดการลงทุน		
นางวรวรรณ	ธาราภูมิ	ประธานกิตติมศักดิ์
นางสาวดวงกมล	พิศาล	เลขาธิการ
7. ผู้ที่มีประสบการณ์ในการปฏิบัติหน้าที่กรรมการบริษัทจดทะเบียน		
นายยุทธ	วรฉัตรธาร	ผู้เชี่ยวชาญพิเศษด้านบรรษัทภิบาลและความรับผิดชอบต่อสังคม ตลาดหลักทรัพย์แห่งประเทศไทย
นางภัทรียา	เบญจพลชัย	ผู้เชี่ยวชาญพิเศษด้านบรรษัทภิบาลและความรับผิดชอบต่อสังคม ตลาดหลักทรัพย์แห่งประเทศไทย
8. ผู้ที่มีประสบการณ์ในการปฏิบัติหน้าที่เลขานุการบริษัท		
นางกอบบุญ	ศรีชัย	เลขานุการบริษัท และรองกรรมการผู้จัดการอาวุโส บริษัท เจริญโภคภัณฑ์อาหาร จำกัด (มหาชน)
นางศิริบรรจง	อุทโยภาศ	เลขานุการบริษัท และผู้ช่วยผู้จัดการใหญ่ ผู้บริหารสูงสุด Corporate Office ธนาคารไทยพาณิชย์ จำกัด (มหาชน)
นางบุญศิริ	จารุศิริ	อดีตเลขานุการบริษัท และที่ปรึกษา บริษัท บ้านปู จำกัด (มหาชน)
9. ผู้เชี่ยวชาญด้านการกำกับดูแลกิจการ		
นางวารุณี	ปรีดานนท์	หุ้นส่วน - ที่ปรึกษาการกำกับดูแลกิจการ การบริหารความเสี่ยง การควบคุมภายใน และการตรวจสอบภายใน บริษัท ไพร้ซวอเตอร์เฮาส์คูเปอร์ส เอบีเอเอส จำกัด
10. ฝ่าย Knowledge สถาบันกรรมการบริษัทไทย (ฝ่ายเลขานุการคณะทำงาน)		
นางศิรินันท์	กิตติเวทางค์	รองกรรมการผู้อำนวยการ - Knowledge (Research & Development and Curriculum & Facilitators)
นายธนกร	พรรัตนานุกูล	รองผู้ช่วยกรรมการผู้อำนวยการ – Curriculum & Facilitators
นายอภิลาภ	เผ่าภิญโญ	CG Supervisor – Research & Development
นางสาวจาร์รวี	จีระมะกร	Senior CG Analyst - Curriculum & Facilitators

ส่วนที่ 1

หลักการสำคัญ
(Key Principles)

ส่วนที่ 1 หลักการสำคัญ (Key Principles)

1. คณะกรรมการพึงใช้แนวคิดการบูรณาการ GRC (Governance, Risk and Compliance) ในการกำกับดูแลองค์กร เพื่อส่งเสริมองค์กรให้มีความก้าวหน้าและยั่งยืน *(โปรดดูแนวปฏิบัติ 1)*

2. การบริหารความเสี่ยงเป็นองค์ประกอบสำคัญของการบูรณาการ GRC เพราะทำให้องค์กรมีความตระหนักและสามารถรับมือกับเหตุการณ์ที่อาจเกิดขึ้นในอนาคต ที่มีผลเชิงลบต่อการบรรลุกลยุทธ์ วัตถุประสงค์ และความคาดหวังของผู้มีส่วนได้ส่วนเสีย *(โปรดดูแนวปฏิบัติ 1)*

3. คณะกรรมการควรมีส่วนร่วมในการกำหนดและติดตามการนำกลยุทธ์ไปปฏิบัติ และกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ที่สอดรับกับการดำเนินกลยุทธ์นั้น โดยควรมีการหารือร่วมกันระหว่างคณะกรรมการและผู้บริหารระดับสูง *(โปรดดูแนวปฏิบัติ 1)*

4. คณะกรรมการควรทำให้ระบบบริหารความเสี่ยงและควบคุมภายในเป็นกระบวนการทำงานปกติทุกๆ วัน ไม่ควรทำให้เป็นกิจกรรมที่แยกต่างหากและทำเป็นครั้งคราว *(โปรดดูแนวปฏิบัติ 1)*

5. คณะกรรมการควรกำกับดูแลให้การบริหารความเสี่ยงถูกนำไปปฏิบัติแบบบูรณาการและสอดรับกับกระบวนการบริหารจัดการด้านความยั่งยืน อันครอบคลุมทั้งมิติด้านสิ่งแวดล้อม สังคม และการกำกับดูแลกิจการ (Environmental, Social and Governance หรือ ESG) *(โปรดดูแนวปฏิบัติ 1)*

6. คณะกรรมการสามารถกำกับดูแลการบริหารความเสี่ยงเอง หรือจัดให้มีคณะกรรมการบริหารความเสี่ยง เพื่อรับมอบหมายอำนาจหน้าที่ในการช่วยกำกับดูแลประสิทธิภาพของระบบบริหารความเสี่ยงของบริษัท และรายงานผลให้คณะกรรมการทราบ *(โปรดดูแนวปฏิบัติ 2)*

7. โครงสร้างคณะกรรมการบริหารความเสี่ยงในแต่ละกิจการขึ้นอยู่กับขนาด ความซับซ้อน และกฎหมายที่เกี่ยวข้อง โดยอาจเป็นคณะเดียวกันกับคณะกรรมการชุดย่อยอื่นๆ เช่น คณะกรรมการตรวจสอบ หรืออาจจัดตั้งคณะกรรมการบริหารความเสี่ยงแยกต่างหาก *(โปรดดูแนวปฏิบัติ 2)*

8. คณะกรรมการควรมอบหมายบทบาท หน้าที่ และความรับผิดชอบให้คณะกรรมการบริหารความเสี่ยงผ่านการจัดทำกฎบัตรอย่างเป็นลายลักษณ์อักษร โดยควรมีหน้าที่หลักในการสนับสนุนการปฏิบัติหน้าที่ของคณะกรรมการให้มั่นใจว่า ระบบการบริหารความเสี่ยงและระบบควบคุมภายในขององค์กรเป็นไปอย่างมีประสิทธิภาพ เพียงพอ และเหมาะสม *(โปรดดูแนวปฏิบัติ 2.2)*

9 คณะกรรมการควรกำหนดให้มีการประชุมคณะกรรมการบริหารความเสี่ยงอย่างน้อยปีละ 2 ครั้ง และควรรายงานผลการประชุมต่อคณะกรรมการอย่างสม่ำเสมอ เพื่อให้คณะกรรมการรับทราบถึงผลการดำเนินงาน ประเด็นสำคัญด้านการบริหารความเสี่ยง รวมถึงคำแนะนำสำหรับการตัดสินใจที่จำเป็น *(โปรดดูแนวปฏิบัติ 2)*

10 คณะกรรมการบริหารความเสี่ยงควรได้รับการประเมินผลการปฏิบัติหน้าที่อย่างน้อยปีละ 1 ครั้ง และควรจัดทำรายงานผลการปฏิบัติหน้าที่ให้คณะกรรมการทราบเป็นประจำทุกปี *(โปรดดูแนวปฏิบัติ 2)*

ส่วนที่ 2

แนวปฏิบัติ
(Guidelines)

แนวปฏิบัติ 1 บทบาท หน้าที่ และความรับผิดชอบของคณะกรรมการด้านการบริหารความเสี่ยง

1.1 หลักการสำคัญของการกำกับดูแลตามกรอบแนวคิด GRC

1.1.1 คณะกรรมการมีความรับผิดชอบในการกำกับดูแลให้องค์กรมีความยั่งยืน ตลอดจนบรรลุความคาดหวังของผู้มีส่วนได้ส่วนเสีย ดังนั้น คณะกรรมการจึงต้องกำกับดูแลให้องค์กรมีการบริหารงานแบบบูรณาการกันทั้งในด้านการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎเกณฑ์ หรือที่เรียกว่า GRC (Governance, Risk, and Compliance)

1.1.2 GRC เป็นกระบวนการต่อเนื่อง ที่เริ่มจากการเข้าใจความต้องการของผู้มีส่วนได้ส่วนเสีย แล้วจึงวางแผนกลยุทธ์ / ทิศทางการดำเนินธุรกิจให้สอดรับกับความต้องการเหล่านั้น ตลอดจนวิเคราะห์ความเสี่ยงหรือเหตุการณ์ในอนาคตที่อาจทำให้องค์กรไม่สามารถบรรลุตามกลยุทธ์ที่กำหนดไว้ เพื่อแสวงหาวิธีควบคุมหรือบริหารจัดการ (หรือโอกาสที่จะทำได้ดีกว่า) พร้อมตรวจสอบติดตามประสิทธิภาพของกระบวนการดังกล่าวอย่างสม่ำเสมอ

1.1.3 การทำให้ "การบริหารความเสี่ยง" ถูกบูรณาการอยู่ในกรอบ GRC ได้นั้น คณะกรรมการพึงสื่อสารกับฝ่ายจัดการ โดยเฉพาะกรรมการผู้จัดการใหญ่ (CEO) ให้ชัดเจน ว่าควรรายงานเรื่องใดให้คณะกรรมการทราบบ้าง โดยเรื่องสำคัญๆ ที่ควรรายงานนั้น ประกอบด้วย

1.1.3.1 ความเสี่ยงสำคัญขององค์กร
1.1.3.2 วิธีการบริหารจัดการความเสี่ยงเหล่านั้น

1.1.4 เมื่อคณะกรรมการได้รับรายงานแล้ว ควรพิจารณาความเสี่ยงและวิธีการบริหารจัดการเปรียบเทียบกับ "ระดับความเสี่ยงที่ยอมรับได้" (Risk Appetite) พร้อมแนะนำฝ่ายจัดการว่าควรดำเนินการใดๆ เพิ่มเติมหรือไม่ ในทางตรงกันข้าม หากเห็นว่าวิธีการบริหารจัดการทำให้ความเสี่ยงลดลงไปได้มาก จนสามารถรับความเสี่ยงได้เพิ่ม คณะกรรมการอาจพิจารณาปรับกลยุทธ์องค์กร / ระดับความเสี่ยงที่ยอมรับได้ให้สูงขึ้นตามสมควร โดยในการปฏิบัติตามที่กล่าวมาทั้งหมดนี้ คณะกรรมการต้องดูแลให้มั่นใจว่า สามารถทำให้องค์กรปฏิบัติตามกฎหมาย ระเบียบ และนโยบายต่างๆ ได้อย่างถูกต้อง ครบถ้วน

