



ส่วนที่ 1 หลักการสำคัญ (Key Principles)



1. คณะกรรมการมีบทบาทและความรับผิดชอบในฐานะผู้นำองค์กรสร้างคุณค่าให้แก่กิจการอย่างยั่งยืน โดยการกำกับดูแลให้บริษัทมีกลยุทธ์ที่เสริมสร้างการเจริญก้าวหน้า ดำเนินธุรกิจอย่างมีจริยธรรม โปร่งใส คำนึงถึงผู้มีส่วนได้ส่วนเสียทุกฝ่าย และปฏิบัติตามกฎหมาย
2. คณะกรรมการพึงใช้แนวคิดการบูรณาการ GRC เป็นกรอบในการขับเคลื่อนและส่งเสริมให้องค์กรดำเนินกิจกรรมตามแนวปฏิบัติสำคัญ 4 ประการ ตามหลักการของ The Office of Compliance and Ethics Group (OCEG) ได้แก่
 - 2.1 Lean หมายถึง การเรียนรู้และเข้าใจอย่างถ่องแท้ถึงบริบทในการดำเนินธุรกิจ วัฒนธรรมองค์กร และความคาดหวังของผู้มีส่วนได้ส่วนเสีย
 - 2.2 Align หมายถึง การนำสิ่งที่ได้เรียนรู้มากำหนดวัตถุประสงค์ขององค์กร แล้วจึงระบุความเสี่ยงที่อาจเกิดขึ้น ซึ่งทำให้องค์กรไม่บรรลุวัตถุประสงค์
 - 2.3 Perform หมายถึง การขับเคลื่อนให้องค์กรไปสู่เป้าหมายหรือวัตถุประสงค์ ด้วยกระบวนการทำงานที่มีประสิทธิภาพ ถูกต้องตามกฎหมาย และมีระบบการควบคุมภายในที่ดี
 - 2.4 Monitor หมายถึง มีระบบติดตามดูแลการปฏิบัติงานอย่างเพียงพอ เหมาะสมเพื่อให้เป็นไปตามวัตถุประสงค์ที่ตั้งไว้
3. คณะกรรมการควบคุมกำกับดูแลให้องค์กร และวิธีการปฏิบัติแบบก้าวหน้า ทำให้องค์กรสามารถบรรลุวัตถุประสงค์อย่างมีประสิทธิภาพและมีจริยธรรม ท่ามกลางความไม่แน่นอนต่อการเปลี่ยนแปลงอย่างรวดเร็วและรุนแรงของเศรษฐกิจ ตลาด เทคโนโลยี บุคลากร กฎหมาย สิ่งแวดล้อม สังคม เป็นต้น ความไม่แน่นอนเหล่านี้ทำให้องค์กรต้องพิจารณาทั้งความเสี่ยงและโอกาสที่อาจเกิดขึ้น เพื่อลดความเสี่ยงหรือเพิ่มโอกาสในการบรรลุวิสัยทัศน์และกลยุทธ์ที่กำหนดไว้
4. คณะกรรมการควร กำกับดูแลกิจการ (Governance) และกำหนดทิศทางการดำเนินงานอันเป็นไปเพื่อความยั่งยืน ซึ่งมีพื้นฐานมาจากการพิจารณาปัจจัยแวดล้อมทั้งภายในและภายนอก ตลอดจนผลประโยชน์ของผู้มีส่วนได้ส่วนเสียอย่างรอบด้าน พร้อมสื่อสารกลยุทธ์ นโยบาย และหลักการสำคัญต่าง ๆ แก่ฝ่ายจัดการเพื่อนำไปสู่การปฏิบัติ ซึ่งครอบคลุมทั้ง การบริหารความเสี่ยง ที่มีประสิทธิภาพ ยืดหยุ่น และตอบสนองการเปลี่ยนแปลงได้อย่างรวดเร็ว และการปฏิบัติตามกฎหมายระเบียบต่าง ๆ อย่างครบถ้วนสมบูรณ์
5. ทั้งนี้ บทบาทและความรับผิดชอบของคณะกรรมการมีได้แยกเป็นส่วน ๆ หากแต่คณะกรรมการต้องดูแลให้องค์กรสามารถเชื่อมโยงและประสานงานที่เกี่ยวข้องกับการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎหมาย ให้อยู่เป็น ภาพเดียวกับภายใต้วัฒนธรรมองค์กรที่มีจริยธรรม โปร่งใส และซื่อสัตย์ ซึ่งรวมเรียกว่าการบูรณาการ GRC



