แนวปฏิบัติด้านการกำกับดูแลกิจการที่ดี
การบริหารความเสี่ยงและการควบคุมภายใน
และการปฏิบัติตามกฎระเบียบ
(Governance, Risk and Compliance : GRC)

บริษัท อู่กรุงเทพ จำกัด

THE BANGKOK DOCK COMPANY (1957) LIMITED

บทนำ

บริษัทที่จะอยู่ได้อย่างยั่งยืนในโลกยุคใหม่นี้ต้องเป็นบริษัทที่มีพื้นฐานแข็งแกร่งและมีความยืดหยุ่นต่อการปรับเปลี่ยนกลยุทธ์และการบริหาร เข้าใจและจัดการความเสี่ยงได้เป็นอย่างดีภายใต้กฎหมายและระเบียบที่เกี่ยวข้อง ประกอบกับความคาดหวังของผู้มีส่วนได้ส่วนเสียที่ต้องการให้บริษัทเติบโตและทำธุรกิจอย่างโปร่งใส ตอบสนองต่อการเปลี่ยนแปลงได้เร็วและมีประสิทธิภาพ จึงทำให้เกิดเหตุผลมากมายที่ผลักดันให้บริษัทต้องปฏิบัติงานอย่างบูรณาการ ดังนั้น คณะกรรมการบริษัทจึงต้องสามารถกำกับดูแลบริษัทให้สำเร็จลุล่วงตามแผนกลยุทธ์ที่ต้องการ บทบาทหน้าที่ของคณะกรรมการบริษัทจึงต้องมองในภาพรวมของการกำกับดูแลกิจการ การบริหารความเสี่ยงและการควบคุมภายใน และการปฏิบัติตามกฎเกณฑ์ ให้เป็นเรื่องเดียวกัน หรือที่เรียกเป็นคำเดียวกันว่า Governance, Risk and Compliance (GRC) เนื่องจากภารกิจในองค์ประกอบแต่ละด้านของ GRC นั้นต้องทำอย่างต่อเนื่อง ละเอียด และรวดเร็วคณะกรรมการบริษัทในองค์กรขนาดเล็กอาจทำได้เองทั้งหมด แต่ในองค์กรขนาดใหญ่อาจแต่งตั้งคณะกรรมการชุดย่อยเพื่อช่วยทำหน้าที่ในแต่ละด้าน เช่น การกำกับดูแลกิจการ การบริหารความเสี่ยงและการควบคุมภายใน การกำกับการปฏิบัติตามกฎเกณฑ์

อย่างไรก็ตาม การแต่งตั้งคณะกรรมการชุดย่อย เป็นเพียงการแบ่งเบาภาระหน้าที่การปฏิบัติงานจากคณะกรรมการบริษัทเท่านั้น ความรับผิดชอบทั้งหมดยังคงอยู่กับคณะกรรมการบริษัทเช่นเดิม ด้วยเหตุนี้บริษัท อู่กรุงเทพ จำกัด จึงได้จัดทำแนวปฏิบัติด้านการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน และการปฏิบัติตามกฎระเบียบ (Governance, Risk and Compliance : GRC) นี้ขึ้น เพื่อให้คณะกรรมการบริษัทได้ทราบถึงความสำคัญ องค์ประกอบ บทบาทหน้าที่และการทำให้บริษัทบูรณาการการกำกับดูแลกิจการ (Governance) การบริหารความเสี่ยงและการควบคุมภายใน (Risk) และการการกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance) ได้อย่างสำเร็จผล

แผนกแผนงานและงบประมาณ

มกราคม 2569

)

สารบัญ

ส่วนที่ 1

หลักการสำคัญ Key Principles

1 คณะกรรมการมีบทบาทและความรับผิดชอบในฐานะผู้นำองค์กรที่สร้างคุณค่าให้แก่กิจการอย่างยั่งยืน โดยการการกำกับดูแลให้บริษัทมีกลยุทธ์ที่เสริมสร้างการเจริญก้าวหน้า ดำเนินธุรกิจอย่างมีจริยธรรม โปร่งใส คำนึงถึงผู้มีส่วนได้ส่วนเสียทุกฝ่าย และปฏิบัติถูกต้องตามกฎหมาย (โปรดดูแนวปฏิบัติ 1)

2 คณะกรรมการพึงใช้แนวคิดการบูรณาการ GRC เป็นกรอบในการขับเคลื่อนและส่งเสริมให้องค์กรดำเนินกิจการตามแนวปฏิบัติสำคัญ 4 ประการ ตามหลักของ The Office of Compliance and Ethics Group (OCEG) ได้แก่ (โปรดดูแนวปฏิบัติ 1)

2.1 **Learn** หมายถึง การเรียนรู้และเข้าใจอย่างถ่องแท้ถึงบริบทในการดำเนินธุรกิจ วัฒนธรรมองค์กร และความคาดหวังของผู้มีส่วนได้ส่วนเสีย

2.2 **Align** หมายถึง การนำสิ่งที่ได้เรียนรู้มากำหนดวัตถุประสงค์ของบริษัท แล้วจึงระบุความเสี่ยงที่อาจเกิดขึ้น ซึ่งทำให้บริษัทไม่บรรลุวัตถุประสงค์

2.3 **Perform** หมายถึง การขับเคลื่อนให้บริษัทไปสู่เป้าหมายหรือวัตถุประสงค์ ด้วยกระบวนการทำงานที่มีประสิทธิภาพ ถูกต้องตามกฎระเบียบ และมีระบบการควบคุมภายในที่ดี

2.4 **Monitor** หมายถึง มีระบบติดตามดูแลการปฏิบัติงานอย่างเพียงพอ เหมาะสม เพื่อให้เป็นไปตามวัตถุประสงค์ที่ตั้งไว้

3 คณะกรรมการควรกำกับดูแลให้บริษัทมีวิสัยทัศน์และวิธีการปฏิบัติแบบก้าวหน้า ทำให้บริษัทสามารถบรรลุวัตถุประสงค์อย่างมีเหตุผลและมีจริยธรรม ท่ามกลางความไม่แน่นอนต่อการเปลี่ยนแปลงอย่างรวดเร็วและรุนแรงของเศรษฐกิจ ตลาด เทคโนโลยี บุคลากร กฎหมาย สิ่งแวดล้อม สังคม เป็นต้น ความไม่แน่นอนเหล่านี้ทำให้บริษัทต้องพิจารณาทั้งความเสี่ยงและโอกาสที่อาจเกิดขึ้น เพื่อลดความเสี่ยงหรือเพิ่มโอกาสในการบรรลุวิสัยทัศน์และกลยุทธ์ที่กำหนดไว้

4 คณะกรรมการควร “กำกับดูแลกิจการ” (Governance) และกำหนดทิศทางการดำเนินธุรกิจอันเป็นไปเพื่อความยั่งยืน ซึ่งมีพื้นฐานมาจากการพิจารณาปัจจัยแวดล้อมทั้งภายในและภายนอก ตลอดจนผลประโยชน์ของผู้มีส่วนได้ส่วนเสียอย่างรอบด้าน พร้อมสื่อสารกลยุทธ์ นโยบาย และหลักการสำคัญต่างๆ แก่ฝ่ายจัดการเพื่อนำไปสู่การปฏิบัติ ซึ่งครอบคลุมทั้ง “การบริหารความเสี่ยง” (Risk Management) ที่มีประสิทธิภาพ ยืดหยุ่น และตอบสนองการเปลี่ยนแปลงได้อย่างรวดเร็ว และ “การปฏิบัติตามกฎหมายระเบียบต่างๆ” (Compliance) อย่างครบถ้วนสมบูรณ์ (โปรดดูแนวปฏิบัติ 2)

5 ทั้งนี้ บทบาทและความรับผิดชอบของคณะกรรมการมิได้แยกเป็นส่วนๆ หากแต่คณะกรรมการต้องดูแลให้บริษัทสามารถเชื่อมโยงและประสานงานที่เกี่ยวข้องกับการกำกับดูแลกิจการ (Governance) การบริหารความเสี่ยง (Risk Management) และการปฏิบัติตามกฎระเบียบ (Compliance) ให้ร้อยเรียงเป็น “ภาพเดียวกัน” ภายใต้วัฒนธรรมองค์กรที่มีจริยธรรม โปร่งใส และซื่อสัตย์ ซึ่งรวมเรียกว่าการบูรณาการ Governance, Risk and Compliance หรือ GRC (โปรดดูแนวปฏิบัติ 2)

6 สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจได้ให้แนวทางว่าคณะกรรมการอาจแต่งตั้งกรรมการที่มีความรู้ความชำนาญที่เหมาะสม เป็นคณะกรรมการชุดย่อยที่มีหน้าที่เฉพาะในการศึกษาเรื่องสำคัญที่เกิดขึ้นเป็นประจำ หรือเรื่องที่ต้องการการดูแลอย่างใกล้ชิด ซึ่งจะเป็นการเพิ่มประสิทธิภาพของคณะกรรมการได้ เช่น คณะกรรมการตรวจสอบ คณะอนุกรรมการบริหารความเสี่ยงและการควบคุมภายใน อย่างไรก็ตาม คณะกรรมการบริษัทยังคงมีความรับผิดชอบเต็มที่ต่อบทบาทหน้าที่ที่ได้มอบหมายไปยังคณะกรรมการชุดย่อย (โปรดดูแนวปฏิบัติ 3-4)

7 คณะกรรมการชุดย่อย เช่น คณะอนุกรรมการบริหารความเสี่ยงและการควบคุมภายใน ได้รับการแต่งตั้งและมอบหมายงานจากคณะกรรมการบริษัท เพื่อช่วยปฏิบัติหน้าที่กำกับดูแลงานบริหารความเสี่ยงอย่างใกล้ชิดกับหน่วยงานรับผิดชอบ และทำให้คณะกรรมการบริษัทได้รับรายงานความเสี่ยงที่มีคุณภาพอย่างทันเวลา (โปรดดูแนวปฏิบัติ 3-4)

ส่วนที่ 2
นโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการควบคุมภายใน และการปฏิบัติตามกฎเกณฑ์ (Governance, Risk Compliance : GRC)

นโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน และการปฏิบัติตามกฎเกณฑ์ (Governance, Risk Compliance: GRC) ประจำปีงบประมาณ 2569

GRC (Governance, Risk Management, and Compliance) เป็นกลยุทธ์ในการดำเนินงานเพื่อขับเคลื่อนองค์กรไปสู่การบริหารองค์กรแบบบูรณาการอย่างมีคุณค่า (Business Integrity) และการมีคุณธรรมในการบริหาร เช่น การกำหนดกฎเกณฑ์ ระเบียบคำสั่ง และการปฏิบัติ การให้คุณให้โทษจะต้องมีความชัดเจนสอดคล้องกันทั่วทั้งองค์กรในทุกมุมมองของการบริหารตามหลัก Balanced Scorecards และมีการปฏิบัติอย่างจริงจัง รวมถึงผู้บริหารทุกระดับมีหน้าที่ปลูกฝังจิตสำนึกด้านการบริหารความเสี่ยงและการควบคุมภายใน ปรับเปลี่ยนวัฒนธรรมขององค์กร ให้แก่พนักงานและบุคลากร เพื่อสร้างเป็นวัฒนธรรมในการทำงานไปสู่วัตถุประสงค์และเป้าหมายด้านวัฒนธรรมองค์กรที่คาดหวังเพื่อเพิ่มประสิทธิภาพ สนับสนุนหรือผลักดันให้การดำเนินงานขององค์กรบรรลุตามวัตถุประสงค์ได้ดีขึ้น

ปัจจัยสำคัญที่จำเป็นที่ใช้ในการขับเคลื่อนการดำเนินงาน การปฏิบัติการที่มีศักยภาพอย่างยั่งยืนตามหลักการ GRC คือ