หมายเหตุ สามารถศึกษารายละเอียดเพิ่มเติมได้ใน "แนวปฏิบัติที่ดีสำหรับคณะกรรมการเกี่ยวกับการบูรณาการ GRC" โดยสถาบันกรรมการบริษัทไทย (IOD)

1.2 การพิจารณากรอบการบริหารความเสี่ยง

1.2.1 คณะกรรมการมีหน้าที่กำกับดูแลการบริหารความเสี่ยงที่ฝ่ายจัดการได้ดำเนินการ โดยมุ่งเน้นว่าการบริหารความเสี่ยงต้องช่วยผลักดัน-ส่งเสริมให้กลยุทธ์องค์กรประสบความสำเร็จตามที่ผู้มีส่วนได้ส่วนเสียคาดหวัง และช่วยให้องค์กรมีความเสี่ยงไม่สูงเกินกว่าระดับที่ยอมรับได้

1.2.2 คณะกรรมการควรกำหนดกรอบ / นิยามเกี่ยวกับความเสี่ยงให้ชัดเจน ตลอดจนกำกับดูแลให้กิจการมีระบบการบริหารความเสี่ยงและควบคุมภายในอย่างเหมาะสม โดยอาจอ้างอิงจากกรอบปฏิบัติสากลที่เรียกว่า COSO Enterprise Risk Management – Integrating with Strategy and Performance (2017) *(โปรดดูภาคผนวก 1)*

1.2.3 คณะกรรมการควรมีความรู้ ประสบการณ์ทางธุรกิจ และเข้าใจความเสี่ยงที่เกี่ยวข้องเป็นอย่างดี ตลอดจนมีความเป็นอิสระในการตั้งคำถามที่ท้าทาย (Challenge) ต่อฝ่ายจัดการ พร้อมให้การสนับสนุน (Concur) ในประเด็นต่างๆ ดังต่อไปนี้

- 1.2.3.1 ความเหมาะสมของกลยุทธ์และความเสี่ยงที่ยอมรับได้ (Risk Appetite)
- 1.2.3.2 ความสอดคล้องระหว่างกลยุทธ์และเป้าหมาย / วัตถุประสงค์ระยะยาวของกิจการ (วิสัยทัศน์ พันธกิจ ค่านิยม ฯลฯ)
- 1.2.3.3 การพิจารณาความเสี่ยงเมื่อมีการตัดสินใจที่สำคัญๆ เช่น การควบรวมกิจการ การจัดสรรเงินทุน และการใช้เงินปันผล ฯลฯ
- 1.2.3.4 ความสามารถในการตอบสนองอย่างรวดเร็วต่อการผันผวนที่สำคัญในการดำเนินงานหรือความเสี่ยง (Portfolio View of Risk) ของบริษัท

1.2.4 คณะกรรมการควรติดตาม ให้ความเห็น และแนะนำแนวทางการจัดการความเสี่ยงและการควบคุมภายในที่ฝ่ายจัดการจัดให้มีขึ้น เพื่อลดโอกาสเกิดหรือผลกระทบของความเสี่ยง ทั้งนี้ ประเภทความเสี่ยงสำคัญๆ ที่คณะกรรมการควรพิจารณา ประกอบด้วย

- 1.2.4.1 ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)
- 1.2.4.2 ความเสี่ยงด้านการดำเนินงาน (Operational Risk)
- 1.2.4.3 ความเสี่ยงด้านการเงิน (Financial Risk)
- 1.2.4.4 ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk)
- 1.2.4.5 ความเสี่ยงด้านเทคโนโลยี (Technology Risk)
- 1.2.4.6 ความเสี่ยงด้านการทุจริต (Fraud Risk)
- 1.2.4.7 ความเสี่ยงด้านบุคลากร (Human Resource Risk)
- 1.2.4.8 ความเสี่ยงจากภัยพิบัติ (Hazard Risk)
- 1.2.4.9 ความเสี่ยงจากกระบวนการภายในบริษัท (Process Risk)
- 1.2.4.10 ความเสี่ยงอื่นๆ (ถ้ามี)

1.3 การกำหนดระดับความเสี่ยงที่ยอมรับได้

1.3.1 คณะกรรมการควรกำหนด "ระดับความเสี่ยงที่ยอมรับได้" (Risk Appetite) พร้อมกับการวางแผนกลยุทธ์ โดยพิจารณาควบคู่ไปกับสภาพแวดล้อมทางธุรกิจ วัฒนธรรมองค์กร ความสอดคล้องกับพันธกิจ วิสัยทัศน์ ตลอดจนความคาดหวังของผู้มีส่วนได้ส่วนเสีย

1.3.2 "ระดับความเสี่ยงที่ยอมรับได้" หมายถึง ประเภทความเสี่ยงและมูลค่าความเสี่ยงที่องค์กรยอมรับและกำหนดขึ้น เพื่อให้สามารถนำไปใช้ครอบคลุมความเสี่ยงของทั้งบริษัท การกำหนด Risk Appetite ที่ดีจะช่วยให้บริษัทยอมรับความเสี่ยงที่เหมาะสมต่อการบรรลุแผนกลยุทธ์ในระยะยาว รวมถึงการเพิ่มและรักษาคุณค่าของบริษัทต่อไป

1.3.3 "ระดับความเสี่ยงที่ยอมรับได้" สามารถเปลี่ยนแปลงได้ เช่น ในภาวะวิกฤตเศรษฐกิจ บริษัทอาจต้องระมัดระวัง จึงยอมรับความเสี่ยงได้เพียงเล็กน้อย แต่เมื่อเศรษฐกิจดีขึ้น บริษัทก็สามารถปรับ "ระดับความเสี่ยงที่ยอมรับได้" ให้มากขึ้น โดยอาจอยู่ในรูปของข้อความหรือคำบรรยายก็ได้ ตัวอย่างเช่น

1.3.3.1 บริษัทไม่ยอมรับถ้ามีโอกาสมากกว่า 10% ที่ผลประกอบการของบริษัทจะขาดทุนมากกว่า 10 ล้านบาท

1.3.3.2 บริษัทจะใช้นวัตกรรมใหม่เพื่อปรับปรุงการให้บริการลูกค้า ยกเว้นนวัตกรรมใหม่นั้นทำให้มีความเสี่ยงต่อการฝ่าฝืนกฎหมายและอาจทำให้ธุรกิจหยุดชะงักได้

1.3.4 ในการกำหนดระดับความเสี่ยงที่ยอมรับได้ คณะกรรมการควรให้แนวทางที่ชัดเจนแก่ฝ่ายจัดการ ดังต่อไปนี้

1.3.4.1 วิธีการที่องค์กรจะใช้กำหนด "ระดับความเสี่ยงที่ยอมรับได้"

1.3.4.2 การพิจารณา "ระดับความเสี่ยงที่ยอมรับได้" ไม่ใช่ดูแต่เรื่องที่จะทำให้องค์กรเสียหาย แต่ควรดูเรื่องที่จะช่วยเพิ่มคุณค่าให้องค์กรด้วย

1.3.5 คณะกรรมการและผู้บริหารพึงหารือกันเพื่อกำหนด "ระดับความเสี่ยงที่ยอมรับได้" ให้เชื่อมโยงกับวิสัยทัศน์ ค่านิยม และกลยุทธ์องค์กร โดยมีคำถามที่คณะกรรมการอาจหยิบยกนำมาเป็นประเด็นในการหารือ เช่น

1.3.5.1 มีกิจกรรมใดบ้างที่มีความเสี่ยงเกิน "ระดับความเสี่ยงที่ยอมรับได้" และกระทบกับกลยุทธ์องค์กร

1.3.5.2 มีกิจกรรมใดบ้างที่องค์กรยังรับความเสี่ยงน้อยเกินกว่าที่จะทำให้บรรลุวัตถุประสงค์ได้

1.3.5.3 มีส่วนใดของธุรกิจที่มีระดับความเสี่ยงที่ยอมรับได้มากกว่าหรือน้อยกว่าส่วนอื่นๆ

1.3.5.4 กลยุทธ์หรือวัตถุประสงค์ข้อใดบ้างที่สำคัญต่อความสำเร็จขององค์กร และมี "ระดับความเสี่ยงที่ยอมรับได้" ที่เหมาะสมหรือไม่

1.3.5.5 ระดับความเสี่ยงสำคัญขององค์กรปัจจุบันอยู่ในระดับใด (รุนแรง ปานกลาง หรือน้อย)

1.3.5.6 มีความเสี่ยงใดบ้างที่ควรกำหนด "ระดับความเสี่ยงที่ยอมรับได้"

1.4 การกำหนดโครงสร้างการบริหารความเสี่ยง

1.4.1 การกำหนดโครงสร้างการบริหารความเสี่ยงควรสอดคล้องกับกลยุทธ์และวัตถุประสงค์ขององค์กร โดยต้องมอบหมายอำนาจหน้าที่และการรายงานให้ชัดเจน ทั้งระดับคณะกรรมการ ฝ่ายจัดการ และระดับต่างๆ พร้อมจัดสรรให้มีบุคลากร ทรัพยากร และงบประมาณอย่างเพียงพอสำหรับการปฏิบัติงาน *(โปรดดูภาคผนวก 2)*

1.4.2 โครงสร้างการบริหารความเสี่ยงมีหลายรูปแบบ เช่น

1.4.2.1 โครงสร้างการบริหารความเสี่ยงแบบกระจาย จะทำให้เห็นความเสี่ยงหลายประเด็น แต่ไม่เน้นเรื่องใดเรื่องหนึ่ง