ส่วนที่ 2 แนวปฏิบัติ (Guidelines)

แนวปฏิบัติ 1 บทบาทสำคัญของคณะกรรมการในการกำกับดูแลกิจการ



1.1 ความหมายของ Governance Risk and Compliance (GRC)

1.1.1 GRC หมายถึง การบริหารงานในองค์กรให้ทุกหน่วยงาน ระบบงาน กระบวนการ บุคลากร และข้อมูล ประสานกันอย่างเป็นระบบหรือเรียกว่าบูรณาการ เพื่อทำให้องค์กรบรรลุกลยุทธ์วัตถุประสงค์และเป้าหมาย ที่กำหนดไว้โดยคำนึงถึงความคาดหวังอย่างมีเหตุผลของผู้มีส่วนได้ส่วนเสียกลุ่มต่าง ๆ

1.1.2 GRC จึงนับเป็นการบริหารงานที่ครอบคลุมเป็นภาพเดียวกันทั้งหมดของ **(มี 3 ข้อย่อย ตามเอกสารวาระ 3.2)**

1.2 ทำไมคณะกรรมการต้องให้ความสนใจต่อ GRC

1.2.1 คณะกรรมการมีบทบาทสำคัญในฐานะผู้นำที่สร้างคุณค่าให้แก่กิจการอย่างยั่งยืน รวมทั้งมีส่วนร่วมตั้งแต่การกำกับดูแลกลยุทธ์และการจัดการเพื่อทำให้องค์กรสามารถแข่งขันและปรับตัวกับการเปลี่ยนแปลงต่าง ๆ ได้ ดังนั้น คณะกรรมการจึงถือเป็นกลุ่มคนสำคัญที่จะต้องผลักดันให้องค์กรมีระบบการจัดการเป็นแบบ GRC เพื่อที่จะสามารถมั่นใจได้ว่าองค์กรจะสามารถดำเนินงานให้บรรลุผลสำเร็จตามกลยุทธ์ที่กำหนดไว้

1.2.2 ในกรณีที่คณะกรรมการไม่กำกับดูแลให้องค์กรมีการนำหลักการบริหารจัดการแบบ GRC มาใช้ อาจจะเผชิญกับปัญหาต่าง ๆ ได้ **(มี 6 ข้อย่อย ตามเอกสารวาระ 3.2)**

1.2.3 จากการที่ GRC เป็นการบูรณาการในทุกส่วนที่เกี่ยวข้องกับการดำเนินงาน และมีส่วนเกี่ยวข้องกันหลายฝ่ายภายในองค์กร คณะกรรมการจึงมีบทบาทสำคัญที่จะต้องแสดงเจตจำนง ให้คนในองค์กรเห็นพ้องต้องกันถึงความจำเป็นที่ต้องนำหลักการ GRC มาปรับใช้เพื่อเกิดการดำเนินงานที่สอดคล้องประสานกันตามนโยบายที่คณะกรรมการกำหนด

1.2.4 การแสดงเจตจำนงของคณะกรรมการ เพื่อสร้างการรับรู้ให้แก่บุคลากรทุกระดับภายในองค์กรสามารถทำผ่านวิธีต่าง ๆ ได้ **(มี 3 ข้อย่อย ตามเอกสารวาระ 3.2)**

1.3 คุณลักษณะขององค์กรที่บูรณาการ GRC ได้อย่างมีประสิทธิภาพ

องค์กรที่มีการบูรณาการ GRC อย่างมีประสิทธิภาพจะมีความมั่นใจต่อการบรรลุกลยุทธ์ วัตถุประสงค์ และเป้าหมายที่กำหนดไว้ เนื่องจากองค์กรมีวิธีการบริหารงานที่มีประสิทธิภาพจากทั้งกระบวนการ บุคลากร ข้อมูลและเทคโนโลยีสารสนเทศ ภายใต้วัฒนธรรมและจรรยาบรรณที่ดีและโปร่งใส ดังนั้น องค์กรที่มีหลักการบริหารจัดการแบบ GRC มักมีลักษณะต่าง ๆ **(มี 8 ข้อย่อย ตามเอกสารวาระ 3.2)**