1. การบูรณาการด้าน Governance + Risk Management + Compliance (GRC) ที่เป็นรูปธรรมคณะกรรมการและผู้บริหารต้องจัดให้มีการบริหารการเปลี่ยนแปลงโดยเชื่อมโยงให้มีการจัดการที่ดี (Good Governance) เข้ากับกระบวนการบริหารความเสี่ยง (COSO-ERM) ทั่วทั้งองค์กร และการควบคุมความเสี่ยงของกิจกรรมต่าง ๆ ในลักษณะเชิงรุก คือการป้องกันปัญหาที่อาจเกิดขึ้นและกระทบกับการสร้างคุณค่าเพิ่มอย่างมีประสิทธิภาพให้กับองค์กร

2. เชื่อมโยง GRC เข้ากับการดำเนินการและมีการวัดผลที่ตรงประเด็น บูรณาการด้าน GRC ที่ดี มีคุณภาพ มีคุณค่าและส่งเสริมประสิทธิภาพในการดำเนินงานและการปฏิบัติการ ช่วยลดช่องว่างของการดำเนินงาน ที่เกิดขึ้นจากการแยกกันทำงานในแบบต่างคนต่างทำ หรือเป็นตามลักษณะของงาน โดยคำนึงถึงวัตถุประสงค์ กลยุทธ์ กระบวนการ ระบบ การส่งเสริมให้คณะกรรมการสามารถกำกับดูแล องค์กรและให้คำแนะนำแก่ผู้บริหาร เพื่อดำเนินงานให้ปฏิบัติตามกฎระเบียบที่ เกี่ยวข้องได้อย่างมั่นใจ โดยผู้บริหารต้องจัดให้มีการบริหารความเสี่ยงที่เป็นระบบ มุ่งเน้นความเสี่ยงที่ตรงประเด็นและสามารถจัดกระบวนการทำงานเพื่อให้มี การปฏิบัติตามระเบียบหรือ การควบคุมภายในได้อย่างเหมาะสม การดำเนินงานที่สมเหตุสมผล รวมถึงการนำเทคโนโลยีมาสนับสนุนการทำงานให้มีประสิทธิภาพ และการสื่อสารข้อมูลอย่างถูกต้องเหมาะสมทันเวลาต่อผู้เกี่ยวข้องทุกระดับ จนได้ผลลัพธ์ที่สามารถวัดประสิทธิภาพของคุณค่าเพิ่มได้อย่างเป็นรูปธรรม

3. กำหนดให้มีการบริหารความเสี่ยงและการควบคุมภายในทั่วทั้งองค์กรและเป็นความรับผิดชอบของบุคลากรทุกระดับโดยต้องให้ความสำคัญกับการบริหารความเสี่ยงในด้านต่าง ๆ ให้อยู่ในระดับเพียงพอและเหมาะสม ผู้บริหาร พนักงานและบุคลากร นำระบบการการบริหารความเสี่ยงและการควบคุมภายในมาใช้เป็นกลไกล ในการกำหนดมาตรการควบคุม เพื่อป้องกันและลดโอกาสการนำไปสู่ความเสี่ยง ดำเนินงานระดับกิจกรรมที่จะไม่บรรลุวัตถุประสงค์ที่กำหนด และความเสี่ยงจากการทุจริตคอร์รัปชั่น

4. การควบคุมภายใน เป็นส่วนหนึ่งของกระบวนการปฏิบัติงานประจำวันที่ต้องปฏิบัติอย่างต่อเนื่อง ตั้งแต่การวางแผน (Planning) การดำเนินงาน (Executing) และการติดตามผล (Monitoring) ทั้งระหว่างการปฏิบัติงานและการประเมินการควบคุมด้วยตนเอง (Control Self-Assessment : CSA) การควบคุมภายในที่เพียงพอในการลดความเสี่ยงของบุคคล ช่วยกำกับคนมากขึ้น เช่น การกำกับติดตาม (Monitoring) การใช้ระบบควบคุมการตรวจสอบคุณภาพงานและการทดสอบผลงานว่าใช้งานได้จริงอย่างสม่ำเสมอและมีประสิทธิผลหรือกระบวนการฝึกอบรมบุคลากร เพื่อให้เหมาะสมกับความรับผิดชอบในภารกิจ การกำหนดให้มีมาตรฐานการทำงานที่ชัดเจน

5. นำระบบการบริหารความเสี่ยงมาเป็นส่วนหนึ่งของการตัดสินใจในการกำหนดยุทธศาสตร์แนวทางการดำเนินการ ตัวชี้วัด และเป้าหมาย รวมถึงการมุ่งเน้นให้บรรลุความสำเร็จตามเป้าหมาย ตัวชี้วัด แนวทางการดำเนินการและยุทธศาสตร์ที่กำหนดไว้

6. นำระบบบริหารความเสี่ยง (Risk Management System : RMS) ซึ่งเป็นเทคโนโลยีดิจิทัลมาช่วยในการกำกับดูแลที่ดี ทำหน้าที่เป็นระบบเฝ้าระวัง เป็นเครื่องเตือนภัยล่วงหน้า เป็นระบบอัตโนมัติที่กำกับการปฏิบัติในลักษณะที่ฝ่าฝืนกฎเกณฑ์ หรือเป็นระบบ รายงานความผิดปก

7. กำหนดให้มีการติดตาม ประเมิน ทบทวน ปรับปรุงและรายงานผลการกำกับดูแลกิจการ บริหารความเสี่ยงและการควบคุมภายในทุกไตรมาส

ส่วนที่ 3

แนวปฏิบัติ Guidelines

แนวปฏิบัติ 1 : บทบาทสำคัญของคณะกรรมการบริษัทใน การกำกับดูแลกิจการ

1.1 ความหมายของ Governance, Risk and Compliance (GRC)

1.1.1 GRC หมายถึง การบริหารงานในบริษัทให้ทุกหน่วยงาน ระบบงาน กระบวนการ บุคลากร และข้อมูลประสานกันอย่างเป็นระบบหรือเรียกว่าบูรณาการ (Integration) เพื่อทำ ให้บริษัทบรรลุกลยุทธ์ วัตถุประสงค์และเป้าหมาย ที่กำ หนดไว้โดยคำนึงถึงความคาดหวังอย่างมีเหตุผลของผู้มีส่วนได้ส่วนเสีย กลุ่มต่างๆ

1.1.2 GRC จึงนับเป็นการบริหารงานที่ครอบคลุมเป็นภาพเดียวกันทั้งหมดของ

1.1.2.1 “การกำกับดูแลกิจการ” ที่เริ่มต้นจากการทำ ความเข้าใจอย่างถ่องแท้ในบริบทขององค์กรผ่านการประเมินสภาพแวดล้อมทางธุรกิจ พลวัติภายในของอุตสาหกรรม ตลอดจนความคาดหวังต่างๆ ของผู้มีส่วนได้ส่วนเสีย เพื่อใช้เป็นแนวทางในการพัฒนากลยุทธ์องค์กรและรูปแบบการดำเนินธุรกิจที่เหมาะสมต่อไป

1.1.2.2 “การประเมินความเสี่ยง” ที่อาจทำ ให้การดำเนินกลยุทธ์ไม่เป็นไปตามเป้าหมาย พร้อมแสวงหาวิธีในการควบคุม / จัดการ

1.1.2.3 “การปฏิบัติงานให้เป็นไปตามกฎระเบียบ” ถูกต้องตามจรรยาบรรณและแนวปฏิบัติทั้งหลายที่เกี่ยวข้อง

ตัวอย่างของการบริหารงานตามหลักการ GRC

ปัจจัยแวดล้อมในการดำเนินธุรกิจ :

- บริษัทมีช่องทางการจัดจำหน่ายเพียงทางเดียว โดยเช่าพื้นที่ในห้างสรรพสินค้า
- บริษัทเล็งเห็นว่าการทำธุรกิจแบบออนไลน์เติบโตขึ้นอย่างต่อเนื่องและมีแนวโน้มสูงขึ้น เนื่องจากพฤติกรรมของผู้บริโภคที่ค่อยๆ เปลี่ยนจากการซื้อสินค้าตามศูนย์การค้าต่างๆ มาเป็นการสั่งซื้อผ่านช่องทางออนไลน์ที่ง่าย สะดวก และประหยัดเวลามากกว่า
- บริษัทกำลังเผชิญกับคู่แข่งหน้าใหม่ๆ ซึ่งมีช่องทางการจัดจำ หน่ายที่หลากหลายและทันสมัยกว่า ส่งผลให้ยอดขาย / ผลกำไรของบริษัทลดลงต่อเนื่องในช่วงที่ผ่านมาทิศทางและเป้าหมายกลยุทธ์
- บริษัทมีเป้าหมายต้องการกำไรเพิ่มขึ้นอย่างน้อยร้อยละ 20 จากปีก่อน
- บริษัทกำหนดกลยุทธ์โดยเพิ่มช่องทางการขายแบบออนไลน์ให้ได้อย่างน้อยร้อยละ 30 ของยอดขายทั้งหมด

การบริหารจัดการแบบ GRC :

- ประเมินความเสี่ยงของช่องทางการขายแบบออนไลน์ ซึ่งพบว่าเป็นช่องทางใหม่ที่ระบบงานเดิมยังไม่สามารถรองรับได้
- ฝ่ายจัดการตั้งคณะทำงานศึกษาและปรับรูปแบบการทำ งานเดิมของทั้งฝ่ายขายฝ่ายการตลาด และฝ่ายบัญชี เพื่อให้การทำงานทั้งหมดประสานกัน และนำระบบเทคโนโลยีแบบใหม่มาใช้ในการทำงาน

- พิจารณาว่าในแต่ละงานต้องมีกฎหมายใดเกี่ยวข้องบ้าง
- ฝ่ายจัดการรายงานความคืบหน้าตามแผนกลยุทธ์ให้คณะกรรมการทราบทุกไตรมาส

ในอดีต บริษัทมักไม่ได้นำการบริหารแบบ GRC มาใช้ จึงมีแต่เป้าหมายและเริ่มปฏิบัติในกระบวนการต่างๆ โดยไม่ได้คำนึงถึงจุดเสี่ยงและหาแผนรองรับ เมื่อทำ แล้วไม่ประสบความสำเร็จก็เปลี่ยนเป้าหมายหรือเริ่มต้นทำงานใหม่ ทำให้เสียงบประมาณและเวลาเป็นจำนวนมาก คณะกรรมการจึงควรผลักดันให้องค์กรและฝ่ายจัดการมีการพิจารณานำหลักการ GRC มาปรับใช้ในการดำเนินกลยุทธ์และบริหารงาน เพื่อให้องค์กรประสบความสำเร็จตามแผนที่วางไว้

1.2 ทำไมคณะกรรมการบริษัทต้องให้ความสนใจต่อ GRC

1.2.1 คณะกรรมการมีบทบาทสำคัญในฐานะผู้นำ ที่สร้างคุณค่าให้แก่กิจการอย่างยั่งยืน รวมทั้งมีส่วนร่วมตั้งแต่การกำกับดูแลกลยุทธ์และการจัดการ เพื่อทำให้บริษัทสามารถแข่งขันและปรับตัวกับการเปลี่ยนแปลงต่างๆ ได้ ดังนั้น คณะกรรมการบริษัทจึงถือเป็นกลุ่มคนสำคัญที่จะต้องผลักดันให้บริษัทมีระบบการจัดการเป็นแบบ GRC เพื่อที่จะสามารถมั่นใจได้ว่าบริษัทจะสามารถดำเนินงานให้บรรลุผลสำเร็จตามกลยุทธ์ที่กำหนดไว้

1.2.2 ในกรณีที่คณะกรรมการไม่กำกับดูแลให้องค์กรมีการนำหลักการบริหารจัดการแบบ GRC มาใช้ บริษัทอาจจะเผชิญกับปัญหาต่างๆ ได้ดังต่อไปนี้

1.2.2.1 การขาดความเข้าใจในความคาดหวังของผู้มีส่วนได้ส่วนเสียอย่างรอบด้านเพียงพอ จนส่งผลให้รูปแบบการดำเนินธุรกิจขาดมุมมองในระยะยาว และไม่เป็นไปเพื่อความยั่งยืน