1.4.2.2 โครงสร้างการบริหารความเสี่ยงแบบรวมศูนย์ จะทำให้เห็นความเสี่ยงน้อยประเด็น แต่มุ่งเน้นความเสี่ยงสำคัญๆ ขององค์กร

1.5 การสร้างวัฒนธรรมในการบริหารความเสี่ยง

1.5.1 คณะกรรมการควรสนับสนุนการสร้างวัฒนธรรมในการบริหารความเสี่ยง โดยการให้แนวทางที่ชัดเจน (Tone from the Top) และทำให้ฝ่ายจัดการตระหนักและรับผิดชอบต่อการบริหารความเสี่ยงในส่วนงานของตน ซึ่งอาจทำได้โดยการเชื่อมโยงการบริหารความเสี่ยงกับเป้าหมายการปฏิบัติงาน รวมถึงการให้รางวัล / แรงจูงใจในการทำงาน โดยพิจารณาจากประสิทธิภาพในการจัดการความเสี่ยง

1.5.2 ในการประเมินวัฒนธรรมด้านการบริหารความเสี่ยง คณะกรรมการอาจใช้คำถามดังต่อไปนี้

1.5.2.1 คณะกรรมการและผู้บริหารระดับสูงได้ให้แนวทางและสื่อสารความสำคัญของการบริหารความเสี่ยงหรือไม่

1.5.2.2 ฝ่ายจัดการเข้าใจหน้าที่และความรับผิดชอบต่อการบริหารความเสี่ยงหรือไม่

1.5.2.3 การอบรมและการประเมินผลงานของบุคลากรได้รับการพิจารณาร่วมกับผลสัมฤทธิ์ด้านการบริหารความเสี่ยงหรือไม่

1.5.2.4 บุคลากรทุกระดับในองค์กรสามารถแสดงความเห็นในเชิงรุกและหารือกันอย่างเต็มที่ในเรื่องที่เกี่ยวกับความเสี่ยงหรือไม่

1.6 การสื่อสารค่านิยมหลักด้านการบริหารความเสี่ยงขององค์กร

1.6.1 คณะกรรมการควรติดตามการสื่อสารเรื่องการบริหารความเสี่ยงไปยังผู้เกี่ยวข้องทั้งภายในและภายนอกบริษัทให้มีประสิทธิภาพและถูกต้อง โดยเฉพาะเมื่อมีประเด็นที่ผู้มีส่วนได้ส่วนเสียมีความกังวลต่อความยั่งยืนของบริษัท

1.6.2 คณะกรรมการควรรับทราบรายงานผลการบริหารความเสี่ยงอย่างสม่ำเสมอ โดยข้อมูลที่ได้รับควรประกอบด้วยประเด็นสำคัญต่างๆ เช่น ความเสี่ยงที่สำคัญและวิธีที่ฝ่ายจัดการใช้เพื่อจัดการความเสี่ยงนั้นๆ ความเสี่ยงอุบัติใหม่ ผลการบริหารความเสี่ยงที่มีต่อกลยุทธ์และเป้าหมายการดำเนินงานเป็นต้น

1.7 การพัฒนาบุคลากร

1.7.1 คณะกรรมการพึงสนับสนุนให้มีการจัดกิจกรรมพัฒนาบุคลากรให้มีความรู้ความเข้าใจในด้านการประเมินความเสี่ยงและการกำหนดวิธีจัดการความเสี่ยง เพื่อที่จะได้นำองค์ความรู้ดังกล่าวไปประยุกต์ใช้ในการปฏิบัติงานที่ได้รับมอบหมายอย่างเต็มความสามารถ อันเป็นไปเพื่อให้บรรลุกลยุทธ์และวัตถุประสงค์ขององค์กร

1.7.2 คณะกรรมการควรให้แนวทางในการประเมินผลการทำงานและกำหนดแรงจูงใจทั้งที่เป็นตัวเงิน และมิใช่ตัวเงิน เช่น การเลื่อนตำแหน่ง การประกาศเกียรติคุณแก่บุคลากรที่ช่วยองค์กรบริหารความเสี่ยงจนสามารถบรรลุกลยุทธ์และวัตถุประสงค์ที่กำหนดไว้

แนวปฏิบัติ 2 | การแต่งตั้งคณะกรรมการบริหารความเสี่ยง

คณะกรรมการอาจพิจารณาให้มีการแต่งตั้ง “คณะกรรมการบริหารความเสี่ยง” (Risk Management Committee) เพื่อช่วยให้คณะกรรมการปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพมากขึ้น โดยการมอบหมายให้ดูแลงานบริหารความเสี่ยงที่ครอบคลุมตั้งแต่การกำหนดนโยบาย การติดตามให้มีการนำไปปฏิบัติ และการรายงาน

การมีคณะกรรมการบริหารความเสี่ยงช่วยแบ่งเบาภาระหน้าที่ของคณะกรรมการได้เป็นอย่างมาก เพราะคณะกรรมการบริหารความเสี่ยงจะสามารถใช้เวลาได้อย่างเต็มที่ในการปฏิบัติหน้าที่กำกับดูแลการบริหารความเสี่ยงขององค์กร อย่างไรก็ตาม คณะกรรมการยังต้องรับผิดชอบต่อหน้าที่นี้อยู่เช่นเดิม ไม่สามารถถ่ายโอนความรับผิดชอบเรื่องนี้ไปยังคณะกรรมการบริหารความเสี่ยงได้

2.1 การพิจารณาความจำเป็นในการแต่งตั้งคณะกรรมการบริหารความเสี่ยง

2.1.1 คณะกรรมการควรเป็นผู้พิจารณาว่าจำเป็นต้องแต่งตั้งคณะกรรมการบริหารความเสี่ยงหรือไม่ หรือคณะกรรมการจะปฏิบัติหน้าที่นี้เอง โดยข้อควรพิจารณาว่าควรแต่งตั้งคณะกรรมการบริหารความเสี่ยงหรือไม่ มีดังต่อไปนี้

2.1.1.1 คณะกรรมการหรือคณะกรรมการชุดย่อยอื่นๆ มีเวลามุ่งเน้นการกำกับดูแลการบริหารความเสี่ยงอย่างเพียงพอหรือไม่

2.1.1.2 คณะกรรมการต้องการให้มีคณะกรรมการชุดย่อยหนึ่ง ที่เป็นศูนย์รวมในการกำกับและติดตามความเสี่ยงทุกด้านหรือทุกหน่วยงานในบริษัท เพื่อให้เกิดความโปร่งใสในการดูแลการบริหารความเสี่ยงหรือไม่

2.1.1.3 คณะกรรมการต้องการสื่อสารให้ผู้ถือหุ้นและผู้มีส่วนได้ส่วนเสียเห็นว่าบริษัทให้ความสำคัญต่อการบริหารความเสี่ยงเป็นพิเศษหรือไม่

2.1.1.4 คณะกรรมการต้องการให้กรรมการที่ไม่อิสระ เช่น กรรมการที่เป็นผู้บริหาร (Executive Director) เป็นผู้กำกับดูแลการบริหารความเสี่ยงด้วยหรือไม่ (ในกรณีนี้ ทำให้คณะกรรมการตรวจสอบ (Audit Committee) ไม่สามารถปฏิบัติหน้าที่เป็นกรรมการบริหารความเสี่ยงได้)

2.1.1.5 คณะกรรมการมีความกังวลว่าบริษัทยังไม่มีความสามารถอย่างเพียงพอในการระบุ ประเมินและจัดการความเสี่ยงหรือไม่

2.1.2 หากมีการแต่งตั้งคณะกรรมการบริหารความเสี่ยงขึ้น คณะกรรมการจะต้องจัดสรรเวลาให้มีการประชุมร่วมกับคณะกรรมการบริหารความเสี่ยงอย่างเพียงพอ เพื่อให้ได้ทราบผลและปัญหาที่เกิดขึ้นกับการบริหารความเสี่ยง

2.1.3 หากมีการแต่งตั้งคณะกรรมการบริหารความเสี่ยง ควรมีการจัดทำกฎบัตรคณะกรรมการบริหารความเสี่ยงให้คณะกรรมการอนุมัติด้วย *(โปรดดูภาคผนวก 3)* และจัดให้มีการสอบทานกฎบัตรนี้ทุกปี เพื่อให้มั่นใจว่าจะสามารถนำไปปฏิบัติตามได้อย่างเหมาะสม

2.2 องค์ประกอบและคุณสมบัติของคณะกรรมการบริหารความเสี่ยง

2.2.1 องค์ประกอบของคณะกรรมการบริหารความเสี่ยงในแต่ละบริษัทขึ้นอยู่กับขนาด ความซับซ้อนของธุรกิจ และกฎหมายที่เกี่ยวข้อง

2.2.1.1 ในกิจการขนาดเล็กที่ลักษณะการประกอบธุรกิจและโครงสร้างไม่ซับซ้อน มักให้คณะกรรมการทำหน้าที่เป็นคณะกรรมการบริหารความเสี่ยงไปในตัว

2.2.1.2 ในกิจการขนาดกลาง คณะกรรมการบริหารความเสี่ยงมักเป็นคณะกรรมการ หรือเป็นคณะเดียวกันกับคณะกรรมการชุดย่อยอื่นๆ เช่น คณะกรรมการตรวจสอบ

2.2.1.3 ในกิจการขนาดใหญ่ หรือกิจการซึ่งประกอบธุรกิจที่มีการเปลี่ยนแปลงตลอดเวลา อาจพิจารณาให้มี "คณะกรรมการบริหารความเสี่ยง" แยกต่างหาก

2.2.2 สมาชิกในคณะกรรมการบริหารความเสี่ยงอาจเป็น "กรรมการทั้งหมด" หรือเป็นการ "ผสมผสานทั้งกรรมการและผู้บริหาร" หรือเป็น "ผู้บริหารทั้งหมด" แล้วรายงานผลไปยังคณะกรรมการก็ได้

2.2.3 ในกรณีที่คณะกรรมการบริหารความเสี่ยงเป็นผู้บริหารทั้งหมด สมาชิกมักประกอบด้วย กรรมการผู้จัดการใหญ่ (CEO) รองกรรมการผู้จัดการฝ่ายการเงิน (CFO) ฝ่ายปฏิบัติการ (COO) ฝ่ายบริหารความเสี่ยง (CRO) หรือผู้บริหารระดับ C-Suite ฝ่ายอื่นๆ