1.4 บทบาทโดยรวมของคณะกรรมการที่มี GRC

1.4.1 จากการที่คณะกรรมการจะต้องปฏิบัติหน้าที่ด้วยความรับผิดชอบระมัดระวัง และซื่อสัตย์สุจริตต่อองค์กร คณะกรรมการจึงจะเป็นที่จะต้องกำกับดูแลให้องค์กรมีการบริหารจัดการแบบ GRC กล่าวคือมีการกำหนดและเข้าใจกลยุทธ์ วัตถุประสงค์ และเป้าหมายอย่างชัดเจน เพื่อนำไปสู่การประเมินและวางระบบการบริหารความเสี่ยงทั้งในระดับองค์กร และหน่วยงาน ตลอดจนมีการประเมินและควบคุมให้มีการปฏิบัติงานถูกต้องตามกฎหมายและระเบียบกฎเกณฑ์ต่าง ๆ ที่เกี่ยวข้อง โดยสรุปคือ คณะกรรมการต้องสามารถเข้าใจและติดตามการบริหารงานให้เป็นภาพรวมทั้งหมด แทนการดูแบบแยกส่วน (Silo) นั่นเอง

1.4.2 สิ่งที่คณะกรรมการควรให้ความสำคัญมากที่สุด คือการแนะนำและติดตามให้ผู้รับผิดชอบดำเนินการต่าง ๆ **(มี 5 ข้อย่อย ตามเอกสารวาระ 3.2)**

1.4.3 คณะกรรมการควรพิจารณาและคำนึงถึงการบูรณาการ GRC ในกิจกรรมต่าง ๆ **(มี 3 ข้อย่อย ตามเอกสารวาระ 3.2)**

1.4.4 อย่างไรก็ตาม การที่คณะกรรมการจะสามารถทำหน้าที่กำกับดูแลและติดตามได้ คณะกรรมการเองควรมีความเข้าใจเรื่อง GRC อย่างถ่องแท้ ตลอดจนมีความพร้อมเพื่อที่จะสามารถให้แนวทางที่ถูกต้องแก่ฝ่ายจัดการได้ โดยคณะกรรมการสามารถสร้างความพร้อมหรือเตรียมตัวในเรื่อง GRC ได้ด้วยวิธีการดังต่อไปนี้

1.4.4.1 องค์ประกอบของคณะกรรมการ **(มี 2 ข้อย่อย ตามเอกสารวาระ 3.2)**

1.4.4.2 ภาวะผู้นำของคณะกรรมการ : คณะกรรมการต้องมีความเป็นผู้นำ เพื่อที่จะสามารถร่วมกำหนดหรือทบทวนทิศทางของการดำเนินกลยุทธ์ ตลอดจนแผนงานต่าง ๆ ร่วมกับผู้รับผิดชอบได้ โดยคณะกรรมการจำเป็นต้องเข้าใจเรื่องต่าง ๆ **(มี 6 ข้อย่อย ตามเอกสารวาระ 3.2)**

1.4.4.3 การทำหน้าที่สอดส่องดูแลของคณะกรรมการ : คณะกรรมการไม่เพียงแต่ทำหน้าที่ตัดสินใจร่วมกับผู้รับผิดชอบในทิศทางและแผนการดำเนินงานต่าง ๆ ตามหลัก GRC เท่านั้น แต่ต้องทำหน้าที่กำกับดูแลและติดตามดูแลอย่างต่อเนื่อง ดังนั้น เพื่อให้กรรมการมีความพร้อมและสามารถทำหน้าที่กำกับดูแลได้อย่างเต็มที่ คณะกรรมการควรจัดให้มีการกำหนดเป็นกรอบการดำเนินงานตามหลัก GRC ขึ้นมาอย่างชัดเจนเพื่อใช้ในการดำเนินการและติดตามดูแลการนำไปปฏิบัติของผู้รับผิดชอบและคอยให้คำแนะนำแก่ผู้รับผิดชอบเพื่อให้การดำเนินการตามหลัก GRC นั้นมีประสิทธิภาพมากขึ้น โดยกรอบ GRC ที่คณะกรรมการต้องจัดให้มีขึ้น **(มี 5 ข้อย่อย ตามเอกสารวาระ 3.2)**



ส่วนที่ 2 แนวปฏิบัติ (Guidelines)

แนวปฏิบัติ 2 GRC (Governance Risk and Compliance) Building Blocks



2.1 GRC Building Blocks

GRC Building Blocks ประกอบด้วย 3 องค์ประกอบสำคัญคือ การกำกับดูแลกิจการ การบริหารความเสี่ยง และการกำกับการปฏิบัติตามกฎระเบียบ และข้อบังคับ โดยหลักการทั่วไปที่คณะกรรมการควรพิจารณาเกี่ยวกับการบูรณาการเรื่อง GRC เข้ากับการดำเนินงานขององค์กร มีดังนี้