1.2.2.2 การเสียโอกาสในการแข่งขัน เนื่องจากมีปัญหาการจัดการภายในบริษัท

1.2.2.3 การดำเนินงานที่ไม่มีประสิทธิภาพ มีต้นทุนการดำเนินงานสูงกว่าปกติ

1.2.2.4 การไม่สามารถเข้าใจการปฏิบัติงานที่มีความเสี่ยงและจุดอ่อนที่สำคัญเกี่ยวกับการควบคุมเนื่องจากกระบวนการในบริษัทมีความซับซ้อน แยกส่วน ไม่เชื่อมโยงกัน

1.2.2.5 การมีรายงานความเสี่ยงจากหลายประเภทและหลายหน่วยงาน โดยไม่สามารถวิเคราะห์ภาพรวมได้ว่าความเสี่ยงหลักคืออะไร ฝ่ายจัดการต้องดำเนินการอย่างไร และจะมีผลกระทบต่อกลยุทธ์อย่างไรบ้าง

1.2.2.6 การไม่มีรายงานการปฏิบัติที่ไม่ถูกต้องตามกฎระเบียบ (Non-compliance) อย่างทันเวลา ทำให้ทราบเมื่อปัญหาได้เกิดขึ้นแล้ว จึงแก้ไขได้ยากและอาจส่งผลให้เกิดผลกระทบต่อภาพลักษณ์ขององค์กรได้

1.2.3 จากการที่ GRC เป็นการบูรณาการกันในทุกส่วนที่เกี่ยวข้องกับการดำเนินงานและมีส่วนเกี่ยวข้องกับหน่วยงานหลายฝ่ายภายในองค์กร คณะกรรมการจึงมีบทบาทสำคัญที่จะต้องแสดงเจตจำนง (Tone from the top) ให้คนในองค์กรเห็นพ้องต้องกันถึงความจำเป็นที่ต้องนำ หลักการ GRC มาปรับใช้เพื่อเกิดการทำงานที่สอดประสานกันตามนโยบายที่คณะกรรมการกำหนด

1.2.4 การแสดงเจตจำนงของคณะกรรมการ เพื่อสร้างการรับรู้ให้แก่บุคลากรทุกระดับภายในองค์กรสามารถทำผ่านวิธีต่างๆ ได้ดังนี้

1.2.4.1 กำหนดเป็นวาระหรือหัวข้อการประชุมคณะกรรมการที่ชัดเจน เพื่อติดตามดูแลอย่างต่อเนื่อง

1.2.4.2 จัดทำเป็นนโยบายที่ชัดเจนเพื่อสื่อสารถึงแนวทางการปฏิบัติงานตามหลักการ GRC ให้ครอบคลุมทั่วทั้งองค์กร

1.2.4.3 กำหนดรูปแบบรายงานของฝ่ายจัดการ ให้มีการสอดประสานกันในทุกองค์ประกอบตามหลักการ GRC เพื่อให้คณะกรรมการเห็นภาพอย่างครบถ้วน

1.3. คุณลักษณะของบริษัทที่บูรณาการ GRC ได้อย่างมีประสิทธิภาพ

บริษัทที่มีการบูรณาการ GRC อย่างมีประสิทธิภาพ จะมีความมั่นใจต่อการบรรลุกลยุทธ์ วัตถุประสงค์ และเป้าหมายที่กำหนดไว้ เนื่องจากบริษัทมีวิธีการบริหารงานที่มีประสิทธิภาพจากทั้งกระบวนการ บุคลากร ข้อมูลและเทคโนโลยีสารสนเทศ ภายใต้วัฒนธรรมและจรรยาบรรณที่ดีและโปร่งใส ดังนั้น บริษัทที่มีหลักการบริหารจัดการแบบ GRC มักมีลักษณะต่างๆ ดังนี้ คณะกรรมการได้รับทราบข้อมูลที่จำเป็นต่อการกำ กับดูแลแบบเชิงรุกและทันเวลา ตลอดจนสามารถดำเนินงานร่วมกับฝ่ายจัดการได้อย่างมีประสิทธิภาพ

1.3.2 เกิดความเข้าใจที่ถูกต้องเกี่ยวกับบริบทขององค์กร ประเด็นความยั่งยืน และความคาดหวังของผู้มีส่วนได้ส่วนเสียอย่างรอบด้าน จนสามารถนำมาใช้เป็นแนวทางในการกำ หนดรูปแบบการดำเนินธุรกิจ / กลยุทธ์ระยะยาวได้อย่างเหมาะสม

1.3.3 การบริหารงานมีความยืดหยุ่น คล่องตัว มีการใช้ต้นทุนน้อยกว่าบริษัทอื่นที่ดำเนินธุรกิจลักษณะเดียวกัน

1.3.4 การมองเห็นโอกาสในการแข่งขัน และมีความมั่นใจต่อการนำมาปฏิบัติให้ประสบผลสำเร็จ

1.3.5 มีการทำงานคล่องตัว ไม่ซับซ้อน หรือเสียเวลาโดยไม่จำเป็น และไม่เกิดความขัดแย้งระหว่างหน่วยงานภายในองค์กร

1.3.6 การลดการสูญเสียทรัพย์สินต่างๆที่สำคัญของบริษัท

1.3.7 การเข้าถึงข้อมูลที่จำเป็นได้ทันต่อการตัดสินใจ โดยผู้ที่มีอำนาจหน้าที่อย่างเหมาะสม

1.3.8 กระบวนการดำเนินงานตามแผนกลยุทธ์ที่กำ หนดไว้ เป็นไปตามขอบเขต / ระยะเวลาที่กำหนด และให้ผลลัพธ์ที่เป็นไปตามเป้าประสงค์

1.4 บทบาทโดยรวมของคณะกรรมการที่มี GRC

1.4.1 จากการที่คณะกรรมการจะต้องปฏิบัติหน้าที่ด้วยความรับผิดชอบระมัดระวัง (Duty of Care) และซื่อสัตย์สุจริตต่อองค์กร (Duty of Loyalty) คณะกรรมการบริษัทจึงจำเป็นที่จะต้องกำกับดูแลให้บริษัทมีการบริหารจัดการแบบ GRC กล่าวคือมีการกำ หนดและเข้าใจกลยุทธ์ วัตถุประสงค์ และเป้าหมายอย่างชัดเจน เพื่อนำไปสู่การประเมินและวางระบบการบริหารความเสี่ยงทั้งในระดับองค์กร และหน่วยงาน ตลอดจนมีการประเมินและควบคุมให้มีการปฏิบัติงานถูกต้องตามกฎหมายและระเบียบกฎเกณฑ์ต่างๆ ที่เกี่ยวข้อง โดยสรุปคือ คณะกรรมการบริษัทต้องสามารถเข้าใจและติดตามการบริหารงานของฝ่ายจัดการให้เป็นภาพรวมทั้งหมด (Integration) แทนการดูแบบแยกส่วน (Silo) นั่นเอง

1.4.2 สิ่งที่คณะกรรมการควรให้ความสำคัญมากที่สุด คือการแนะนำและติดตามให้ฝ่ายจัดการดำเนินการต่างๆ ดังนี้

1.4.2.1 ประเมินความเหมาะสมของทิศทาง / รูปแบบการดำเนินธุรกิจในปัจจุบัน ว่ามีประสิทธิภาพเพียงพอที่จะรับมือกับความท้าทายต่างๆ ที่กิจการเผชิญอยู่ ตลอดจนสอดรับกับสภาพแวดล้อมทางธุรกิจที่เปลี่ยนแปลงไปอย่างรวดเร็วหรือไม่ อย่างไร

1.4.2.2 นำเสนอร่างแผนกลยุทธ์ที่เหมาะสม ควบคู่กับการประเมินความเสี่ยงระดับกลยุทธ์

1.4.2.3 ระบุวิธีจัดการความเสี่ยงว่าสามารถทำได้หรือไม่ อย่างไร

1.4.2.4 พิจารณาว่ามีความจำเป็นต้องปรับโครงสร้าง หรือแผนการดำเนินงานภายในองค์กรเพื่อให้สอดรับกับกลยุทธ์นั้นหรือไม่ อย่างไร

1.4.2.5 พิจารณาว่าการดำเนินงานตามกลยุทธ์ที่นำเสนอมานั้น มีแนวโน้มที่จะเกิดความเสี่ยงจากการไม่ปฏิบัติตามกฎระเบียบ / ข้อบังคับหรือไม่

1.4.3 คณะกรรมการควรพิจารณาและคำนึงถึงการบูรณาการ GRC ในกิจกรรมต่างๆ ดังนี้

1.4.3.1 <u>การพัฒนากลยุทธ์</u>: คณะกรรมการทำหน้าที่อนุมัติกลยุทธ์ที่ฝ่ายจัดการนำเสนอ ดังนั้นเมื่อฝ่ายจัดการมีการนำเสนอทิศทาง เป้าหมายและกลยุทธ์ใหม่ คณะกรรมการควรพิจารณาให้ฝ่ายจัดการนำเสนอข้อมูลเชิงบูรณาการ ทั้งในแง่ทิศทางกลยุทธ์ใหม่ ความเหมาะสมเมื่อประเมินถึงความเสี่ยงและแนวทางการควบคุมความเสี่ยงของฝ่ายจัดการ ความพร้อมและโครงสร้างการทำงานที่รองรับทิศทางกลยุทธ์ใหม่ ตลอดจนแนวโน้มความเสี่ยงทางด้านการปฏิบัติตามกฎ ระเบียบและข้อบังคับ โดยการปฏิบัติทั้งหมดนี้จะต้องเชื่อมโยงเป็นระบบไม่ซับซ้อนและเป็นไปในทิศทางเดียวกัน

1.4.3.2 <u>การดำเนินงานตามกลยุทธ์</u>: จากทิศทางและกลยุทธ์ที่คณะกรรมการได้อนุมัติให้ฝ่ายจัดการไว้ฝ่ายจัดการจะต้องนำเสนอแผนการดำเนินงานที่สอดรับกับทิศทางกลยุทธ์ดังกล่าวเพื่อให้คณะกรรมการพิจารณา โดยเฉพาะอย่างยิ่งแผนการลงทุนหรือการทำรายการที่มีสาระสำคัญดังนั้น คณะกรรมการจึงควรติดตามดูแลให้มั่นใจว่าแผนการดำเนินงานนั้นสอดรับกับทิศทางกลยุทธ์ที่วางไว้ บริษัทมีระบบบริหารความเสี่ยงและระบบการติดตามให้มีการปฏิบัติตามกฎเกณฑ์ (Compliance) รวมถึงการควบคุมภายในที่ดี มีข้อมูล บุคลากร และเทคโนโลยีที่มีคุณภาพ สามารถสนับสนุนการตัดสินใจได้อย่างทันเวลา กล่าวโดยสรุปคือ คณะกรรมการจะต้องติดตามดูแลว่าหลักการ GRC ที่กำหนดไว้มีความเหมาะสมและสามารถช่วยทำให้การดำเนินงานนั้นเป็นไปอย่างมีประสิทธิภาพอย่างแท้จริง หากมีส่วนใดที่ยังไม่เหมาะสมจะต้องติดตามและกำชับให้ฝ่ายจัดการมีการจัดการต่อไป

1.4.3.3 <u>การติดตามผลการดำเนินงานตามกลยุทธ์</u>: คณะกรรมการจะต้องมีการวางกระบวนการให้ฝ่ายจัดการมีการรายงานภาพรวมของการดำเนินงานอยู่เป็นระยะ เพื่อให้มั่นใจถึงความมีประสิทธิภาพของกระบวนการดำเนินงานตามหลักการ GRC