2.2.4 คณะกรรมการบริหารความเสี่ยงต้องเป็นผู้ที่มีความรู้เกี่ยวกับลักษณะการประกอบธุรกิจของบริษัทพลวัติภายในอุตสาหกรรม ทั้งยังควรมีวิสัยทัศน์กว้าง สามารถวิเคราะห์-คาดการณ์เหตุการณ์ในอนาคตได้อย่างรอบด้านและสมเหตุสมผล เป็นผู้นำ และกล้าตัดสินใจ ตลอดจนมีความรู้เกี่ยวกับวิธีการจัดการความเสี่ยงนั้นๆ

2.3 บทบาท หน้าที่ และความรับผิดชอบของคณะกรรมการบริหารความเสี่ยง

2.3.1 คณะกรรมการบริหารความเสี่ยงมีหน้าที่สนับสนุนและแบ่งเบาภาระของคณะกรรมการในการปฏิบัติหน้าที่เพื่อธำรงไว้ซึ่งประสิทธิภาพของกลไกการบริหารความเสี่ยงขององค์กร ตั้งแต่การกำหนดนโยบาย การติดตามให้มีการนำไปปฏิบัติ และการรายงาน *(ดังกล่าวแล้วในแนวปฏิบัติที่ 1)* อาทิเช่น

2.3.1.1 พิจารณากลั่นกรองร่างนโยบายและกรอบการบริหารความเสี่ยงองค์กร ก่อนนำเสนอต่อคณะกรรมการเพื่อพิจารณาอนุมัติ

2.3.1.2 พิจารณาผลการประเมินความเสี่ยงและแผนบริหารจัดการความเสี่ยงเหล่านั้น พร้อมให้ข้อเสนอแนะหรือแนวทางลดผลกระทบของความเสี่ยงต่างๆ ให้อยู่ในระดับที่ยอมรับได้ เพื่อให้มั่นใจว่ากิจการมีระบบการบริหารจัดการความเสี่ยงที่เพียงพอและเหมาะสม

2.3.1.3 ให้ข้อชี้แนะ / คำแนะนำแก่คณะกรรมการบริษัท ตลอดจนฝ่ายจัดการ ในด้านการบริหารความเสี่ยง รวมถึงส่งเสริมให้กิจการมีการพัฒนากรอบ / ระบบการบริหารความเสี่ยงภายในกิจการอย่างต่อเนื่อง

2.3.1.4 ดูแลให้มีการสอบทานกรอบ / นโยบายการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อให้มั่นใจว่ากรอบ / นโยบายดังกล่าว ยังคงสอดรับกับบริบทและสภาพแวดล้อมการดำเนินธุรกิจของกิจการ

2.3.1.5 รายงานความเสี่ยงสำคัญ สถานะของความเสี่ยง ตลอดจนความคืบหน้าหรือผลการบริหารจัดการความเสี่ยงเหล่านั้นให้คณะกรรมการทราบเป็นประจำ

2.4 วาระการดำรงตำแหน่ง

2.4.1 ในกรณีที่สมาชิกในคณะกรรมการบริหารความเสี่ยงเป็น “กรรมการทั้งหมด” หรือเป็นการ “ผสมผสานทั้งกรรมการและผู้บริหาร” คณะกรรมการควรกำหนดวาระการดำรงตำแหน่งของกรรมการบริหารความเสี่ยงไว้อย่างชัดเจน โดยพิจารณาให้สอดคล้องกับวาระการเป็นกรรมการบริษัท

2.4.2 ในกรณีที่กรรมการลาออก หรือสิ้นสุด หรือมีสาเหตุอื่นใดให้ต้องพ้นจากตำแหน่งในคณะกรรมการบริหารความเสี่ยง จนทำให้สมาชิกในคณะมีกรรมการคงเหลือไม่ถึง “จำนวนขั้นต่ำ” ที่กำหนด คณะกรรมการควรพิจารณาเลือกบุคคลใดบุคคลหนึ่งซึ่งมีคุณสมบัติเข้าเป็นกรรมการบริหารความเสี่ยงแทน

2.5 การประชุมคณะกรรมการบริหารความเสี่ยง

2.5.1 กิจการควรกำหนดให้มีการประชุมคณะกรรมการบริหารความเสี่ยงอย่างน้อยปีละ 2 ครั้ง (บางกิจการอาจกำหนดให้มีการประชุมไตรมาสละ 1 ครั้ง) ทั้งนี้ ประธานคณะกรรมการบริหารความเสี่ยงอาจเรียกประชุมเพิ่มเติมได้ตามที่เห็นสมควร โดยช่วงเวลาในการประชุมนั้นสามารถพิจารณาได้ตามความเหมาะสม อย่างไรก็ตาม คณะกรรมการบริหารความเสี่ยงควรกำหนดวันประชุมฯ เป็นการล่วงหน้าไว้ในปฏิทินประจำปี (Annual Board Calendar)

2.5.2 คณะกรรมการบริหารความเสี่ยงควรกำหนดวาระการประชุม (ในเบื้องต้น) ร่วมกับเลขานุการของคณะกรรมการบริหารความเสี่ยง ก่อนที่จะนำเสนอให้คณะกรรมการพิจารณาเห็นชอบ

2.5.3 หนังสือเชิญประชุมฯ ควรกำหนดวัน เวลา สถานที่ หัวข้อที่จะประชุม พร้อมข้อมูลเอกสารประกอบการประชุมไว้อย่างชัดเจน และควรจัดส่งถึงกรรมการบริหารความเสี่ยง ตลอดจนบุคคลที่เกี่ยวข้องอย่างน้อย 7 วันก่อนการประชุม ทั้งนี้ หากมีประเด็นเพิ่มเติม สามารถจัดประชุมเพิ่มได้ตามที่เห็นสมควร

2.5.4 สมาชิกในคณะกรรมการบริหารความเสี่ยงแต่ละท่าน ควรเข้าร่วมประชุมอย่างน้อยร้อยละ 75 ของจำนวนครั้งการประชุมของคณะกรรมการบริหารความเสี่ยงทั้งหมดที่ได้จัดขึ้นในรอบปี โดย "องค์ประชุมขั้นต่ำ" (Quorum) ควรประกอบด้วยกรรมการบริหารความเสี่ยงเข้าร่วมประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการที่มีอยู่ในขณะนั้น

2.5.5 "มติในที่ประชุม" ให้ถือเสียงข้างมากขององค์ประชุมที่ออกเสียงคะแนน โดยให้กรรมการบริหารความเสี่ยง 1 คนมี 1 เสียงในการลงคะแนน ในกรณีที่คะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมฯ ออกเสียงเพิ่มขึ้นอีก 1 เสียงเพื่อเป็นเสียงชี้ขาด

2.5.6 หากประธานกรรมการบริหารความเสี่ยงไม่สามารถเข้าร่วมประชุมได้ สมาชิกในคณะกรรมการบริหารความเสี่ยงสามารถแต่งตั้ง "รองประธานบริหารความเสี่ยง" (ถ้ามี) หรือกรรมการบริหารความเสี่ยงท่านหนึ่งเพื่อทำหน้าที่เป็น "ประธานชั่วคราว" ในที่ประชุมได้

2.5.7 คณะกรรมการบริหารความเสี่ยงมีอำนาจเชิญฝ่ายจัดการ ตลอดจนบุคคลที่เกี่ยวข้องหรือที่เห็นสมควรเข้าร่วมประชุมในบางวาระเพื่อขอข้อมูลตามความจำเป็น

2.5.8 "เลขานุการคณะกรรมการบริหารความเสี่ยง" ต้องเข้าร่วมประชุมด้วยทุกครั้ง เพื่อทำหน้าที่บันทึกการประชุม และจัดทำรายงานการประชุม ในกรณีมีเหตุจำเป็นที่เลขานุการคณะกรรมการบริหารความเสี่ยงไม่สามารถเข้าร่วมประชุมได้ คณะกรรมการบริหารความเสี่ยงอาจมอบหมายให้บุคคลอื่นๆ ทำหน้าที่ดังกล่าวแทน ตามที่เห็นสมควร

2.6 การรายงานต่อคณะกรรมการ

2.6.1 คณะกรรมการบริหารความเสี่ยงควรรายงานผลการประชุมต่อคณะกรรมการอย่างสม่ำเสมอ เพื่อให้คณะกรรมการรับทราบถึงผลการดำเนินงาน ประเด็นสำคัญที่เกี่ยวกับความเสี่ยงขององค์กร รวมถึงคำแนะนำต่างๆ ที่เป็นประโยชน์ต่อการตัดสินใจ

2.6.2 คณะกรรมการบริหารความเสี่ยงควรจัดทำ “รายงานผลการปฏิบัติหน้าที่ในรอบปีของคณะกรรมการบริหารความเสี่ยง” ให้คณะกรรมการรับทราบเป็นประจำทุกปี ซึ่งรายงานฉบับดังกล่าวควรลงนามโดยประธานคณะกรรมการบริหารความเสี่ยง และควรเปิดเผยไว้ในรายงานประจำปี ควบคู่ไปกับการเปิดเผยรายละเอียดในด้านอื่นๆ เช่น

2.6.2.1 การทบทวนกรอบและแนวทางการบริหารความเสี่ยง

2.6.2.2 รายการความเสี่ยงสำคัญที่องค์กรเผชิญอยู่

2.6.2.3 ปัจจัยที่อาจส่งผลกระทบต่อสถานะความเสี่ยงขององค์กรในอนาคต

2.6.3 คณะกรรมการบริหารความเสี่ยงควรได้รับการประเมินผลการปฏิบัติหน้าที่เป็นประจำทุกปี เพื่อใช้เป็นโอกาสในการพิจารณาทบทวนแนวทางการดำเนินงานที่ผ่านมา ตลอดจนระบุปัญหาหรืออุปสรรคที่เป็นเหตุให้การปฏิบัติงานไม่บรรลุตามวัตถุประสงค์ แล้วจึงรายงานผลการประเมินดังกล่าวให้คณะกรรมการทราบ เพื่อแสวงหาแนวทางปรับปรุงและพัฒนาการปฏิบัติหน้าที่ให้มีประสิทธิภาพยิ่งขึ้นต่อไป *(ตัวอย่างประเด็นที่ใช้ในการประเมินตนเองของคณะกรรมการบริหารความเสี่ยง โปรดดูภาคผนวก 4)*