2.1.1 GRC ที่ดีต้องเชื่อมโยงการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบข้อบังคับต่าง ๆ อย่างมีประสิทธิภาพและประสิทธิผล โดยเริ่มจากการที่ผู้รับผิดชอบนำเสนอทิศทาง แผนกลยุทธ์ แผนการดำเนินงาน หรือรายงานผลความคืบหน้าของแผนการดำเนินงาน พร้อมกับผลการประเมินความเสี่ยงและวิธีการจัดการความเสี่ยงนั้น ๆ ให้กับคณะกรรมการ

2.1.2 เมื่อคณะกรรมการพิจารณาแล้วเห็นว่าข้อมูลจากผู้รับผิดชอบนำเสนอมีความเหมาะสมและอยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite) ประกอบกับแนวทางการกำกับดูแลกิจการในปัจจุบันยังมีความเหมาะสมอยู่ก็จะทำการอนุมัติแผนกลยุทธ์หรือแผนการดำเนินงานนั้นให้ผู้รับผิดชอบนำไปใช้พัฒนาหรือปฏิบัติต่อไป หรือหากเป็นกรณีการรายงานความคืบหน้า คณะกรรมการก็จะรับทราบผลการดำเนินงานและให้ผู้รับผิดชอบดำเนินการตามแผนต่อไปได้

2.1.3 ในส่วนการกำกับการปฏิบัติตามกฎ ระเบียบ และข้อบังคับ คณะกรรมการควรกำกับให้ผู้รับผิดชอบไปพร้อมกับการบริหารความเสี่ยงโดยทั่วไป โดยควรมีการประเมินความเสี่ยงด้านการปฏิบัติตามกฎระเบียบและข้อบังคับ มีการสอบทาน และการรายงานผลการปฏิบัติไปยังคณะกรรมการอย่างสม่ำเสมอเช่นกัน

2.1.4 คณะกรรมการควรกำกับดูแลให้มั่นใจว่า ผู้รับผิดชอบได้จัดให้มีการสอบทานประสิทธิภาพและประสิทธิผลของ GRC Building Blocks อย่างสม่ำเสมอโดยผู้ตรวจสอบภายใน และรายงานผลการสอบทานให้คณะกรรมการทราบ โดยคณะกรรมการควรแนะนำผู้รับผิดชอบให้ปรับปรุง Building Blocks ได้ เมื่อเห็นถึงจุดบกพร่องที่ต้องปรับปรุง หรือเมื่อพิจารณาเห็นว่ากลยุทธ์ สภาพแวดล้อมการดำเนินงานหรือความคาดหวังของผู้มีส่วนได้เสียเปลี่ยนแปลงไป

2.2 การกำกับดูแลกิจการ (Governance)

หากพิจารณาเฉพาะในส่วนของการกำกับดูแลกิจการ คณะกรรมการจะต้องกำกับดูแลว่าทิศทาง แผนกลยุทธ์ แผนการดำเนินงานที่ผู้รับผิดชอบนำเสนอ หรือดำเนินการอยู่นั้น สอดรับกับโครงสร้างการกำกับดูแลภายในองค์กร ตลอดจนนโยบายการดำเนินงานต่าง ๆ ที่สำคัญขององค์กรหรือไม่ โดยคณะกรรมการจะต้องพิจารณาในเรื่องต่าง ๆ ดังนี้

2.2.1 ทิศทาง แผนกลยุทธ์แผนการดำเนินงานที่ผู้รับผิดชอบ สอดรับกับเป้าหมาย พันธกิจและวิสัยทัศน์ขององค์กร หรือไม่ หรือแม้แต่แผนที่ได้รับการอนุมัติไปแล้วและกำลังดำเนินการอยู่นั้น ยังสอดคล้องกับเป้าหมาย ทิศทางในปัจจุบันอยู่หรือไม่

2.2.2 โครงสร้างองค์กร ในปัจจุบันยังสามารถรองรับทิศทาง กลยุทธ์ และแผนการดำเนินงานขององค์กรหรือไม่ จำเป็นต้องมีการปรับเปลี่ยนปรับขนาดโครงสร้างองค์กรหรือไม่

2.2.3 ทิศทาง กลยุทธ์และแผนการดำเนินงานมีความสอดคล้องกับวัฒนธรรมขององค์กร หรือไม่ เช่น วัฒนธรรมที่ไม่กล้าเสี่ยง หรือวัฒนธรรมที่ขอบความเสี่ยง หากเป็นกรณีที่ไม่มีความสอดคล้อง ผู้รับผิดชอบมีแนวทางจัดการอย่างไร เช่น การจัดตั้งหน่วยงานที่จะดำเนินการตามแผนกลยุทธ์ใหม่แยกจากโครงสร้างการทำงานโดยปกติ เพื่อการตัดสินใจและมีแนวทางการทำงานที่รวดเร็วและยืดหยุ่นมากขึ้น