1.4.4 อย่างไรก็ตาม การที่คณะกรรมการจะสามารถทำหน้าที่กำกับดูแลและติดตามได้ คณะกรรมการเองควรมีความเข้าใจเรื่อง GRC อย่างถ่องแท้ ตลอดจนมีความพร้อมเพื่อที่จะสามารถให้แนวทางที่ถูกต้องแก่ฝ่ายจัดการได้ โดยคณะกรรมการสามารถสร้างความพร้อมหรือเตรียมตัวในเรื่อง GRC ได้ด้วยวิธีการดังต่อไปนี้

1.4.4.1 องค์ประกอบของคณะกรรมการ (Board Composition):

1.4.4.1.1 คณะกรรมการควรดูแลให้มีองค์ประกอบคณะกรรมการที่เหมาะสม โดยนอกจากการสรรหาบุคคลที่มีความเชี่ยวชาญและประสบการณ์ที่หลากหลายแล้วกรรมการทุกท่านยังควรต้องมีความเข้าใจในบริบทขององค์กรอย่างถ่องแท้ตลอดจนเห็นถึงความเชื่อมโยงของกระบวนการทาง

ธุรกิจในองค์รวม เพื่อที่จะสามารถทำหน้าที่กำกับดูแล และให้แนวทางในการพัฒนาระบบ GRC แก่ฝ่ายจัดการได้อย่างเหมาะสม

1.4.4.1.2 องค์ประกอบของคณะกรรมการที่เหมาะสมดังกล่าวย่อมเอื้อให้เกิดการหารือเพื่อแลกเปลี่ยนเรียนรู้ ประสานความคิด และสร้างมุมมองที่สมดุล ระหว่างกรรมการที่มีความเชี่ยวชาญด้านกลยุทธ์ (Strategy Expertise) กรรมการที่มีความเชี่ยวชาญด้านการบริหารความเสี่ยง (Risk Expertise) รวมถึงกรรมการที่มีความรู้เฉพาะทางเกี่ยวกับกฎเกณฑ์ที่เกี่ยวข้อง (Compliance Expertise) อันส่งผลให้การตัดสินใจของคณะกรรมการเป็นไปอย่างมีประสิทธิภาพ

1.4.4.2 ภาวะผู้นำของคณะกรรมการ (Board Leadership):คณะกรรมการต้องมีความเป็นผู้นำ เพื่อที่จะสามารถร่วมกำหนดหรือทบทวนทิศทางการดำเนินกลยุทธ์ ตลอดจนแผนงานต่างๆ ร่วมกับฝ่ายจัดการได้ โดยคณะกรรมการจำเป็นจะต้องเข้าใจเรื่องต่างๆ ดังนี้

1.4.4.2.1 คณะกรรมการควรเข้าใจถึง “เงื่อนไขความยั่งยืนขององค์กร” กล่าวคือการที่องค์กรจะสามารถเติบโตอย่างยั่งยืนได้ จำเป็นต้องคำนึงถึงปัจจัยอะไรบ้างเป็นสำคัญโดยนอกเหนือไปจากปัจจัยภายนอกต่างๆ ที่อาจเข้ามากระทบกับการดำเนินงานขององค์กร (Disruption issues) แล้ว อีกประเด็นที่ควรคำนึงถึงคือ ความคาดหวังของผู้มีส่วนได้ส่วนเสีย (Stakeholder concerns) ซึ่งถือเป็นเรื่องที่ส่งผลกระทบต่อการดำเนินธุรกิจขององค์กรโดยตรง

1.4.4.2.2 ซึ่งการเข้าใจในเรื่องเหล่านี้ จะทำให้คณะกรรมการสามารถทำหน้าที่ตัดสินใจและกำกับดูแลการดำเนินงานตามหลัก GRC ได้มีประสิทธิภาพมากขึ้น ทั้งในแง่การพิจารณาทิศทางและเป้าหมายองค์กร การกำหนดทิศทางกลยุทธ์ การประเมินและบริหารจัดการความเสี่ยงที่ตรงกับบริบทขององค์กร ตลอดจนประเด็นเรื่องกฎระเบียบและข้อบังคับต่างๆ ที่เกี่ยวข้อง

1.4.4.2.3 การที่คณะกรรมการจะเข้าใจเรื่องเหล่านี้ได้ คณะกรรมการจำเป็นที่จะต้องมีการเข้าถึงกลุ่มผู้มีส่วนได้ส่วนเสียที่สำคัญอย่างเหมาะสม มีการรับรายงานจากฝ่ายจัดการเกี่ยวกับประเด็นความยั่งยืนและแนวทางการบริหารจัดการประเด็นดังกล่าว และคอยติดตามกระแสและสถานการณ์ต่างๆ ที่เกิดขึ้นรอบตัวที่อาจจะเป็นประโยชน์หรือส่งผลกระทบต่อองค์กรได้

1.4.4.2.4 คณะกรรมการต้องเข้าใจสภาพแวดล้อม บริบท และลักษณะการประกอบธุรกิจขององค์กร โดยศึกษาผ่านวิธีการต่างๆ เช่น การขอข้อมูลฝ่ายจัดการเพื่อทำความเข้าใจ การหารือหรือประชุมกับฝ่ายจัดการในเรื่องธุรกิจ การขวนขวายหาความรู้เพิ่มเติมจากการเข้าอบรมสัมมนา เป็นต้น

1.4.4.2.5 ข้อมูลเหล่านี้ถือเป็นข้อมูลพื้นฐานสำคัญที่กรรมการพึงทราบทั้งในช่วงก่อนที่จะรับตำแหน่ง และระหว่างที่ดำรงตำแหน่ง เนื่องด้วยสถานการณ์แวดล้อมทางธุรกิจเปลี่ยนแปลงตลอดเวลา กรรมการจึงจำเป็นต้องรับทราบข้อมูลเพิ่มเติมตามไปด้วย

1.4.4.2.6 คณะกรรมการควรเข้าใจถึงความเสี่ยงสำคัญขององค์กร ตลอดจนหลักการบริหารจัดการความเสี่ยงขององค์กร ทั้งความเสี่ยงทางด้านกลยุทธ์ (Strategic Risk) ความเสี่ยงด้านการเงิน (Financial Risk) ความเสี่ยงด้านการปฏิบัติการ (Operational Risk) และความเสี่ยงด้านการปฏิบัติตามกฎ ระเบียบและข้อบังคับ(Compliance Risk) เป็นต้น โดยต้องจัดให้มีการรายงานจากฝ่ายจัดการอยู่เป็นประจำ เพื่อนำ ข้อมูลเหล่านั้นมาใช้ในการกำ กับดูแลฝ่ายจัดการต่อไป

1.4.4.3 การทำหน้าที่สอดส่องดูแลของคณะกรรมการ (Board Oversight) : คณะกรรมการบริษัทไม่เพียงแต่จะทำหน้าที่ตัดสินใจร่วมกับฝ่ายจัดการในทิศทางและแผนการดำเนินงานต่างๆ ตามหลัก GRC เท่านั้น แต่ต้องทำหน้าที่กำกับดูแลและติดตามดูแลอย่างต่อเนื่อง ดังนั้น เพื่อให้กรรมการมีความพร้อมและสามารถทำหน้าที่กำกับดูแลได้อย่างเต็มที่ คณะกรรมการควรจัดให้มีการกำหนดเป็นกรอบการดำเนินงานตามหลัก GRC ขึ้นมาอย่างชัดเจนเพื่อใช้ในการดำเนินการและติดตามดูแลการนำไปปฏิบัติของฝ่ายจัดการ และคอยให้คำแนะนำแก่ฝ่ายจัดการเพื่อให้การดำเนินการตามหลัก GRC นั้นมีประสิทธิภาพมากขึ้น โดยกรอบ GRC ที่คณะกรรมการต้องจัดให้มีขึ้น มีดังนี้

1.4.4.3.1 การดำเนินธุรกิจจะต้องมีการประเมินบริบทและสภาพแวดล้อม (Landscape and environment) อยู่เสมอว่ามีการเปลี่ยนแปลงหรือไม่ และหากมีการเปลี่ยนแปลงเกิดขึ้น สิ่งนั้นจะส่งผลกระทบทางใดต่อแผนการดำเนินงานขององค์กร ดังนั้น คณะกรรมการควรสอบถามและติดตามให้ฝ่ายจัดการมีการพิจารณาและคำนึงถึงสภาพแวดล้อมทางธุรกิจ และมีการนำ เสนอข้อมูลส่วนนี้เมื่อมีการนำเสนอทิศทาง แผนกลยุทธ์ และแผนการดำเนินงาน ตลอดจนการรายงานความคืบหน้าการดำเนินการตามแผน เพื่อให้มั่นใจว่าสิ่งต่างๆ ที่ฝ่ายจัดการนำเสนอหรือดำเนินการอยู่นั้นยังสอดรับกับสภาพแวดล้อมทางธุรกิจ

1.4.4.3.2 คณะกรรมการพึงตระหนักว่า บริบทและสภาพแวดล้อมทางธุรกิจที่เปลี่ยนแปลงไปอย่างรวดเร็วในปัจจุบัน อาจนำมาซึ่ง “ความเสี่ยงอุบัติใหม่” (Emerging Risk) ซึ่งเป็นความเสี่ยงที่ไม่เคยเกิดขึ้นมาก่อน มีความไม่แน่นอนสูง และคาดการณ์ระดับความรุนแรงได้ยากจนอาจทำให้ฝ่ายจัดการมองข้ามความเสี่ยงเหล่านี้ไปดังนั้น คณะกรรมการจึงควรดูแลให้มั่นใจว่ากระบวนการวางแผนเชิงกลยุทธ์ (ซึ่งต้องดำ เนินควบคู่ไปกับกระบวนการบริหารความเสี่ยง) ได้พิจารณาครอบคลุมไปถึงความเสี่ยงอุบัติใหม่เหล่านี้ด้วย

1.4.4.3.3 คณะกรรมการควรกำกับดูแลฝ่ายจัดการ ไม่ว่าจะเป็นตอนที่ฝ่ายจัดการนำเสนอทิศทาง แผนกลยุทธ์ แผนการดำ เนินงาน หรือตอนที่นำเสนอถึงความคืบหน้าของการดำเนินการตามแผน ว่าให้มีการคำนึงถึงและนำเสนอรายงานต่อคณะกรรมการถึงความเหมาะสมขององค์ประกอบต่างเหล่านี้ร่วมด้วย อันได้แก่ โครงสร้างและการกำกับดูแลองค์กร (Governance) การบริหารความเสี่ยงที่อาจเกิดขึ้นและการควบคุม (Risk and Control Continuum) การปฏิบัติงานที่เป็นไปตามกฎ ระเบียบและข้อบังคับ (Compliance) โครงสร้างหรือแนวทางการสร้างความเชื่อมั่น (Assurance) ว่าแผนการดำเนินงานมีการปฏิบัติตามและดำเนินการอย่างถูกต้อง วัฒนธรรมและพฤติกรรมที่พึงประสงค์ (Culture, behavior and change) ตลอดจนแหล่งข้อมูลและความรู้ (Knowledge and data) ที่เข้าถึงได้และสนับสนุนการดำเนินงานตามหลัก GRC

1.4.4.3.4 อย่างไรก็ตาม การดำเนินงานตามข้างต้นอาจต้องปรับเปลี่ยนไปตามระดับการเติบโตของธุรกิจ การสอดรับกับแนวทางดำเนินงานและสภาพแวดล้อม และต้องเป็นไปในลักษณะบูรณาการเข้าหากัน (Business maturity, relevance ,integration and convergence) โดยไม่สามารถพิจารณาแยกจากกันเป็นส่วนๆ ได้ดังนั้น คณะกรรมการควรกำกับดูแลให้ฝ่ายจัดการมีการนำเสนอข้อมูลเหล่านี้ในเชิงบูรณาการ และคำนึงถึงสภาพแวดล้อมและระดับการเติบโตของบริษัทร่วมด้วย

1.4.4.3.5 องค์ประกอบสุดท้ายที่สำคัญ คือ ผู้นำอย่างคณะกรรมการร่วมกับฝ่ายจัดการจะต้องทำหน้าที่เป็นผู้นำ ในการขับเคลื่อนเรื่องเหล่านี้ให้เกิดขึ้น ต้องรับผิดชอบต่อผลลัพธ์ต่างๆ ที่