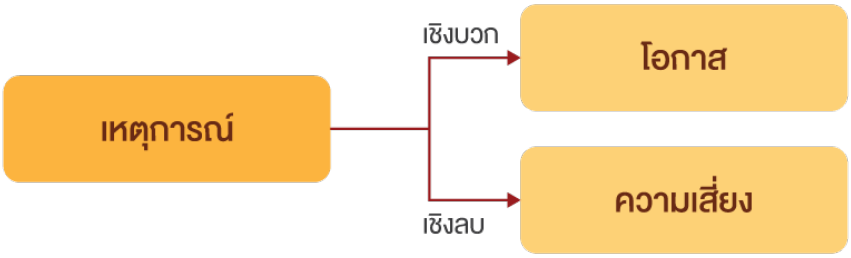
2.6.4 การประเมินผลคณะกรรมการบริหารความเสี่ยงสามารถทำได้โดยใช้วิธีการเดียวกันกับการประเมินผลคณะกรรมการ หรืออาจจัดให้มีผู้เชี่ยวชาญจากภายนอกทำการประเมินและให้คำแนะนำก็ได้ โดยการประเมินผลควรทำอย่างน้อยปีละ 1 ครั้ง หรือตามความถี่ในการประเมินผลการปฏิบัติงานของคณะกรรมการ

ภาคผนวก

ภาคผนวก 1 กรอบการบริหารความเสี่ยงองค์กรตามหลัก COSO ERM Framework

แนวคิดเบื้องต้น

- ความเสี่ยง (Risk) คือ เหตุการณ์ที่อาจจะเกิดขึ้นในอนาคตและมีผลกระทบต่อการบรรลุกลยุทธ์และวัตถุประสงค์ของธุรกิจ โดยเหตุการณ์นั้นอาจมีผลเชิงบวกหรือเชิงลบต่อองค์กรก็ได้



กรอบการบริหารความเสี่ยงองค์กรตามแนวคิดของ COSO มีองค์ประกอบ 5 ประการ ได้แก่

1. Governance and Culture หมายถึง การที่คณะกรรมการมีความเข้าใจในความเสี่ยงของบริษัท ตลอดจนกำกับดูแลการบริหารความเสี่ยง พร้อมสร้างวัฒนธรรมที่ช่วยขับเคลื่อนให้การบริหารความเสี่ยงนั้นประสบความสำเร็จ

2. Strategy and Objective Setting หมายถึง การประสานกันของการบริหารความเสี่ยง กลยุทธ์ และการกำหนดวัตถุประสงค์ในกระบวนการวางแผนกลยุทธ์ โดยมีการกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ให้สัมพันธ์กับกลยุทธ์ ส่วนวัตถุประสงค์ช่วยให้มีการนำกลยุทธ์ไปปฏิบัติ และเป็นพื้นฐานของการระบุ ประเมิน และจัดการความเสี่ยง

3. Performance หมายถึง การระบุ ประเมิน และหาวิธีจัดการความเสี่ยง

4. Review and Revision หมายถึง การพิจารณาผลการดำเนินงานเพื่อดูว่าจะต้องปรับปรุงระบบบริหารความเสี่ยงหรือไม่ อย่างไร

5. Information, Communication and Reporting หมายถึง การสื่อสารเพื่อรับและให้ข้อมูลด้านการบริหารความเสี่ยงอย่างต่อเนื่อง ทั้งข้อมูลภายในและภายนอก และระหว่างหน่วยงานภายในบริษัท

- กรอบการบริหารความเสี่ยงที่ดีจะต้องเป็นส่วนหนึ่งของการปฏิบัติงาน (Performance) เพื่อช่วยให้บรรลุกลยุทธ์ (Strategy) ตามความคาดหวังของผู้มีส่วนได้ส่วนเสีย และช่วยให้บริษัทเติบโตอย่างยั่งยืน เพราะหลังจากเข้าใจความเสี่ยงและสามารถจัดการได้แล้ว บริษัทอาจเห็นโอกาสใหม่ๆ ที่ควรทำต่อไป

การบูรณาการการบริหารความเสี่ยงกับกลยุทธ์และการดำเนินงานของบริษัท

- การบริหารความเสี่ยงไม่ใช่กระบวนการหรือการปฏิบัติที่แยกจากกระบวนการอื่นๆ ในทางตรงกันข้าม คณะกรรมการควรกำกับและติดตามดูว่า ผู้บริหารได้พัฒนาและนำการบริหารความเสี่ยงไปใช้ร่วมกับการปฏิบัติงานอื่นๆ ตามปกติของธุรกิจหรือไม่ โดยการบูรณาการที่สำคัญของการบริหารความเสี่ยง ควรมีดังต่อไปนี้

1. **การบูรณาการกับกระบวนการวางแผนกลยุทธ์**
   การวางแผนกลยุทธ์ คือการที่บริษัทต้องตัดสินใจต่อทางเลือกที่ดีที่สุดที่จะเกิดขึ้นในอนาคต เพื่อให้บริษัทเติบโตต่อไปอย่างยั่งยืน การตัดสินใจนี้จึงมีทั้งความเสี่ยงและโอกาส ดังนั้น เพื่อให้การตัดสินใจผิดพลาดน้อยที่สุด บริษัทจึงควรนำการบริหารความเสี่ยงมาประกอบกับการวางแผนกลยุทธ์ เพื่อให้สามารถเลือกกลยุทธ์ที่เหมาะสมและอยู่ในระดับความเสี่ยงที่บริษัทยอมรับได้

   COSO Enterprise Risk Management – Integrating with Strategy and performance ได้ให้แนวทางว่าบริษัทควรพิจารณาความเสี่ยงในขั้นตอนนี้ โดยจำแนกออกเป็น 3 มุมมอง ได้แก่

   1.1 ความเสี่ยงที่แผนกลยุทธ์อาจไม่สอดคล้องกับพันธกิจ วิสัยทัศน์ และค่านิยมของบริษัท
   ความเสี่ยงนี้อาจมีสาเหตุจากพันธกิจ วิสัยทัศน์ และค่านิยมไม่ชัดเจนเพียงพอ ทำให้กำหนดกลยุทธ์ที่ไม่สอดคล้องกัน หรือในทางตรงข้าม พันธกิจ วิสัยทัศน์ และค่านิยมมีความชัดเจน แต่กลยุทธ์ไม่ดีพอที่จะทำให้บรรลุตามนั้นได้

   1.2 ความเสี่ยงจากการเลือกแผนกลยุทธ์ผิด
   ในการกำหนดกลยุทธ์นั้น บริษัทมักมีทางเลือกหลายประการว่าจะเลือกกลยุทธ์ใด โดยแต่ละกลยุทธ์จะมีความเสี่ยงแตกต่างกัน ดังนั้น บริษัทจึงควรประเมินความเสี่ยงของแต่ละทางเลือกว่าสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) หรือไม่

1.3 ความเสี่ยงในการนำกลยุทธ์ไปปฏิบัติไม่สำเร็จ
ความเสี่ยงประเภทนี้มักเกิดจากเหตุการณ์ที่เกิดขึ้นระหว่างการดำเนินกลยุทธ์ ทั้งจากภายในและภายนอกบริษัท เช่น ความเสี่ยงด้านการเงิน การดำเนินงาน การปฏิบัติตามกฎระเบียบ การตลาด เทคโนโลยี บุคลากร ฯลฯ ดังนั้น บริษัทจึงควรทำให้ทุกคนเข้าใจ ปฏิบัติ และร่วมกันสร้างวัฒนธรรมการบริหารความเสี่ยง เพื่อให้การบริหารความเสี่ยงถูกผนวกเข้าไปเป็นส่วนหนึ่งของการปฏิบัติงานตามปกติ และนำไปสู่เป้าหมายที่ต้องการร่วมกัน

2. **การบูรณาการกับกระบวนการวัดผลการดำเนินงาน**
บริษัทควรมีกระบวนการเชื่อมโยงการวัดผลการดำเนินงานกับการบริหารความเสี่ยง โดยนำเกณฑ์ชี้วัดผลการดำเนินงานมาเป็นเป้าหมาย และให้ผู้บริหารประเมินว่ามีเหตุการณ์ใดบ้างที่อาจเกิดขึ้นและมีผลเชิงลบต่อการบรรลุเป้าหมาย จากนั้นให้ผู้บริหารกำหนดวิธีการจัดการความเสี่ยงเพื่อให้บรรลุเป้าหมายนั้น เมื่อบริษัทสามารถบรรลุเป้าหมายในปัจจุบันได้แล้ว ก็จะสามารถเพิ่มระดับเป้าหมายได้ในครั้งต่อๆ ไป ทำให้เพิ่ม (Create) และรักษา (Preserve) คุณค่าของบริษัท และทำให้สร้างโอกาสใหม่ให้แก่บริษัทด้วย

3. **การบูรณาการกับการควบคุมภายใน**
การจัดการความเสี่ยงไม่ใช่แค่เพียงการกำหนดว่าจะทำสิ่งใด แต่รวมถึงการออกแบบและปฏิบัติตามกระบวนการที่มีอยู่ในหน่วยงานและแผนกต่างๆ ด้วย เช่น กระบวนการจัดซื้อ บริหารสินค้า รับและจ่ายเงิน จัดทำรายงานทางการเงิน ฯลฯ กระบวนการที่ดีนั้นจะต้องมีการควบคุมภายในที่เพียงพอและเหมาะสมเพื่อให้สามารถจัดการความเสี่ยงและบรรลุตามวัตถุประสงค์ของงานนั้นๆ ได้