2.2.4 นโยบาย ทั้งองค์กรมีในปัจจุบันเอื้อให้สามารถดำเนินการตามทิศทาง กลยุทธ์และแผนการดำเนินงานหรือไม่ หากนโยบายที่มีอยู่ไปจำกัดการดำเนินงาน ผู้รับผิดชอบมีแนวทางจัดการอย่างไร เช่น ไม่ดำเนินการตามแผนเนื่องจากขัดกับนโยบายขององค์กร หรือจะมีการปรับเปลี่ยนนโยบายเพื่อเอื้อให้เกิดการดำเนินการได้อย่างเหมาะสม

2.2.5 การปฏิบัติงานตามทิศทาง กลยุทธ์ และแผนการดำเนินงานนั้น มีการมอบหมายหน้าที่ในการดำเนินการอย่างเหมาะสมหรือไม่

2.2.6 การดำเนินการตามทิศทางกลยุทธ์และแผนการดำเนินงานดังกล่าวมีการกำหนดตัวชี้วัดใดบ้าง เหมาะสมหรือไม่ทั้งในแง่ของผลสัมฤทธิ์ที่คาดหวัง และในแง่ที่มีผลต่อวัฒนธรรมและพฤติกรรมของคนในองค์กร

ในระหว่างการทำงานตามกลยุทธ์ที่คณะกรรมการอนุมัติแล้ว ผู้รับผิดชอบควรประเมินความเสี่ยงระดับองค์กร ระดับสายงานและกระบวนการ และรายงานความเสี่ยงที่สำคัญพร้อมทั้งวิธีจัดการความเสี่ยงนั้นให้คณะกรรมการทราบอย่างสม่ำเสมอ หรืออย่างน้อยทุกไตรมาส เมื่อคณะกรรมการได้รับทราบแล้วควรพิจารณาความถูกต้องและครบถ้วนของความเสี่ยง ความเหมาะสมของวิธีการจัดการความเสี่ยง และให้ความเห็นหรือข้อเสนอแนะเกี่ยวกับความเสี่ยง วิธีการจัดการความเสี่ยง หรืออาจเป็นข้อเสนอแนะในการปรับปรุงแผนกลยุทธ์ให้เหมาะสมกับเหตุการณ์ความเสี่ยง ในการพิจารณาข้อมูลทั้งหมดที่กล่าวมานี้ คณะกรรมการและฝ่ายจัดการอาจเห็นโอกาสในการสร้างมูลค่าเพิ่มให้องค์กรได้ เช่น กรณีที่มีความเสี่ยงด้านเงินทุนและบุคลากร จึงทำให้เพิ่มโอกาสในการนำเทคโนโลยีแบบใหม่มาใช้ในองค์กรได้



ส่วนที่ 2 แนวปฏิบัติ (Guidelines)

แนวปฏิบัติ 2 GRC (Governance Risk and Compliance) Building Blocks (ต่อ)



2.3 การบริหารความเสี่ยง (Risk Management)

องค์ประกอบสำคัญของการบริหารความเสี่ยงที่คณะกรรมการควรกำกับดูแล เมื่อผู้รับผิดชอบนำเสนอเป้าหมาย ทิศทางกลยุทธ์องค์กร หรือการตัดสินใจดำเนินการในเรื่องสำคัญ หรือแม้แต่ในขั้นตอนของการติดตามผลการดำเนินงาน มีดังนี้

2.3.1 การดำเนินการดังกล่าวมีความสอดคล้องหรืออยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) หรือไม่ หากมีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้รับผิดชอบจะดำเนินการอย่างไร ควรหยุดที่จะดำเนินการต่อหรือมีการพิจารณาทบทวนระดับความเสี่ยงที่ยอมรับได้ใหม่ เป็นต้น

2.3.2 ความเสี่ยงที่สำคัญที่เกิดจากการดำเนินการตามทิศทาง กลยุทธ์และแผนการดำเนินงานได้ถูกระบุ และประเมินจัดลำดับความสำคัญ หรือไม่ ความเสี่ยงที่สำคัญขององค์กรนั้นมีเปลี่ยนแปลงไปตามสถานการณ์ เวลาและระยะเวลาการเติบโตขององค์กรหรือไม่