อาจเกิดขึ้น โดยต้องติดตามดูแลอย่างใกล้ชิดเพื่อให้เกิดความเชื่อมั่นในประสิทธิภาพของการดำเนินงาน (Leadership, accountability and assurance)

ภาพที่ 1: กรอบการดำเนินงานตามหลัก GRC

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

2.1 GRC Building Blocks

GRC Building Blocks ประกอบด้วย 3 องค์ประกอบสำคัญคือ การกำ กับดูแลกิจการ การบริหารความเสี่ยง และการกำ กับการปฏิบัติตามกฎ ระเบียบ และข้อบังคับ โดยหลักการทั่วไปที่คณะกรรมการควรพิจารณาเกี่ยวกับการบูรณาการเรื่อง GRC เข้ากับการดำ เนินงานขององค์กร มีดังนี้

2.1.1 GRC ที่ดีต้องเชื่อมโยงการกำ กับดูแลกิจการ (Governance) การบริหารความเสี่ยง (Risk) และการปฏิบัติตามกฎ ระเบียบและข้อบังคับ (Compliance) อย่างมีประสิทธิภาพและประสิทธิผล โดยเริ่มจากการที่ฝ่ายจัดการนำเสนอทิศทาง แผนกลยุทธ์ แผนการดำเนินงาน หรือรายงานผลความคืบหน้าของแผนการดำเนินงาน พร้อมกับผลการประเมินความเสี่ยงและวิธีจัดการความเสี่ยงนั้น ๆ ให้กับคณะกรรมการบริษัท

2.1.2 เมื่อคณะกรรมการบริษัทพิจารณาแล้วเห็นว่าข้อมูลที่ฝ่ายจัดการนำ เสนอมานั้นมีความเหมาะสมและอยู่ในระดับความเสี่ยงที่บริษัทยอมรับได้ (Risk Appetite) ประกอบกับแนวทางการกำกับดูแลกิจการในปัจจุบันยังมีความเหมาะสมอยู่ ก็จะทำการอนุมัติแผนกลยุทธ์หรือแผนการดำเนินงานนั้นให้ฝ่ายจัดการนำไปใช้พัฒนาหรือปฏิบัติต่อไป หรือหากเป็นกรณีการรายงานความคืบหน้าคณะกรรมการก็จะรับทราบผลการดำเนินงานและให้ฝ่ายจัดการดำ เนินการตามแผนต่อไปได้

2.1.3 ในส่วนการกำกับการปฏิบัติตามกฎ ระเบียบ และข้อบังคับ (Compliance) คณะกรรมการควรกำ กับให้ฝ่ายจัดการดำเนินการไปพร้อมกับการบริหารความเสี่ยงโดยทั่วไป โดยควรมีการประเมินความเสี่ยงด้านการปฏิบัติตามกฎ ระเบียบ และข้อบังคับ (Compliance Risk) มีการสอบทาน และการรายงานผลการปฏิบัติไปยังคณะกรรมการบริษัทอย่างสม่ำเสมอเช่นกัน

2.1.4 คณะกรรมการควรกำ กับดูแลให้มั่นใจว่า ฝ่ายจัดการได้จัดให้มีการสอบทานประสิทธิภาพและประสิทธิผลของ GRC Building Blocks อย่างสม่ำเสมอโดยผู้ตรวจสอบภายใน และรายงานผลการสอบทานให้คณะกรรมการบริษัททราบ โดยคณะกรรมการบริษัทควรแนะนำ ฝ่ายจัดการให้ปรับปรุง GRC Building Blocks ได้ เมื่อเห็นถึงจุดบกพร่องที่ต้องปรับปรุง หรือเมื่อพิจารณาเห็นว่ากลยุทธ์ สภาพแวดล้อมการดำเนินธุรกิจ ขนาดบริษัท หรือความคาดหวังของผู้มีส่วนได้ส่วนเสียได้เปลี่ยนแปลงไป

2.2 การกำ กับดูแลกิจการ (Governance)

หากพิจารณาเฉพาะในส่วนของการกำ กับดูแลกิจการ คณะกรรมการจะต้องกำ กับดูแลว่าทิศทาง แผนกลยุทธ์ แผนการดำเนินงานที่ฝ่ายจัดการนำเสนอ หรือดำเนินการอยู่นั้น สอดรับกับโครงสร้างการกำกับดูแลภายในองค์กร ตลอดจนนโยบายการดำเนินงานต่างๆ ที่สำคัญขององค์กรหรือไม่ โดยคณะกรรมการจะต้องพิจารณาในเรื่องต่างๆ ดังนี้

2.2.1 ทิศทางแผนกลยุทธ์ แผนการดำเนินงานที่ฝ่ายจัดการนำเสนอ สอดรับกับเป้าหมาย พันธกิจและวิสัยทัศน์ขององค์กร (Alignment with purpose, mission and vision) หรือไม่ หรือแม้แต่แผนที่ได้รับการอนุมัติไปแล้วและกำลังดำเนินการอยู่นั้น ยังสอดรับกับเป้าหมาย ทิศทางในปัจจุบันอยู่หรือไม่

2.2.2 โครงสร้างองค์กร (Organizational structure) ในปัจจุบันยังสามารถรองรับทิศทางกลยุทธ์ และแผนการดำเนินงานขององค์กรหรือไม่จำเป็นต้องมีการปรับเปลี่ยน ปรับขนาดโครงสร้างองค์กรหรือไม่

2.2.3 ทิศทาง กลยุทธ์และแผนการดำเนินงานนั้นมีความสอดคล้องกับวัฒนธรรมขององค์กร (Organizational Culture) หรือไม่ เช่น วัฒนธรรมที่ไม่กล้าเสี่ยง หรือวัฒนธรรมที่ชอบความเสี่ยง หากเป็นกรณีที่ไม่มีความสอดคล้อง ฝ่ายจัดการมีแนวทางจัดการอย่างไร เช่น การจัดตั้งหน่วยงานที่จะดำเนินการตามแผนกลยุทธ์ใหม่แยกจากโครงสร้างการทำ งานโดยปกติ เพื่อการตัดสินใจและมีแนวทางทำงานที่รวดเร็วและยืดหยุ่นมากขึ้น

2.2.4 นโยบาย (Related policies) ที่องค์กรมีในปัจจุบันเอื้อให้สามารถดำ เนินการตามทิศทางกลยุทธ์และแผนการดำเนินงานหรือไม่ หากนโยบายที่มีอยู่ไปจำกัดการดำเนินงาน ฝ่ายจัดการมีแนวทางจัดการอย่างไร เช่น ไม่ดำเนินการตามแผนเนื่องจากขัดกับนโยบายของบริษัท หรือจะมีการปรับเปลี่ยนนโยบายเพื่อเอื้อให้เกิดการดำเนินการได้อย่างเหมาะสม

2.2.5 การปฏิบัติงานตามทิศทาง กลยุทธ์และแผนการดำเนินงานนั้น มีการมอบหมายหน้าที่ในการดำเนินการ (Delegation of authorities) อย่างเหมาะสมหรือไม่

2.2.6 การดำเนินการตามทิศทาง กลยุทธ์และแผนการดำเนินงานดังกล่าวมีการกำหนดตัวชี้วัด (Performance metrics) ใดบ้าง เหมาะสมหรือไม่ทั้งในแง่ของผลสัมฤทธิ์ที่คาดหวัง และในแง่ที่มีผลต่อวัฒนธรรมและพฤติกรรมของคนในองค์กร

ในระหว่างการดำเนินงานตามแผนกลยุทธ์ที่คณะกรรมการบริษัทอนุมัติแล้ว ฝ่ายจัดการควรประเมินความเสี่ยงระดับองค์กร หน่วยงาน และกระบวนการ และรายงานความเสี่ยงที่สำคัญพร้อมทั้งวิธีจัดการความเสี่ยงนั้นให้คณะกรรมการบริษัททราบอย่างสม่ำเสมอหรืออย่างน้อยทุกไตรมาส เมื่อคณะกรรมการบริษัทได้รับรายงานแล้ว ควรพิจารณาความถูกต้องและครบถ้วนของความเสี่ยง ความเหมาะสมของวิธีจัดการความเสี่ยง และให้ความเห็นหรือข้อแนะนำ เกี่ยวกับความเสี่ยง วิธีจัดการความ

เสี่ยง หรืออาจเป็นข้อแนะนำ ในการปรับปรุงแผนกลยุทธ์ให้เหมาะสมกับเหตุการณ์ความเสี่ยง ในการพิจารณาข้อมูลทั้งหมดที่กล่าวมานี้ คณะกรรมการบริษัทและฝ่ายจัดการอาจเห็นโอกาสในการสร้างมูลค่าเพิ่มให้แก่ธุรกิจได้ เช่น กรณีที่บริษัทมีความเสี่ยงต่ำด้านเงินทุนและบุคลากร จึงทำให้เพิ่มโอกาสในการนำเทคโนโลยีแบบใหม่มาใช้ในธุรกิจได้

2.3 การบริหารความเสี่ยง (Risk Management)

องค์ประกอบสำคัญของการบริหารความเสี่ยงที่คณะกรรมการบริษัทควรกำกับดูแล เมื่อฝ่ายจัดการนำเสนอเป้าหมาย ทิศทางกลยุทธ์องค์กร หรือการตัดสินใจดำ เนินการในเรื่องสำคัญ หรือแม้แต่ในขั้นตอนของการติดตามผลการดำ เนินงาน มีดังนี้

2.3.1 การดำเนินการดังกล่าวมีความสอดคล้องหรืออยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)หรือไม่ หากมีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ฝ่ายจัดการจะดำเนินการอย่างไร ควรหยุดที่จะดำเนินการต่อหรือมีการพิจารณาทบทวนระดับความเสี่ยงที่ยอมรับได้ใหม่ เป็นต้น

2.3.2 ความเสี่ยงที่สำคัญที่เกิดจากการดำ เนินการตามทิศทาง กลยุทธ์และแผนการดำเนินงาน ได้ถูกระบุ และประเมินจัดลำ ดับความสำคัญ (Risk Identification and Assessment) หรือไม่ ความเสี่ยงที่สำคัญของบริษัทนั้นมีเปลี่ยนแปลงไปตามสถานการณ์ เวลาและระยะเวลาการเติบโตของธุรกิจหรือไม่

2.3.3 บริษัทมีแนวทางจัดการความเสี่ยง (Risk Treatment) เหล่านั้นอย่างไร เช่น ทำให้ความรุนแรงลดลง (Reduce) ยอมรับโดยไม่ทำอะไรเพิ่มเติม (Accept) หาผู้ร่วมรับความเสี่ยง (Transfer) หลีกเลี่ยงความเสี่ยงนั้นโดยการทบทวนเป้าหมายหรือกลยุทธ์ใหม่ (Avoid) หรือยอมรับการมีความเสี่ยงเพื่อทำให้บริษัทเติบโตต่อไป (Pursue)

2.3.4 จัดให้มีการรายงานความเสี่ยง (Risk Report) ที่สำคัญพร้อมทั้งวิธีจัดการความเสี่ยงนั้นให้คณะกรรมการบริษัททราบอย่างสม่ำเสมอหรืออย่างน้อยทุกไตรมาส เมื่อคณะกรรมการบริษัทได้รับรายงานแล้วควรพิจารณาความถูกต้องและครบถ้วนของความเสี่ยง ความเหมาะสมของวิธีจัดการความเสี่ยงและให้ความเห็นหรือข้อแนะนำ เกี่ยวกับความเสี่ยงและวิธีจัดการความเสี่ยงที่มีประสิทธิภาพมากขึ้น หรืออาจเป็นข้อแนะนำ ในการปรับปรุงแผนกลยุทธ์ให้เหมาะสมกับความเสี่ยงที่ประเมินได้