ตัวอย่างเช่น บริษัทมีความเสี่ยงต่อการลดลงของรายได้ เนื่องจากมีคู่แข่งเพิ่มขึ้นในตลาด แผนจัดการความเสี่ยงคือการหาลูกค้าใหม่โดยเร็วที่สุด ฝ่ายขายจึงต้องกำหนดคุณสมบัติของลูกค้าใหม่ที่เป็นเป้าหมาย อย่างไรก็ตาม ฝ่ายขายต้องเสนอคุณสมบัติของลูกค้าใหม่นี้ให้ที่ประชุมผู้บริหารอนุมัติ เพื่อควบคุมให้มั่นใจว่าคุณสมบัติเหล่านี้สอดคล้องกับกลยุทธ์และทำให้บริษัทแข่งขันในตลาดได้

4. **การบูรณาการกับการจัดการความยั่งยืน** (Sustainability)
ความยั่งยืนเป็นเป้าหมายของทุกบริษัท อย่างไรก็ตาม มีเหตุการณ์หลายอย่างที่หากเกิดขึ้นแล้วอาจทำลายความยั่งยืนของบริษัทได้ เหตุการณ์เหล่านี้เรียกว่าความเสี่ยง บริษัทต้องประเมินดูว่าเหตุการณ์ใดจะเกิดขึ้นบ้าง และหาวิธีจัดการกับเหตุการณ์ที่เป็นความเสี่ยงเหล่านั้น

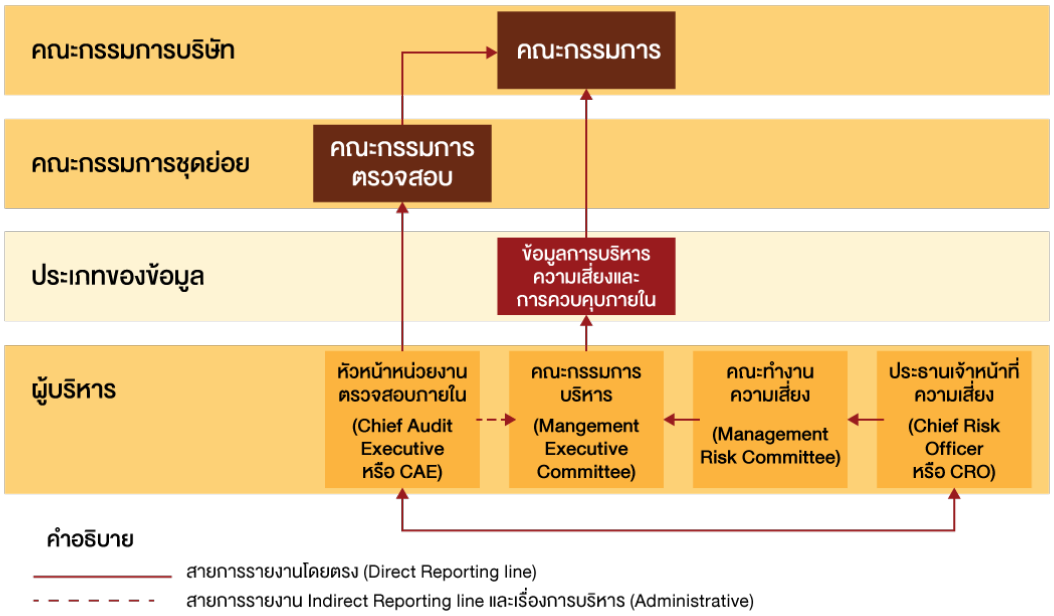
ตัวอย่างความเสี่ยงด้านความยั่งยืน เช่น ความเสี่ยงจากการกำกับดูแลกิจการไม่เพียงพอ การไม่เป็นที่ยอมรับของชุมชน วิกฤตเศรษฐกิจ ภาวะโลกร้อน ฯลฯ

5. **การบูรณาการกับการจัดการสิ่งแวดล้อม สังคม และการกำกับดูแลกิจการ** (Environmental, Social and Governance **หรือ** ESG)
คณะกรรมการบริหารความเสี่ยงควรกำกับดูแลให้บริษัทนำระบบบริหารความเสี่ยงไปใช้เพื่อประเมิน จัดการ และรายงานความเสี่ยงด้าน ESG ด้วย โดยควรกำหนดโครงสร้างให้มีการทำงานร่วมกันระหว่างหน่วยงานบริหารความเสี่ยง และหน่วยงานที่รับผิดชอบการบริหารความยั่งยืนขององค์กร จัดให้มีแนวทางการประเมินและจัดลำดับความสำคัญของความเสี่ยงด้าน ESG ตลอดจนสื่อสารผลการบริหารความเสี่ยงด้าน ESG ให้แก่ผู้เกี่ยวข้อง ทั้งภายในและภายนอกบริษัท เช่น ผู้ลงทุน คู่ค้า ลูกค้า องค์กรภาคประชาสังคม และสังคม

ภาคผนวก 2 รูปแบบต่างๆ ของโครงสร้างการกำกับดูแลความเสี่ยงองค์กร

โครงสร้างแบบที่ 1

"คณะกรรมการ" มีหน้าที่กำกับดูแลการบริหารความเสี่ยงและการควบคุมภายใน

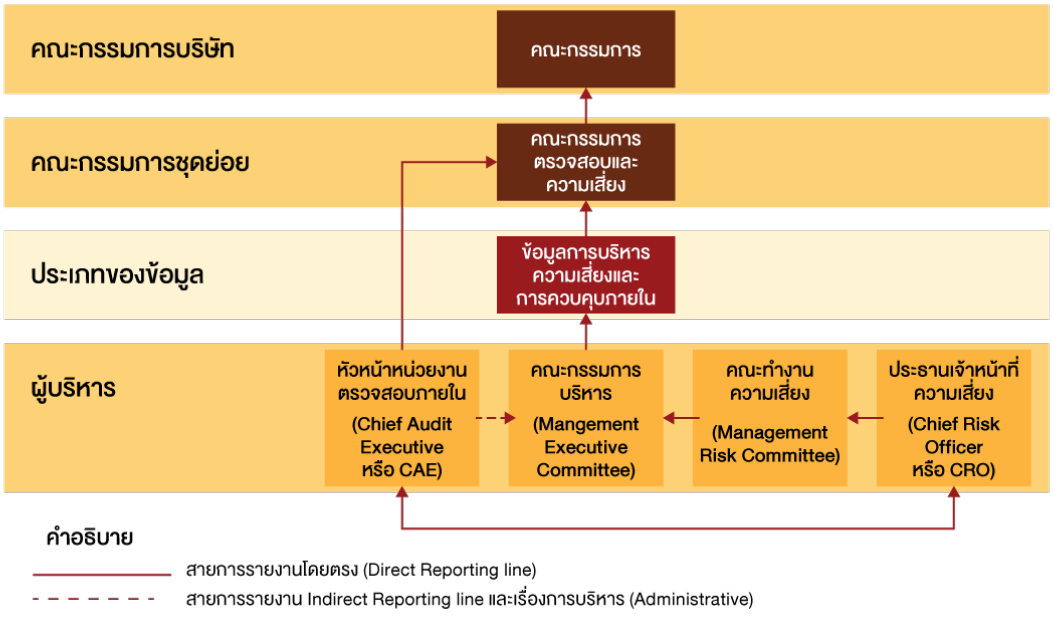


Source : IOD Singapore

หมายเหตุ: กรรมการผู้จัดการใหญ่ (CEO) เป็นสมาชิกของคณะกรรมการบริหาร (Executive Committee)

โครงสร้างแบบที่ 2

"คณะกรรมการตรวจสอบและความเสี่ยง" กำกับดูแลการบริหารความเสี่ยงและการควบคุมภายใน

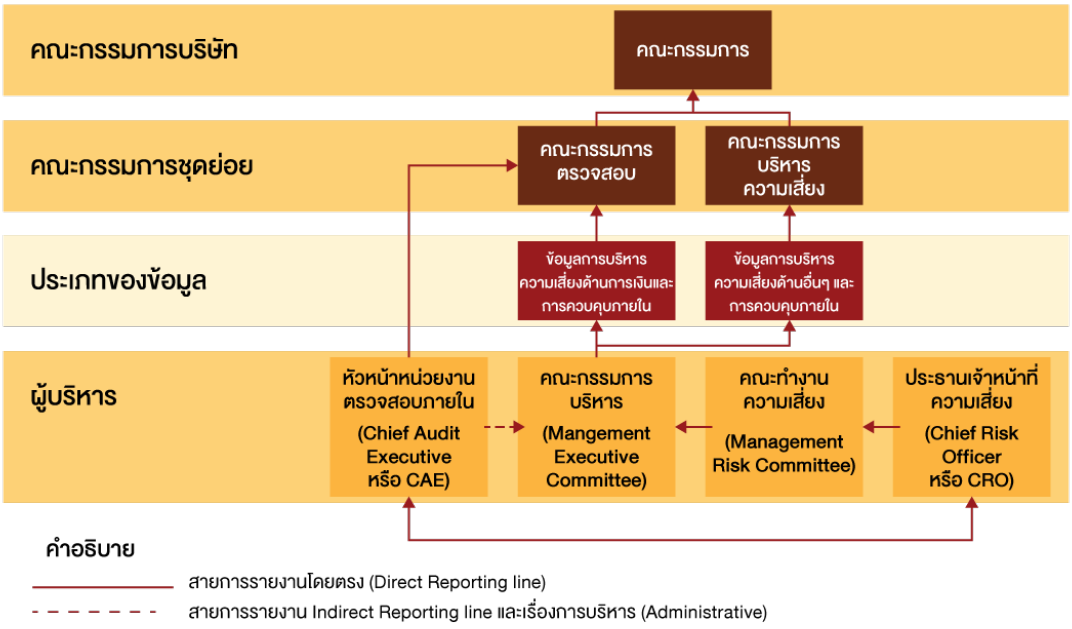


Source : IOD Singapore

หมายเหตุ: กรรมการผู้จัดการใหญ่ (CEO) เป็นสมาชิกของคณะกรรมการบริหาร (Executive Committee)