2.3.3 องค์กรมีแนวทางการจัดการความเสี่ยง (Risk Treatment) เหล่านี้ได้อย่างไร เช่น

ทำให้ความรุนแรงลดลง ยอมรับโดยไม่ทำอะไรเพิ่มเติม หากผู้ร่วมรับความเสี่ยง หลีกเลี่ยงความเสี่ยงนั้นโดยการทบทวนเป้าหมายหรือกลยุทธ์ใหม่ หรือยอมรับการมีความเสี่ยงเพื่อทำให้องค์กรเติบโตต่อไป

2.3.4 จัดให้มีการรายงานความเสี่ยงที่สำคัญ พร้อมทั้งวิธีการจัดการความเสี่ยงนั้นให้คณะกรรมการองค์กรทราบอย่างสม่ำเสมอหรืออย่างน้อยทุกไตรมาส เมื่อคณะกรรมการองค์กรได้รับรายงานแล้วพิจารณาความถูกต้องและครบถ้วนของความเสี่ยง ความเหมาะสมของวิธีการจัดการความเสี่ยงและให้ความเห็นหรือข้อเสนอแนะเกี่ยวกับความเสี่ยงและวิธีการจัดการความเสี่ยงที่มีประสิทธิภาพมากขึ้นหรืออาจเป็นข้อเสนอแนะในการปรับแผนกลยุทธ์ให้เหมาะสมกับความเสี่ยงที่ประเมินได้

2.4 การกำกับการปฏิบัติตามกฎระเบียบ กฎเกณฑ์ (Compliance)

คณะกรรมการควรกำกับดูแลให้มั่นใจ และสามารถปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับต่าง ๆ ได้อย่างถูกต้องและครบถ้วน การปฏิบัติตามกฎเกณฑ์ให้ครบถ้วนและถูกต้องนี้ถือเป็นวัตถุประสงค์หนึ่งขององค์กร ดังนั้น ผู้รับผิดชอบจะต้องประเมินความเสี่ยงด้าน Compliance และกำหนดวิธีการจัดการเพื่อลดความเสี่ยงดังกล่าว รวมทั้งรายงานผลให้คณะกรรมการทราบอย่างสม่ำเสมอ

ทั้งนี้ ในส่วนของการกำกับดูแล Compliance คณะกรรมการควรพิจารณาเรื่องสำคัญดังต่อไปนี้เมื่อผู้รับผิดชอบนำเสนอเป้าหมาย ทิศทางกลยุทธ์องค์กร หรือเรื่องสำคัญต่าง ๆ ให้กับคณะกรรมการพิจารณา

2.4.1 ประเด็นทางกฎหมาย จริยธรรม หรือเรื่องที่มีผลกระทบทางลบต่อผู้มีส่วนได้ส่วนเสียที่อาจเกิดขึ้นได้พร้อมแนวทางการบริหารจัดการ

2.4.2 มีความสอดคล้องหรือเป็นไปตามมาตรฐานหรือแนวปฏิบัติที่ดีที่เกี่ยวข้องหรือไม่

2.4.3 มีแนวทางการตรวจสอบเพื่อให้เกิดความมั่นใจว่าการปฏิบัติตามกฎระเบียบ และข้อบังคับอย่างไร

2.4.4 มีกระบวนการรายงานต่อคณะกรรมการและผู้มีส่วนได้ส่วนเสียที่สำคัญขององค์กรอย่างไร



ส่วนที่ 2 แนวปฏิบัติ (Guidelines)

แนวปฏิบัติ 3 การพิจารณาแต่งตั้งคณะกรรมการชุดย่อย

3.1 คณะกรรมการมีหน้าที่กำกับดูแล GRC ซึ่งประกอบด้วยระบบการกำกับดูแลกิจการ การบริหารความเสี่ยงและการปฏิบัติตามกฎเกณฑ์ ซึ่งถือว่าเป็นภาระความรับผิดชอบที่สูง ดังนั้น ในทางปฏิบัติ คณะกรรมการส่วนใหญ่จึงมักแต่งตั้งคณะกรรมการชุดย่อยต่าง ๆ เพื่อเข้ามาช่วยสนับสนุนการดำเนินงานของกรรมการ

3.2 โดยทั่วไป คณะกรรมการชุดย่อยที่คณะกรรมการแต่งตั้งหรือมอบหมาย เพื่อดำเนินการตามดูแลเรื่อง GRC ประกอบด้วยคณะกรรมการด้านกำกับดูแลกิจการ ในส่วนงานด้านการกำกับดูแลกิจการ คณะกรรมการตรวจสอบ ในส่วนงานกำกับดูแลให้มีการปฏิบัติตามกฎระเบียบ กฎเกณฑ์และข้อบังคับต่าง ๆ และคณะกรรมการบริหารความเสี่ยง เพื่อช่วยกำกับดูแลงานด้านบริหารความเสี่ยงและควบคุมภายใน