เมื่อคณะกรรมการบริษัทอนุมัติแผนกลยุทธ์แล้ว ฝ่ายจัดการควรจัดให้มีการประเมินความเสี่ยงระดับองค์กร (Corporate Risk) ซึ่งแสดงความเสี่ยงสำคัญทั้งหมดของบริษัท และความเสี่ยงระดับหน่วยงาน (Business Unit Risk) ซึ่งแสดงความเสี่ยงสำคัญของแต่ละหน่วยงาน โดยความเสี่ยงเหล่านี้จะเกี่ยวข้องกับการดำเนินงานแต่ละวันทั้งด้านการดำเนินงาน (Operational Risk) การเงิน (Financial Risk) และการปฏิบัติตามกฎเกณฑ์ (Compliance Risk) ทั้งนี้ ฝ่ายจัดการสามารถประเมินความเสี่ยงจากระดับองค์กรไปยังหน่วยงาน หรือนำความเสี่ยงสำคัญจากระดับหน่วยงานขึ้นมาเป็นของระดับองค์กรได้ แต่การทำในลักษณะทั้งสองทางนี้ ต้องมั่นใจว่าความเสี่ยงทั้งสองระดับนั้นเป็นไปในทิศทางเดียวกัน คือมุ่งสู่ความสำเร็จในการบรรลุกลยุทธ์และวัตถุประสงค์ของบริษัท ในระหว่างการดำ เนินงานตามแผนกลยุทธ์ที่ได้รับการอนุมัติจากคณะกรรมการ คณะกรรมการควรกำ กับดูแลให้ฝ่ายจัดการทบทวนและประเมินความเสี่ยงด้านกลยุทธ์ร่วมด้วย โดยเฉพาะอย่างยิ่งในกรณีที่เห็นว่ามีความเสี่ยงที่อาจส่งผลกระทบกับแผนกลยุทธ์โดยตรง เช่น การมีโรคระบาดรุนแรงแบบ Covid-19 เกิดขึ้น ทำให้บริษัทไม่สามารถดำเนินธุรกิจแบบเดิมได้ และคาดว่าผลกระทบจะรุนแรงมากขึ้น จึงต้องหาวิธีลดความเสี่ยงโดย

การปรับแผนกลยุทธ์ไปสู่รูปแบบใหม่ เช่น ทำธุรกิจแบบ On-line มากขึ้น เป็นต้น ทั้งนี้ หากฝ่ายจัดการพบว่ามีความเสี่ยงที่อาจกระทบกับแผนกลยุทธ์ ฝ่ายจัดการต้องรายงานให้คณะกรรมการบริษัททราบ เพื่อหารือเกี่ยวกับการปรับปรุงแผนกลยุทธ์ให้มีความเหมาะสม

2.4 การกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance)

คณะกรรมการบริษัทควรกำกับดูแลให้มั่นใจว่าบริษัทเข้าใจและสามารถปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับต่างๆ ได้อย่างถูกต้องและครบถ้วน การปฏิบัติตามกฎเกณฑ์ให้ครบถ้วนและถูกต้องนี้ถือเป็นวัตถุประสงค์หนึ่งของบริษัท ดังนั้น ฝ่ายจัดการจะต้องประเมินความเสี่ยงด้าน Compliance และกำหนดวิธีจัดการเพื่อลดความเสี่ยงดังกล่าว รวมทั้งรายงานผลให้คณะกรรมการบริษัททราบอย่างสม่ำเสมอทั้งนี้ ในส่วนของการกำกับดูแลด้าน Compliance คณะกรรมการบริษัทควรพิจารณาเรื่องสำคัญดังต่อไปนี้เมื่อฝ่ายจัดการนำ เสนอเป้าหมาย ทิศทางกลยุทธ์องค์กร หรือเรื่องสำคัญอื่นๆ ให้กับคณะกรรมการพิจารณา

2.4.1 ประเด็นทางกฎหมาย จริยธรรม หรือ เรื่องที่มีผลกระทบทางลบต่อผู้มีส่วนได้ส่วนเสียที่อาจเกิดขึ้นได้พร้อมแนวทางการบริหารจัดการ (Laws, Ethics and Stakeholder Concerns)

2.4.2 มีความสอดคล้องหรือเป็นไปตามมาตรฐานอุตสาหกรรมหรือแนวปฏิบัติที่ดี (Standard or Best Practices) ที่เกี่ยวข้องหรือไม่

2.4.3 มีแนวทางการตรวจสอบ (Audit) เพื่อให้เกิดความมั่นใจว่ามีการปฏิบัติตามกฎ ระเบียบและข้อบังคับอย่างไร

2.4.4 มีกระบวนการรายงาน (Reporting Procedure) ต่อคณะกรรมการ และผู้มีส่วนได้ส่วนเสีย (Stakeholders) ที่สำคัญขององค์กรอย่างไร

แนวปฏิบัติ 3 การพิจารณาแต่งตั้งคณะกรรมการชุดย่อย

3.1 คณะกรรมการบริษัทมีหน้าที่กำกับดูแล GRC ซึ่งประกอบด้วย ระบบการกำกับดูแลกิจการ การบริหารความเสี่ยงและการควบคุมภายใน และการปฏิบัติตามกฎเกณฑ์ ซึ่งถือว่าเป็นภาระความรับผิดชอบที่สูง ดังนั้น ในทางปฏิบัติ คณะกรรมการส่วนใหญ่จึงมักแต่งตั้งคณะกรรมการชุดย่อยต่างๆ เพื่อเข้ามาช่วยสนับสนุนการทำ หน้าที่ของกรรมการ

3.2 โดยทั่วไป คณะกรรมการชุดย่อยที่คณะกรรมการแต่งตั้งหรือมอบหมายเพื่อมาติดตามดูแลเรื่อง GRC ประกอบด้วยคณะกรรมการด้านกำกับดูแลกิจการ (Corporate Governance Committee) ในส่วนงานด้านการกำกับดูแลกิจการ คณะกรรมการตรวจสอบ (Audit Committee) ในส่วนงานกำกับดูแลให้มีการปฏิบัติตามกฎ ระเบียบและข้อบังคับ หรือบางองค์กรอาจพิจารณาแต่งตั้งคณะกรรมการชุดย่อยด้านกำกับการปฏิบัติตามกฎ ระเบียบ และข้อบังคับ (Compliance Committee) ขึ้นมาโดยเฉพาะก็ได้ โดยพิจารณาตามความเหมาะสมของบริบทธุรกิจองค์กร และคณะกรรมการการบริหารความเสี่ยงและการควบคุมภายใน (Risk Committee) เพื่อช่วยกำกับดูแลงานด้านการบริหารความเสี่ยงและการควบคุมภายใน

3.3 โดยปกติ บริษัทจดทะเบียนจะถูกกำหนดให้มีการจัดตั้งคณะกรรมการตรวจสอบ เพื่อช่วยคณะกรรมการบริษัทกำกับดูแลการจัดทำรายงานทางการเงิน การกำกับดูแลกิจการ การบริหาร

ความเสี่ยงและการควบคุมภายใน ในขณะที่การจัดตั้งคณะกรรมการชุดย่อยด้านอื่นๆ นั้น ขึ้นอยู่กับความเหมาะสมของแต่ละองค์กร โดยปัจจัยสำคัญในการพิจารณาคือการดูว่าคณะกรรมการบริษัทสามารถกำกับดูแลงานนั้นๆ ได้เองหรือไม่

3.4 อย่างไรก็ตาม แม้มีการแต่งตั้งคณะกรรมการชุดย่อยแล้ว คณะกรรมการบริษัทยังมีบทบาทหน้าที่และความรับผิดชอบต่อการกำกับดูแลงานทั้งหมด โดยไม่อาจมอบความรับผิดชอบดังกล่าวไปยังคณะกรรมการชุดย่อยเพียงลำพังได้ ดังนั้น คณะกรรมการบริษัทควรกำหนดให้คณะกรรมการชุดย่อยต่างๆ ต้องรายงานผลการปฏิบัติงานให้คณะกรรมการบริษัทรับทราบอย่างสม่ำเสมอหรืออย่างน้อยทุกไตรมาส

3.5 จากการที่การกำกับดูแลเรื่อง GRC เป็นการบูรณาการเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยงและการควบคุมภายใน และการปฏิบัติตามกฎ ระเบียบและข้อบังคับเข้าด้วยกัน ดังนั้น คณะกรรมการชุดย่อยต่างๆ ควรมีการทำ งานที่สอดประสานกัน และเห็นภาพไปในทิศทางเดียวกัน โดยคณะกรรมการบริษัทอาจพิจารณาให้มีการดำเนินการดังต่อไปนี้เพื่อเอื้อให้เกิดการบูรณาการในการทำงานระหว่างคณะกรรมการชุดย่อย

3.5.1 จัดให้มีการรายงานจากคณะกรรมการชุดย่อยต่อคณะกรรมการบริษัทเป็นระยะ เพื่อให้กรรมการทั้งหมดได้เห็นภาพของการดำเนินงานว่ามีความสอดคล้องและสอดประสานกันหรือไม่

3.5.2 จัดให้มีกรรมการที่นั่งอยู่ในคณะกรรมการชุดย่อยคาบเกี่ยวกันตามความเหมาะสม เพื่อเป็นตัวเชื่อมระหว่างคณะกรรมการชุดย่อย และดูถึงความสอดรับกันในส่วนงานที่แต่ละคณะกรรมการชุดย่อยต้องกำกับดูแล อย่างไรก็ตาม การพิจารณาในส่วนนี้ต้องคำนึงถึงปัจจัยสำคัญอื่นร่วมด้วย เช่น ทักษะ ความรู้ และประสบการณ์ในการทำ หน้าที่ในคณะกรรมการชุดย่อยนั้น

แนวปฏิบัติ 4 บทบาทหน้าที่ของคณะกรรมการชุดย่อยต่อ GRC

4.1 คณะอนุกรรมการกำกับดูแลกิจการ (Corporate Governance Committee) มีบทบาทหน้าที่ต่อไปนี้

4.1 คณะกรรมการกำกับดูแลกิจการมีบทบาทหน้าที่กำหนดกรอบการกำกับดูแลกิจการตามหลักการกำกับดูแลกิจการของตลาดหลักทรัพย์แห่งประเทศไทย และหลักการกำกับดูแลกิจการที่ดีสำหรับบริษัทจดทะเบียน (Corporate Governance Code) ของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ พร้อมทั้งติดตามการปฏิบัติให้สำเร็จตามกรอบเหล่านั้น

4.2 สร้างและส่งเสริมวัฒนธรรมที่ดีและจรรยาบรรณในบริษัทที่สนับสนุนให้บริษัทสามารถบรรลุตามกลยุทธ์และวัตถุประสงค์ที่กำ หนดไว้

4.3 พิจารณากรอบและแนวปฏิบัติ GRC ของบริษัทว่าได้รับการออกแบบและปฏิบัติอย่างเหมาะสมตั้งแต่ระดับคณะกรรมการบริษัท ฝ่ายจัดการ และพนักงานทุกคน

4.4 จัดแนวทางการประเมินการทำ งานของคณะกรรมการบริษัทและฝ่ายจัดการให้สอดรับกับกรอบและแนวปฏิบัติ GRC

)

4.2 คณะอนุกรรมการบริหารความเสี่ยง (Risk Committee) มีบทบาทหน้าที่ต่อไปนี้

4.2.1 กำกับดูแลให้มีการกำ หนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ขององค์กร เพื่อเป็นกรอบให้ฝ่ายจัดการใช้ในการพิจารณาดำเนินงาน

4.2.2 หารือกับฝ่ายจัดการเกี่ยวกับระดับความเสี่ยงที่ยอมรับได้อย่างสม่ำเสมอ โดยเฉพาะเมื่อสถานการณ์แวดล้อมเปลี่ยนแปลงหรือมีโอกาสใหม่ๆ เกิดขึ้น