โครงสร้างแบบที่ 3

"คณะกรรมการบริหารความเสี่ยง" กำกับดูแลการบริหารความเสี่ยงและการควบคุมภายใน

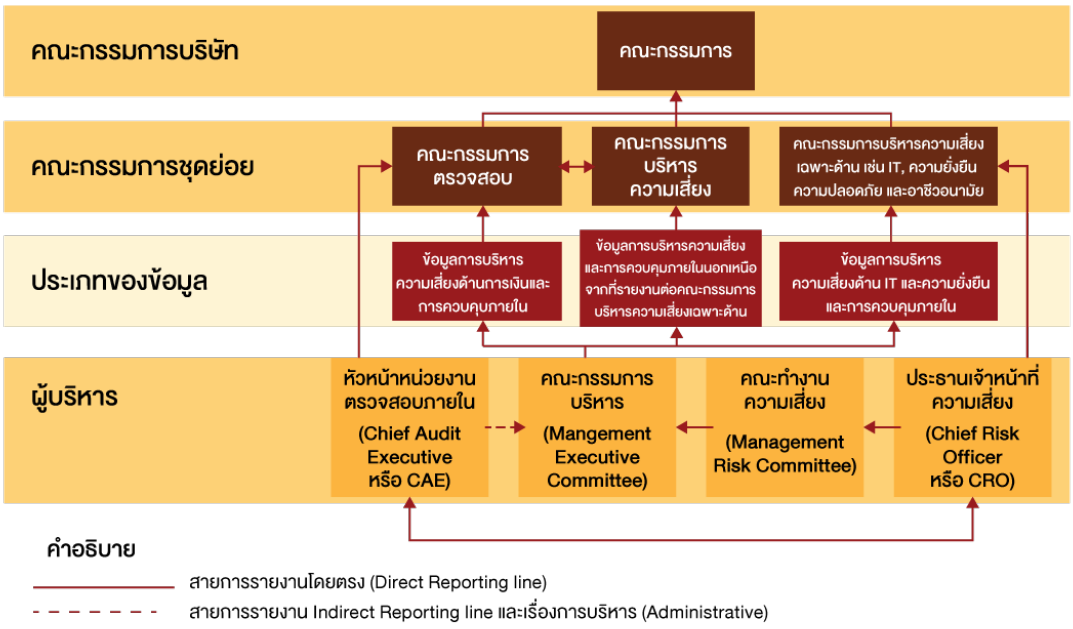


Source : IOD Singapore

หมายเหตุ: กรรมการผู้จัดการใหญ่ (CEO) เป็นสมาชิกของคณะกรรมการบริหาร (Executive Committee)

โครงสร้างแบบที่ 4

"คณะกรรมการบริหารความเสี่ยง" ปฏิบัติงานร่วมกับคณะกรรมการชุดย่อยอื่นๆ



Source : IOD Singapore

หมายเหตุ: กรรมการผู้จัดการใหญ่ (CEO) เป็นสมาชิกของคณะกรรมการบริหาร (Executive Committee)

ภาคผนวก 3 ตัวอย่าง กฎบัตรคณะกรรมการบริหารความเสี่ยง

1. วัตถุประสงค์

คณะกรรมการเป็นผู้พิจารณาแต่งตั้งคณะกรรมการบริหารความเสี่ยง ซึ่งประกอบด้วยกรรมการและ/หรือผู้บริหารจำนวนหนึ่งที่มีคุณสมบัติเหมาะสม เพื่อกำหนดนโยบายด้านการบริหารความเสี่ยงให้ครอบคลุมทั่วทั้งองค์กร รวมทั้งกำกับดูแลให้มีระบบการบริหารจัดการความเสี่ยงเพื่อควบคุมความเสี่ยงและลดผลกระทบของความเสี่ยง กำหนดมาตรการป้องกันและติดตามดูแลการปฏิบัติตามมาตรการดังกล่าวได้อย่างเหมาะสม กฎบัตรฉบับนี้ทำขึ้นเพื่อให้คณะกรรมการบริหารความเสี่ยงมีความเข้าใจบทบาท หน้าที่ และความรับผิดชอบของตนเอง และใช้กฎบัตรนี้เป็นแนวทางในการปฏิบัติหน้าที่

2. องค์ประกอบ

2.1 คณะกรรมการบริหารความเสี่ยงประกอบด้วยกรรมการและ/หรือผู้บริหารจำนวนไม่น้อยกว่า ..... คน

2.2 คณะกรรมการหรือคณะกรรมการบริหารความเสี่ยง จะเลือกกรรมการบริหารความเสี่ยงคนหนึ่งเป็นประธานกรรมการบริหารความเสี่ยง

3. คุณสมบัติ

3.1 กรรมการบริหารความเสี่ยงต้องเป็นบุคคลที่มีความรู้ ความสามารถ และประสบการณ์ที่จะเป็นประโยชน์ต่อการดำเนินธุรกิจของบริษัทเป็นอย่างดี มีความซื่อสัตย์ สุจริต มีจริยธรรมในการดำเนินธุรกิจ และมีเวลาเพียงพอที่จะอุทิศความรู้ ความสามารถ และปฏิบัติหน้าที่ให้แก่บริษัทอย่างเต็มที่ โดยเฉพาะอย่างยิ่งต้องมีความรู้เกี่ยวกับความเสี่ยงที่อาจเกิดขึ้น และส่งผลกระทบต่อการประกอบธุรกิจของบริษัท

3.2 กรรมการบริหารความเสี่ยงต้องมีคุณสมบัติและไม่มีลักษณะต้องห้ามตามกฎหมายว่าด้วยบริษัทมหาชนจำกัด กฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์ และกฎหมายอื่นใดที่เกี่ยวข้องกับการประกอบธุรกิจของบริษัทฯ

4. หน้าที่และความรับผิดชอบ

4.1 พิจารณาและระบุความเสี่ยงที่สำคัญของการประกอบธุรกิจของบริษัท เช่น ความเสี่ยงด้านกลยุทธ์ ด้านการเงิน ด้านการปฏิบัติการ ด้านกฎระเบียบ ด้านการตลาด ตลอดจนความเสี่ยงที่มีผลกระทบต่อชื่อเสียงของกิจการ รวมถึงเสนอแนะวิธีป้องกัน และวิธีบริหารความเสี่ยงดังกล่าวให้อยู่ในระดับที่ยอมรับได้ โดยกำหนดเป็นนโยบายและเสนอแนะแนวทางในการบริหารความเสี่ยงต่างๆ ที่เกี่ยวกับการดำเนินธุรกิจของบริษัทให้เหมาะสมและมีประสิทธิภาพ รวมถึงให้คำแนะนำแก่คณะกรรมการและฝ่ายจัดการในเรื่องการบริหารความเสี่ยง

4.2 กำหนดแผนจัดการความเสี่ยงและกระบวนการบริหารความเสี่ยงสำหรับบริษัท

4.3 กำกับดูแลและสนับสนุนให้การบริหารความเสี่ยงประสบความสำเร็จ โดยมีหน้าที่ติดตามและประเมินผลการปฏิบัติตามกรอบการบริหารความเสี่ยงทั่วทั้งบริษัท อีกทั้งทบทวนความเพียงพอของนโยบาย ระบบบริหารความเสี่ยง และปรับปรุงแผนการดำเนินงานเพื่อลดความเสี่ยงอย่างต่อเนื่อง ให้เหมาะสมกับสภาวะการดำเนินธุรกิจของบริษัท

4.4 สื่อสารกับคณะกรรมการตรวจสอบเกี่ยวกับความเสี่ยงที่สำคัญ เพื่อพิจารณาถึงความเพียงพอของระบบการควบคุมภายในของบริษัท

4.5 รายงานผลการประเมินความเสี่ยงและผลการดำเนินงานเพื่อลดความเสี่ยง เพื่อให้คณะกรรมการทราบเป็นประจำ ในกรณีที่มีเรื่องสำคัญซึ่งส่งผลกระทบอย่างมีนัยสำคัญต่อฐานะการเงินและผลการดำเนินงานของบริษัท จะต้องรายงานต่อคณะกรรมการโดยเร็วที่สุด

4.6 ปฏิบัติหน้าที่อื่นใดตามที่คณะกรรมการมอบหมาย

5. วาระการดำรงตำแหน่งและการเลือกตั้งกรรมการบริหารความเสี่ยง

5.1 กรรมการบริหารความเสี่ยงจะพ้นจากตำแหน่งเมื่อ

1. ตาย
2. ลาออก
3. ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามกฎหมายว่าบริษัทมหาชนจำกัด และ/หรือกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์
4. ที่ประชุมคณะกรรมการมีมติให้ออก
5. ศาลมีคำสั่งให้ออก
6. พ้นสภาพจากการเป็นกรรมการหรือผู้บริหารของบริษัทฯ

5.2 กรรมการบริหารความเสี่ยงคนใดจะลาออกจากตำแหน่งให้ยื่นใบลาออกเป็นลายลักษณ์อักษรต่อบริษัท การลาออกให้มีผลตั้งแต่วันที่ใบลาออกไปถึงบริษัท

5.3 ในกรณีที่ตำแหน่งกรรมการบริหารความเสี่ยงว่างลง และทำให้องค์คณะมีจำนวนน้อยกว่าจำนวนขั้นต่ำที่กำหนด ให้คณะกรรมการพิจารณาเลือกบุคคลใดบุคคลหนึ่งซึ่งมีคุณสมบัติเข้าเป็นกรรมการบริหารความเสี่ยงแทน ส่วนในกรณีอื่นๆ คณะกรรมการอาจพิจารณาเลือกบุคคลใดบุคคลหนึ่งซึ่งมีคุณสมบัติเข้าเป็นกรรมการบริหารความเสี่ยงแทนตามความเหมาะสม

5.4 ในกรณีที่กรรมการบริหารความเสี่ยงพ้นจากตำแหน่งทั้งคณะ ให้คณะกรรมการบริหารความเสี่ยงที่พ้นจากตำแหน่งต้องอยู่รักษาการในตำแหน่งเพื่อดำเนินงานต่อไปก่อน จนกว่าคณะกรรมการบริหารความเสี่ยงชุดใหม่จะเข้ารับหน้าที่