3.3 โดยปกติ องค์กรจะถูกกำหนดให้มีการจัดตั้งคณะกรรมการตรวจสอบ ตั้งคํ่ายงและควบคุมภายใน ดสนุนการกํ่าหน้าที่ของกรรมการ

เป็นงาน การเงิน และการปเพื่อช่วยคณะกรรมการกำกับดูแลการจํ่ากรายงานทางการเงิน การกํ่ากํ่าดูแลกิจการ การบริหารความเสี่ยง และการควบคุมภายใน ในขณะที่การจํ่าตั้งคณะกรรมการชุดย่อยด้านอื่น ๆ นั้น ขึ้นอยู่กับความเหมาะสมของแต่ละองค์กร โดยปัจจัยสำคัญในการพิจารณาคือการดูว่า คณะกรรมการสามารถกำกับดูแลงานนั้น ๆ ได้เองหรือไม่

3.4 อย่างไรก็ตาม แม้มีการแต่งตั้งคณะกรรมการชุดย่อยแล้ว คณะกรรมการยังมีบทบาทหน้าที่และความรับผิดชอบต่อการกำกับดูแลงานทั้งหมด โดยไม่อาจมอบความรับผิดชอบดังกล่าวไปยังคณะกรรมการชุดย่อยเพียงลำพังได้ ดังนั้น คณะกรรมการควรกำหนดให้คณะกรรมการชุดย่อยต่าง ๆ ต้องรายงานผลการปฏิบัติงานให้คณะกรรมการรับทราบอย่างสม่ำเสมอ

3.5 จากการที่การกำกับดูแลเรื่อง GRC เป็นการบูรณาการเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ ดังนั้น คณะกรรมการชุดย่อยต่าง ๆ ควรมีการทำงานที่สอดประสานกัน และเห็นภาพไปในทิศทางเดียวกัน โดยคณะกรรมการอาจพิจารณาให้มีการดำเนินการดังต่อไปนี้เพื่อเอื้อให้เกิดการบูรณาการในการทำงานระหว่างคณะกรรมการชุดย่อย **(มี 2 ข้อย่อย ตามเอกสารวาระ 3.2)**



ส่วนที่ 2 แนวปฏิบัติ (Guidelines)

แนวปฏิบัติ 4 บทบาทหน้าที่ของคณะกรรมการชุดย่อยต่อ GRC



4.1 คณะกรรมการกำกับดูแลกิจการ มีบทบาทหน้าที่ต่อไปนี้

- 4.1.1 คณะกรรมการกำกับดูแลกิจการมีบทบาทหน้าที่กำหนดกรอบการกำกับดูแลกิจการ ตามหลักการกำกับดูแลกิจการของสำนักงานคณะกรรมการรัฐวิสาหกิจ
- 4.1.2 สร้างและส่งเสริมวัฒนธรรมที่ดีและจรรยาบรรณในองค์กรที่สนับสนุนให้องค์กรสามารถบรรลุตามกลยุทธ์และวัตถุประสงค์ที่กำหนดไว้
- 4.1.3 พิจารณากรอบและแนวปฏิบัติ GRC ขององค์กรว่าได้รับการออกแบบและปฏิบัติอย่างเหมาะสมตั้งแต่ระดับคณะกรรมการ ผู้บริหาร ผู้รับผิดชอบ และพนักงานทุกคน
- 4.1.4 จัดแนวทางการประเมินการทำงานของคณะกรรมการและผู้รับผิดชอบให้สอดคล้องกับกรอบและแนวปฏิบัติ GRC