4.2.3 กำกับดูแลให้ฝ่ายจัดการมีการวางกระบวนการบริหารจัดการความเสี่ยงที่ดี ซึ่งประกอบด้วยการระบุ ประเมิน จัดการ ติดตาม และรายงานความเสี่ยงที่สำคัญ รวมถึงมีการพิจารณาปรับปรุงระบบการบริหารความเสี่ยงอย่างต่อเนื่อง

4.2.4 ให้คำแนะนำ เกี่ยวกับความเสี่ยงสำคัญแก่ฝ่ายจัดการอย่างทันเวลา

4.2.5 กำกับดูแลการปฏิบัติและสอบทานผลการประเมินความเสี่ยงทุกด้าน (Enterprise-wide Risk Assessment) รวมถึงการบ่งชี้และรายงานความเสี่ยงที่สำคัญของบริษัท

4.2.6 ในกรณีที่กำกับดูแลการบริหารความเสี่ยงด้านที่มีความซับซ้อนและสำคัญ อาจพิจารณาสรรหากรรมการที่มีความรู้ความชำ นาญพิเศษในด้านนั้นๆ

4.2.7 สอดส่องพฤติกรรมที่ไม่เหมาะสมที่มีผลต่อประสิทธิภาพของระบบบริหารความเสี่ยง และทำให้บริษัทยอมรับความเสี่ยงที่มากเกินไป (Risk Taking) เช่น การกำ หนดผลตอบแทนที่ไม่เหมาะสมหรือสูงเกินไป อาจทำให้พนักงานยอมรับความเสี่ยงมากขึ้น เพื่อทำงานให้ถึงจุดที่จะได้รับผลตอบแทน เป็นต้น

4.3 คณะอนุกรรมการกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance Committee) มีบทบาทหน้าที่ต่อไปนี้

4.3.1 ติดตามและกำกับดูแลให้มั่นใจว่ากรรมการบริษัท ฝ่ายจัดการ และพนักงาน มีการปฏิบัติตามจรรยาบรรณกฎระเบียบ และข้อบังคับ ทั้งที่กำหนดจากภายในบริษัทและภายนอกบริษัท

4.3.2ดูแลให้มีการประเมินกฎ ระเบียบ และข้อบังคับที่อาจส่งผลกระทบต่อการดำ เนินธุรกิจขององค์กรได้ พร้อมทั้งมีการพิจารณาถึงความเพียงพอและความเหมาะสมของระบบการควบคุมภายในเพื่อป้องกันความเสี่ยงจากการไม่ปฏิบัติตามกฎ ระเบียบ และข้อบังคับ

4.3.3 กำ กับดูแลให้มั่นใจว่าประเด็นสำคัญที่ต้องปฏิบัติตามกฎ ระเบียบ และข้อบังคับต่างๆ ทั้งจากภายในและภายนอกบริษัท ได้ถูกนำไปบูรณาการอยู่ในทุกกระบวนการที่ปฏิบัติเป็นประจำวัน รวมถึงกำกับดูแลให้มีการจัดอบรม สื่อสาร และติดตามดูแลให้เกิดการปฏิบัติตามขั้นตอนและกระบวนการที่กำหนดไว้ด้วย

4.3.4 บริษัทที่มีขนาดกลางหรือขนาดเล็ก หรือมีบริบททางธุรกิจที่ไม่ได้เกี่ยวข้องกับกฎ ระเบียบและข้อบังคับที่มีความซับซ้อน อาจไม่ได้พิจารณาแต่งตั้งคณะกรรมการชุดย่อยนี้ คณะกรรมการอาจมอบหน้าที่นี้ให้คณะกรรมการชุดย่อยอื่นๆ เพื่อทำ หน้าที่แทนได้ เช่น คณะกรรมการกำกับดูแลกิจการ หรือคณะกรรมการตรวจสอบ เป็นต้น

4.4 คณะกรรมการตรวจสอบ (Audit Committee) มีบทบาทหน้าที่ต่อไปนี้

4.4.1 ทำหน้าที่สอบทานการกำ กับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบและข้อบังคับ และทำหน้าที่รับรายงานผลการสอบทานโดยตรงจากผู้ตรวจสอบภายในและผู้สอบบัญชี เพื่อให้มั่นใจว่าบริษัทได้จัดให้มีระบบการควบคุมภายในที่มี

ประสิทธิภาพ เพียงพอ และเหมาะสมต่อการปฏิบัติให้บรรลุตามวัตถุประสงค์ของเรื่องเหล่านี้ โดยสรุปแล้ว คณะกรรมการตรวจสอบถือว่ามีส่วนสำคัญ เพราะทำ หน้าที่ให้ความเชื่อมั่น (Assurance) ต่อการดำเนินงานของกิจการว่ามีความถูกต้อง โปร่งใส และสอบทานได้

4.4.2 ด้วยภาระหน้าที่ของคณะกรรมการตรวจสอบที่ต้องติดตามดูแลและสอบทานภาพรวมของการดำเนินงานขององค์กร คณะกรรมการบริษัทจึงมักมอบหมายให้คณะกรรมการตรวจสอบทำหน้าที่ติดตามดูแลในส่วนของการกำกับดูแลกิจการ การบริหารความเสี่ยง และการติดตามดูแลให้มีการปฏิบัติตามกฎ ระเบียบ และข้อบังคับร่วมด้วย โดยเฉพาะอย่างยิ่งในองค์กรที่มีขนาดกลางและขนาดเล็ก และองค์กรที่ไม่มีความซับซ้อนในการดำเนินธุรกิจ

ส่วนที่ 4

แผนงาน/โครงการ GRC

แผนปฏิบัติการด้านการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และควบคุมภายใน และการปฏิบัติตามกฎของ บอท.

องค์ประกอบที่ 1 : การกำกับดูแลที่ดีและการนำองค์กร

หลักเกณฑ์ : การกำกับดูแลกิจการที่ดี เป็นกลไกในการกำหนดวัตถุประสงค์ขององค์กร และกำหนดวิธีการที่จะระบุวัตถุประสงค์เหล่านั้น รวมถึงการติดตามผลการดำเนินงานขององค์กร

ที่	แผนงาน / โครงการ	น้ำหนัก	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
1	จัดให้มีคณะอนุกรรมการ คณะทำงาน หน่วยงาน/ผู้รับผิดชอบหลักในการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน และการกำกับดูแลการปฏิบัติงาน โดยมีการกำหนดบทบาท อำนาจหน้าที่ และกระบวนการทำงานที่ชัดเจนเป็นรูปธรรม	2	←	—	→									
2	กำหนดและสรรหาบุคลากรที่มีคุณสมบัติ และความรู้ความสามารถในการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน และการกำกับดูแลการปฏิบัติงาน	1	←	→										
3	จัดให้มีการบูรณาการการทำงานร่วมกันของคณะทำงาน คณะอนุกรรมการ หน่วยงาน/ผู้รับผิดชอบหลักระหว่างการดำเนินงานด้านการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน และการกำกับดูแลการปฏิบัติงาน	4				↔				↔				
4	กำหนดให้มีการติดตาม ประเมินผล การปฏิบัติงานอย่างต่อเนื่องและสม่ำเสมอ โดยให้มี	4			↔			↔			↔			↔

	การรายงานผลต่อคณะกรรมการบริษัทฯ คณะอนุกรรมการหรือผู้บริหารให้ทราบอย่างน้อยไตรมาสละ 1 ครั้ง เพื่อให้มั่นในได้ว่าการดำเนินงานด้านการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายในและการกำกับดูแลการปฏิบัติงาน มีความเพียงพอเหมาะสม และสามารถปฏิบัติได้จริงอย่างชัดเจน ตรวจพบปัญหาและอุปสรรคจะได้รับการปรับปรุงแก้ไขได้ทันเวลาและสอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป													
5	เสริมสร้างคุณธรรม จริยธรรม มีจรรยาบรรณต่อตนเอง องค์กรและผู้มีส่วนได้ส่วนเสีย โดยคำนึงถึงหลักในการกำกับดูแลกิจการที่ดี 7 ประการ	4	←	—	—	—	—	—	—	—	—	—	—	→
6	พัฒนาและปรับปรุงแนวทางการเสริมสร้างวัฒนธรรมองค์กรให้สอดคล้องกับแนวปฏิบัติการบูรณาการด้านการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติตามกฎหมาย กฎระเบียบข้อบังคับและมาตรฐานที่เกี่ยวข้อง GRC	3	←	—	—	—	—	—	—	—	—	—	—	→
7	กำหนดให้มีการสอบทานประสิทธิผลของกระบวนการด้านการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการ	2							←	—	→			
	ปฏิบัติตามกฎหมาย กฎระเบียบข้อบังคับและมาตรฐานที่เกี่ยวข้อง GRC และเสนอคณะกรรมการตรวจสอบเพื่อพิจารณา													
	รวม	**20**												

)

องค์ประกอบที่ 2 : การบริหารความเสี่ยงและการควบคุมภายใน (Risk Management & Internal Control)

หลักเกณฑ์ : หน่วยงานที่ทำหน้าที่ด้านการบริหารความเสี่ยงและการควบคุมภายในต้องเป็นผู้เชี่ยวชาญที่ไม่เพียงแต่บริหารจัดการความเสี่ยงที่ได้รับมอบหมาย และการกำหนดกิจกรรมการควบคุมของแผนงาน/โครงการ/กิจกรรม ตามแผนปฏิบัติการ

ที่	แผนงาน / โครงการ	น้ำหนัก	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
1	สร้างทัศนคติ พฤติกรรมและวัฒนธรรมด้านการบริหารความเสี่ยงของผู้จัดการ ผู้บริหาร พนักงานและลูกจ้าง ของ บอท.	2				←	—	→						
2	จัดให้มีการเผยแพร่ สื่อสาร ความรู้ความเข้าใจ สร้างความตระหนักและความสำคัญ เกี่ยวกับการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการปฏิบัติงาน	2				←	—	→						
3	วิเคราะห์ข้อมูลที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร เพื่อเป็นข้อมูลสำหรับการระบุปัจจัยเสี่ยงและสาเหตุความเสี่ยงบนฐานการวิเคราะห์ที่ประเมินรอบด้าน (Intelligence Risk)	2	←	—	→									
4	จัดให้มีระบบควบคุมภายในที่ดี เพื่อเป็นแนวทางในการดำเนินงานอย่างมีประสิทธิภาพและ ประสิทธิผล มีการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ นโยบาย ที่เกี่ยวข้อง สามารถลดหรือป้องกันความเสียหายที่จะเกิดขึ้นได้	2	←	—	→									
5	จัดให้มีการบริหารจัดการความเสี่ยงให้อยู่ในระดับที่คณะกรรมการ อนุกรรมการ และผู้บริหารยอมรับได้	2		↔			↔			↔			↔	
6	จัดให้มีกระบวนการสื่อสารและสร้างการมีส่วนร่วมในขั้นตอนการกำหนด/วิเคราะห์สร้างมูลค่า (Value Creation) และเพิ่มมูลค่า (Value Enhancement)	2	←	—	→									

)

7	จัดให้มีถ่ายทอดตัวชี้วัดระดับองค์กรสู่ระดับสายงาน โดยเฉพาะตัวชี้วัดการการบริหารความเสี่ยงและการควบคุมภายใน	1		←	→									
8	จัดให้มีการนำเทคโนโลยีสารสนเทศมาใช้เพื่อสนับสนุนการทำงานด้านการบริหารความเสี่ยงและการควบคุมภายใน เช่น การเตือนภัยความเสี่ยงองค์กร (Early Warning System : EWS)	2		↔			↔			↔			↔	
9	จัดให้มีบุคลากรหรือหน่วยงานที่มีความเป็นอิสระในการปฏิบัติหน้าที่เป็นผู้รับผิดชอบในการตรวจสอบระบบควบคุมภายใน	1	↔											
10	ทบทวนระบบควบคุมภายใน ที่สำคัญอย่างน้อยปีละ 1 ครั้ง	1											↔	→
11	จัดให้มีการสำรวจพฤติกรรม ทัศนคติ และความรู้ความเข้าใจของพนักงาน เกี่ยวกับการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติงาน และสรุปเสนอผู้บริหารในสายงานที่เกี่ยวข้อง	1										←	→	
12	จัดให้มีการติดตามความก้าวหน้าและจัดทำรายงานความก้าวหน้าของการบริหารความเสี่ยงและการควบคุมภายในทั้งในระดับองค์กรและระดับหน่วยงาน เพื่อเสนอต่อคณะอนุกรรมการบริหารความเสี่ยงและการควบคุมภายในของ บอท. อย่างน้อยไตรมาสละ 1 ครั้ง	2		↔			↔			↔			↔	
	รวม	**20**												