6. การประชุม

6.1 การประชุมคณะกรรมการบริหารความเสี่ยง ต้องมีกรรมการบริหารความเสี่ยงมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการบริหารความเสี่ยงทั้งหมดจึงเป็นองค์ประชุม ในกรณีที่ประธานกรรมการบริหารความเสี่ยงไม่อยู่ในที่ประชุม หรือไม่สามารถปฏิบัติหน้าที่ได้ ถ้ามีรองประธานกรรมการบริหารความเสี่ยง ให้รองประธานกรรมการบริหารความเสี่ยงเป็นประธานที่ประชุม ถ้าไม่มีรองประธานกรรมการบริหารความเสี่ยง หรือมี แต่ไม่สามารถปฏิบัติหน้าที่ได้ ให้กรรมการบริหารความเสี่ยงซึ่งมาประชุมเลือกกรรมการบริหารความเสี่ยงคนหนึ่งเป็นประธานฯ

6.2 การวินิจฉัยชี้ขาดของที่ประชุมคณะกรรมการบริหารความเสี่ยง ให้ถือเสียงข้างมาก โดยกรรมการบริหารความเสี่ยงคนหนึ่งมีหนึ่งเสียงในการลงคะแนน เว้นแต่กรรมการบริหารความเสี่ยงซึ่งมีส่วนได้ส่วนเสียในเรื่องใดไม่มีสิทธิออกเสียงลงคะแนนในเรื่องนั้น ถ้าคะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกหนึ่งเสียงเป็นเสียงชี้ขาด

6.3 การประชุมคณะกรรมการบริหารความเสี่ยงจะจัดให้มีหรือเรียกประชุมได้ตามที่เห็นสมควร แต่การประชุมตามปกติต้องจัดขึ้นอย่างน้อยไตรมาสละ 1 ครั้ง เว้นแต่มีเหตุจำเป็นไม่สามารถประชุมได้ โดยให้ประธานกรรมการบริหารความเสี่ยงเป็นผู้เรียกประชุมคณะกรรมการบริหารความเสี่ยง หรือในกรณีจำเป็น กรรมการบริหารความเสี่ยงตั้งแต่ 2 คนขึ้นไป อาจร้องขอให้ประธานกรรมการเรียกประชุมกรรมการบริหารความเสี่ยงได้ ในกรณีดังกล่าว ให้ประธานกรรมการบริหารความเสี่ยงกำหนดวันประชุมภายใน 14 วัน นับแต่วันที่ได้รับการร้องขอ

6.4 ให้ประธานกรรมการบริหารความเสี่ยง หรือกรรมการบริหารความเสี่ยงที่ได้รับมอบหมายจากประธานกรรมการบริหารความเสี่ยงเป็นผู้กำหนดวัน เวลา และสถานที่ในการประชุมคณะกรรมการบริหารความเสี่ยง ซึ่งสถานที่ที่ประชุมนั้นอาจกำหนดเป็นอย่างอื่นนอกเหนือไปจากท้องที่อันเป็นที่ตั้งสำนักงานใหญ่ของบริษัทฯ ก็ได้ หากประธานกรรมการบริหารความเสี่ยง หรือกรรมการบริหารความเสี่ยงที่ได้รับมอบหมายจากประธานกรรมการบริหารความเสี่ยง มิได้กำหนดสถานที่ประชุม ให้ใช้สำนักงานใหญ่ของบริษัทฯ เป็นสถานที่ประชุม

6.5 ในการเรียกประชุมคณะกรรมการบริหารความเสี่ยง ให้ประธานกรรมการบริหารความเสี่ยง หรือผู้ซึ่งได้รับมอบหมายส่งหนังสือนัดประชุมและเอกสารอื่นใดที่จำเป็นต่อการประชุมและการลงมติของกรรมการบริหารความเสี่ยงโดยทางไปรษณีย์ลงทะเบียน หรือส่งมอบให้แก่กรรมการบริหารความเสี่ยงโดยตรง โดยระบุวัน เวลา สถานที่ และกิจการที่จะประชุมไปยังกรรมการบริหารความเสี่ยง ไม่น้อยกว่า 7 วันก่อนวันประชุม เว้นแต่กรณีเร่งด่วนเพื่อรักษาประโยชน์ของบริษัท จะแจ้งนัดประชุมโดยวิธีอื่น หรือกำหนดวันประชุมให้เร็วกว่านั้นก็ได้

7. อำนาจการดำเนินการ

7.1 คณะกรรมการบริหารความเสี่ยงมีอำนาจแต่งตั้งเลขานุการคณะกรรมการบริหารความเสี่ยงเพื่อช่วยเหลือการดำเนินงานของคณะกรรมการบริหารความเสี่ยง

7.2 คณะกรรมการบริหารความเสี่ยงมีอำนาจที่จะขอความเห็นที่เป็นอิสระจากที่ปรึกษาวิชาชีพอื่นใดเมื่อเห็นว่าจำเป็นด้วยค่าใช้จ่ายของบริษัท ซึ่งการดำเนินการว่าจ้างให้เป็นไปตามระเบียบปฏิบัติของบริษัท

7.3 คณะกรรมการบริหารความเสี่ยงมีอำนาจเรียกขอข้อมูลจากหน่วยงานต่างๆ ของบริษัทและบริษัทย่อย เพื่อประกอบการพิจารณาเพิ่มเติมในเรื่องต่าง ๆ ได้

8. การรายงาน

คณะกรรมการบริหารความเสี่ยงเป็นคณะกรรมการชุดย่อยที่แต่งตั้งโดยคณะกรรมการ เพื่อให้ช่วยศึกษาและกลั่นกรองงาน ดังนั้น คณะกรรมการบริหารความเสี่ยงจึงมีความรับผิดชอบในการรายงานผลการปฏิบัติหน้าที่ต่อคณะกรรมการอย่างสม่ำเสมอ

9. ค่าตอบแทน

ให้คณะกรรมการบริหารความเสี่ยงได้รับค่าตอบแทนตามจำนวนที่คณะกรรมการได้อนุมัติ โดยพิจารณาความเห็นและคำแนะนำของคณะกรรมการสรรหา กำหนดค่าตอบแทน และบรรษัทภิบาล ประกอบการพิจารณาอนุมัติ

ที่ประชุมคณะกรรมการ ครั้งที่ XX/25XX เมื่อวันที่ XXX ได้มีมติอนุมัติกฎบัตรคณะกรรมการบริหารความเสี่ยง ให้มีผลบังคับใช้ตั้งแต่วันที่ XXX

ประกาศ ณ วันที่ ..... เดือน ..... พ.ศ. .....
ลงนาม .....
ประธานกรรมการบริษัท

ภาคผนวก 4 ตัวอย่างประเด็นสำหรับใช้ในการประเมินตนเองของคณะกรรมการบริหารความเสี่ยง

ประเด็น
Governance and Culture
1. ความรู้และความเข้าใจเกี่ยวกับระบบบริหารความเสี่ยง 2. การอบรมอย่างต่อเนื่องเพื่อให้ทันยุคสมัยกับการเปลี่ยนแปลงของการบริหารความเสี่ยง 3. ความสัมพันธ์และการทำงานร่วมกับผู้บริหารเพื่อให้เข้าใจแนวคิด ทัศนคติ และวิธีจัดการความเสี่ยงในบริษัท 4. ความสามารถในการสื่อสารเพื่อให้ทุกคนเข้าใจและยอมรับความสำคัญของการบริหารความเสี่ยง อันนำไปสู่การปฏิบัติอย่างต่อเนื่อง จนกลายเป็นวัฒนธรรมองค์กร
Strategy and Objective Setting
5. การทำให้มีการประเมินความเสี่ยงพร้อมกับกระบวนการวางแผนกลยุทธ์ 6. การกำหนดความเสี่ยงที่ยอมรับได้ (Risk Appetite) ที่เหมาะสมกับบริษัท และสื่อสารให้ทุกคนที่เกี่ยวข้องทราบ
Performance
7. การกำกับดูแลกระบวนการบริหารความเสี่ยงให้เป็นส่วนหนึ่งของการดำเนินงานตามปกติ และช่วยให้บรรลุเป้าหมายที่บริษัทต้องการ
Review and Revision
8. การติดตามผลและปรับปรุงวิธีการบริหารความเสี่ยงที่มีอยู่ และประเมินความเสี่ยงใหม่อย่างสม่ำเสมอ
Information, Communication and Reporting
9. การรายงานความเสี่ยงให้แก่คณะกรรมการอย่างครบถ้วน ตรงประเด็น สม่ำเสมอ และทันเวลา 10. การนำเทคโนโลยีมาใช้เพื่อให้การบริหารความเสี่ยงมีข้อมูลครบถ้วน เข้าถึงได้ และสื่อสารได้อย่างรวดเร็ว

เอกสารอ้างอิง

1. COSO 3 Lines of Defence
2. COSO ERM Creating and Protecting Value
3. COSO Guidance on Risk Appetite
4. **Developing a Strong Risk Culture**, PwC December 2010
5. **Enterprise Risk Management – Integrating with Strategy and Performance**, Committee of Sponsoring Organizations of The Treadway Commission, 2017
6. **GRC Capability Model version 3.0**, The Open Compliance and Ethics Group
7. **GRC And The Board: What They Really Need To Know**, Forbes, March 2020
8. **G20/OECD Principles of Corporate Governance**, Organization for Economic Co-operation and Development (OECD), 2015
9. **How your Board can influence culture and risk appetite**, PwC, February 2017
10. **How your Board can decide if it needs risk committee**, PwC, March 2017
11. **How your Board can ensure enterprise risk management connects with startegy**, PwC, April 2017
12. **Striking a Balance – Whistleblowing arrangements as part of a speakup strategy**, PwC, January 2011
13. **The Building Blocks of GRC**, The Open Compliance and Ethics Group, April 2016
14. **Guidance on Risk Appetite – a critical to success**, COSO

Thai Institute of Directors Association

Capital Market Academy Building 2, 2/9 Moo 4 Northpark Project,
Vibhavadi - Rangsit Road, Thung SongHong, Laksi, Bangkok
10210, Thailand

Phone : (66) 2955 1155 Fax: (66) 2955 1156 - 57 www.thai-iod.com