4.2 คณะกรรมการบริหารความเสี่ยง มีบทบาทหน้าที่ต่อไปนี้

- 4.2.1 กำกับดูแลให้มีการกำหนดระดับความเสี่ยงที่ยอมรับได้ขององค์กร เพื่อเป็นกรอบให้ผู้รับผิดชอบใช้ในการพิจารณาดำเนินงาน
- 4.2.2 หารือกับผู้รับผิดชอบเกี่ยวกับระดับความเสี่ยงที่ยอมรับได้อย่างสม่ำเสมอ โดยเฉพาะเมื่อสภาพแวดล้อมเปลี่ยนแปลงหรือมีอากาศใหม่ ๆ เกิดขึ้น
- 4.2.3 กำกับดูแลให้ผู้รับผิดชอบมีการวางแผนการบริหารจัดการความเสี่ยงที่ดี ซึ่งประกอบด้วย การระบุประเมิน จัดการ ติดตามและรายงานความเสี่ยงที่สำคัญ รวมถึงมีการพิจารณาปรับปรุงระบบการบริหารความเสี่ยงอย่างต่อเนื่อง
- 4.2.4 ให้คำแนะนำเกี่ยวกับความเสี่ยงสำคัญแก่ผู้รับผิดชอบจัดการอย่างทันเวลา
- 4.2.5 กำกับดูแลการปฏิบัติและสอบทานผลการประเมินความเสี่ยงทุกด้านรวมถึงการบ่งชี้และรายงานความเสี่ยงที่สำคัญขององค์กร
- 4.2.6 ในกรณีที่กำกับดูแลการบริหารความเสี่ยงด้านที่มีความซับซ้อนและสำคัญ อาจพิจารณาสรรหากรรมการที่มีความรู้ความชำนาญพิเศษในด้านนั้น ๆ
- 4.2.7 สอดส่องพฤติกรรมที่ไม่เหมาะสมที่มีผลต่อประสิทธิภาพของระบบการบริหารความเสี่ยง และทำให้องค์กรยอมรับความเสี่ยงมากเกินไป

4.3 คณะกรรมการกำกับการปฏิบัติตามกฎหมาย มีบทบาทหน้าที่ต่อไปนี้

- 4.3.1 ติดตามและกำกับดูแลให้มั่นใจว่ากรรมการ ผู้บริหาร ผู้รับผิดชอบและพนักงานทุกคน มีการปฏิบัติตามจรรยาบรรณกฎระเบียบ และข้อบังคับ ทั้งที่กำหนดจากภายในองค์กรและภายนอก
- 4.3.2 ดูแลให้มีการประเมินกฎ ระเบียบ และข้อบังคับที่อาจส่งผลกระทบต่อการทำงานขององค์กรได้พร้อมทั้งมีการพิจารณาถึงความเพียงพอและความเหมาะสมของระบบการควบคุมภายในเพื่อป้องกันความเสี่ยงจากการไม่ปฏิบัติตามกฎระเบียบ และข้อบังคับ
- 4.3.3 กำกับดูแลให้มั่นใจว่าประเด็นสำคัญที่ต้องปฏิบัติตามกฎ ระเบียบ และข้อบังคับต่าง ๆ ทั้งภายในและภายนอก ได้ถูกนำไปบูรณาการอยู่ในทุกกระบวนการที่ปฏิบัติเป็นประจำวัน รวมถึงกำกับดูแลให้คณะกรรมการชุดย่อยอื่น ๆ เพื่อทำหน้าที่แทนได้

เช่น คณะกรรมการกำกับดูแลกิจการ หรือคณะกรรมการตรวจสอบ เป็นต้น

4.4 คณะกรรมการตรวจสอบ มีบทบาทหน้าที่ต่อไปนี้

- 4.4.1 ทำหน้าที่สอบทานการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎ ระเบียบและข้อบังคับ และทำหน้าที่รับรายงานผลการสอบทานโดยตรงจากผู้ตรวจสอบภายในเพื่อให้มั่นใจว่าองค์กรได้จัดให้มีระบบการควบคุมภายในที่มีประสิทธิภาพ เพียงพอ และเหมาะสมต่อการปฏิบัติให้บรรลุตามวัตถุประสงค์ของเรื่องเหล่านั้น โดยสรุปแล้ว คณะกรรมการตรวจสอบถือว่ามีส่วนสำคัญ เพราะทำหน้าที่ให้ความเชื่อมั่น ต่อการดำเนินงานขององค์กรว่ามีความถูกต้อง โปร่งใส และตรวจสอบได้
- 4.4.2 ด้วยการหน้าที่ของคณะกรรมการตรวจสอบที่ต้องติดตามดูแลและสอบทานภาพรวมของการดำเนินงานขององค์กร คณะกรรมการจึงมีบทบาทหน้าที่ให้คณะกรรมการตรวจสอบทำหน้าที่ติดตามดูแลในส่วนของการกำกับดูแลกิจการ การบริหารความเสี่ยง และการติดตามดูแลให้มีการปฏิบัติตามกฎระเบียบ และข้อบังคับร่วมด้วย โดยเฉพาะอย่างยิ่งในองค์กรที่มีขนาดกลางและขนาดเล็ก และองค์กรที่ไม่มีความซับซ้อนในการดำเนินงาน