)

องค์ประกอบที่ 3 : การกำกับดูแลการปฏิบัติงาน (Compliance)

หลักเกณฑ์ : การกำกับดูแลการปฏิบัติงานทำหน้าที่ควบคุมเพื่อให้องค์กรบรรลุวัตถุประสงค์ผ่านการกำกับควบคุมดูแลให้บุคลากรขององค์กรปฏิบัติตามกฎหมาย กฎระเบียบ ข้อบังคับ คู่มือการปฏิบัติงาน เพื่อป้องกันความเสียหายที่ส่งผลกระทบต่อการดำเนินงาน

ที่	แผนงาน / โครงการ	น้ำหนัก	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
1	คณะกรรมการ ผู้บริหาร พนักงานและลูกจ้างของ บอท. จะต้องทำความเข้าใจในกฎหมาย กฎ ระเบียบ ข้อบังคับ ที่เกี่ยวข้องกับการปฏิบัติงานของตนเอง รวมทั้งศึกษาหน้าที่ความรับผิดชอบของตนตามบรรยายลักษณะงานในแต่ละตำแหน่ง	3				←	—	→						
2	กำหนดให้ทุกหน่วยงานมีส่วนร่วมในการศึกษาวิเคราะห์และทบทวนคำสั่ง กฎระเบียบ ข้อบังคับ คู่มือการปฏิบัติงาน เพื่อสนับสนุนการทำงานให้มีประสิทธิภาพ และให้มีการนำระเบียบข้อบังคับของ บอท. ไปใช้ประกอบการจัดทำแนวทางปฏิบัติงานหรือคู่มือปฏิบัติงานในด้านต่างๆ ของหน่วยงาน	3				←	—	→						
3	จัดให้มีการะบวนการสื่อสารคำสั่ง กฎระเบียบ ข้อบังคับของ บอท. ให้แก่ทุกหน่วยงานอย่างเป็นรูปธรรม	2				←	—	→						
4	ห้ามมิให้คณะกรรมการ ผู้บริหาร พนักงานและลูกจ้างของ บอท. นำตำแหน่งหน้าที่ไปแสวงหาผลประโยชน์ให้แก่ตนเองและบุคคลอื่นโดยมิชอบ และหลีกเลี่ยงการกระทำที่ก่อให้เกิดผลประโยชน์ทับซ้อน (Conflict of Interest) รวมทั้งไม่ยอมรับการทุจริต	3	←	—	—	—	—	—	—	—	—	—	—	→

)

	คอร์รัปชั่นทุกรูปแบบ												
5	บุคลากรของ บอท. ต้องไม่เลือกปฏิบัติโดยไม่เป็นธรรมต่อผู้มีส่วนได้ส่วนเสียภายในและผู้มีส่วนได้ส่วนเสียภายนอก	1	←	—	—	—	—	—	—	—	—	—	→
6	บุคลากรของ บอท. ต้องให้ความสำคัญและปฏิบัติตามหลักการรักษาความปลอดภัยของข้อมูล โดยยึดถือกฎหมายและจริยธรรมที่จำไม่นำข้อมูลของ บอท. บุคคล หรือนิติบุคคลที่เข้าร่วมดำเนินการเกี่ยวกับกิจการของ บอท. ไปเปิดเผยหรือใช้เพื่อแสวงหาผลประโยชน์อย่างอื่น	1	←	—	—	—	—	—	—	—	—	—	→
7	การตกลงทำนิติกรรมสัญญาข้อตกลงใดๆ ของ บอท ต้องเป็นไปตามกระบวนการขั้นตอนและหลักเกณฑ์ที่มีกฎหมาย กฎ ระเบียบข้อบังคับกำหนดไว้ และต้องไม่ขัดต่อกฎหมายหรือขัดต่อความสงบเรียบร้อย ศีลธรรมอันดีของประชาชน รวมทั้งจารีตประเพณี	2	←	—	—	—	—	—	—	—	—	—	→
8	เมื่อหน่วยงานต่างๆ นำกฎหมายไปบังคับใช้แล้วเกิดปัญหาในทางปฏิบัติ ฝ่ายกฎหมายและหน่วยงาน Compliance Unit สามารถเป็นที่ปรึกษาในการตอบข้อหารือเกี่ยวกับปัญหาข้อกฎหมายตามระเบียบข้อบังคับของ บอท.	1	←	—	—	—	—	—	—	—	—	—	→
9	จัดให้มีการรายงานติดตามความคืบหน้าผลการดำเนินงานการบูรณาการด้านการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติงามตามกฎหมาย กฎระเบียบ ข้อบังคับและมาตรฐานที่เกี่ยวข้อง GRC	4		↔			↔			↔			↔	
	รวม	**20**												

)

องค์ประกอบที่ 4 : การวางแผนเชิงกลยุทธ์ (Strategic Planning)

หลักเกณฑ์ : การวางแผนเชิงกลยุทธ์ เป็นการกำหนดทิศทางขององค์กร โดยการวิเคราะห์สภาพแวดล้อมทั้งภายในและภายนอกองค์กร เพื่อกำหนดกลยุทธ์ที่เหมาะสมกับองค์กร เพื่อที่จะนำกลยุทธ์เหล่านั้นไปประยุกต์ปฏิบัติและควบคุมประเมินผลการดำเนินงานขององค์กรได้อย่างมีประสิทธิภาพและประสิทธิผล

ที่	แผนงาน / โครงการ	น้ำหนัก	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
1	บอท. ต้องกำหนดตำแหน่งยุทธศาสตร์ที่ต้องการบรรลุสอดคล้องกับวิสัยทัศน์ขององค์กร กำหนดเป้าหมายที่ชัดเจน เพื่อให้การวางแผนยุทธศาสตร์มีกรอบเวลาที่ชัดเจน	4							←	→				
2	กำหนดให้มีการรวบรวมและวิเคราะห์ปัจจัยนำเข้าในการวางแผนยุทธศาสตร์	2							←	→				
3	กำหนดให้มีกลยุทธ์ที่รองรับในแต่ยุทธศาสตร์ที่สนับสนุนซึ่งกันและกัน (Strategy Map)	2							←	→				
4	กำหนดให้มีการวิเคราะห์ Business Model ภายใต้การเปลี่ยนแปลงของสภาพแวดล้อม การแข่งขัน	2							←	→				
5	กำหนด Intelligence Risk ด้วยการวิเคราะห์ Scenario ต่างๆ	2							←	→				
6	กำหนดให้มการออกแบบ/ทบทวนระบบงาน (Work Systems) ขององค์กร	2							←	→				
7	กำหนดให้ทุกหน่วยงานจะต้องจัดทำแผนปฏิบัติการในแต่ละขั้นตอนให้ครบถ้วน	2								←	→			
8	กำหนดให้มีการสื่อสารแผนปฏิบัติการทั้งภายในและภายนอกองค์กร และถ่ายทอดตัวชี้วัดในการดำเนินงานไปยังบุคลกรที่เกี่ยวข้อง	2											←	→
9	กำหนดให้มีกระบวนการ	2	←	→										

)

	ปรับเปลี่ยนแผนปฏิบัติการ การดำเนินงานตาม แผนปฏิบัติการที่ ปรับเปลี่ยนอย่างทันท่วงที													
	รวม	**20**												

องค์ประกอบที่ 5 : การมุ่งเน้นผู้มีส่วนได้ส่วนเสียและลูกค้า (Stakeholder & Customer Management)

หลักเกณฑ์ : การมุ่งเน้นผู้มีส่วนได้ส่วนเสียและลูกค้า (Stakeholder & Customer Management) และความคาดหวังของผู้มีส่วนได้ส่วนเสียของลูกค้าทุกกลุ่ม สร้างโอกาสใหม่ทางการตลาด และสร้างผลกระทบในเชิงบวก ลดผลกระทบเชิงลบทางสังคมภายใต้ข้อกำหนดของกฎหมายและกฎระเบียบที่เกี่ยวข้อง ซึ่งจะก่อให้เกิดการบูรณาการกับการกำกับดูแลกิจการที่ดี การวางแผนเชิงกลยุทธ์และการบริหารจัดการในทุกระดับ เพื่อพัฒนาการดำเนินธุรกิจให้ลดความเสี่ยงและเพิ่มความสามารถในการแข่งขัน ซึ่งนำไปสู่การพัฒนาธุรกิจอย่างยั่งยืน

ที่	แผนงาน / โครงการ	น้ำหนัก	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
1	กำหนดให้มีการจัดทำแผนยุทธศาสตร์ด้านผู้มีส่วนได้ส่วนเสียและด้านลูกค้าและตลาด โดยจะต้องได้รับความเห็นชอบจากคณะกรรมการบริษัทฯ ซึ่งจะต้องมีการศึกษากำหนดวัตถุประสงค์และขอบเขตของการสร้างความสัมพันธ์กับผู้มีส่วนได้ส่วนเสียและลูกค้า (Stakeholder & Customer) ขององค์กร และมีแนวทางในการจัดทำข้อมูลผู้มีส่วนได้ส่วนเสียและลูกค้า (Stakeholder & Customer Profile) อย่างเป็นระบบ	4	←	→	→									
2	กำหนดให้มีการรับฟังและวิเคราะห์ความต้องการ/ความคาดหวังของกลุ่มเป้าหมาย (Target Group)	2	←	→										

)

3	ทบทวนระบบและกระบวนการทำงานสำหรับใช้ประกอบการกำหนดการบูรณาการ Business Model และ Intelligent Risk ที่เหมาะสม เพื่อเข้าถึงโอกาสทางธุรกิจและเติบโตอย่างยั่งยืน รองรับการเปลี่ยนแปลงอย่างพลิกผัน (Disruptive Innovation)	2	←	—	→									
4	กำหนดให้มีการจัดการความสัมพันธ์กับผู้มีส่วนได้ส่วนเสียและลูกค้าอย่างเป็นระบบ	2	←	—	→									
5	นำความต้องการ/ความคาดหวังมาวิเคราะห์และจัดทำแผนงาน/โครงการจัดการความสัมพันธ์กับผู้มีส่วนได้ส่วนเสียและลูกค้า โดยนำเทคโนโลยีดิจิทัลมาปรับใช้อย่างเหมาะสม	2	←	—	→									
6	กำหนดให้มีช่องทางในการรับข้อร้องเรียนและมีระเบียบวิธีปฏิบัติในการจัดการข้อร้องเรียน	2	←	—	→									
7	ดำเนินการเผยแพร่นโยบายและระเบียบวิธีปฏิบัติในการจัดการข้อร้องเรียนทั้งภายในและภายนอกองกรผ่านช่องทางที่สำคัญ	2		←	—	→								
8	บูรณาการเชื่อมโยงข้อมูลผู้มีส่วนได้ส่วนเสียและลูกค้าที่รวบรวมจากทุกจุดที่ให้บริการมาวิเคราะห์ประเมิน	2							←	—	→			

)

	ประสิทธิผล เพื่อนำไปปรับปรุงการดำเนินงาน													
9	กำหนดให้มีนโยบายในการปฏิบัติต่อผู้มีส่วนได้ส่วนเสียและลูกค้า ด้วยความเสมอภาคและเป็นธรรม โดยคำนึงถึงสิทธิของผู้มีส่วนได้ส่วนเสียและลูกค้าทุกกลุ่ม	2	◄	———	►									
	รวม	**20**												

)

ภาคผนวก GRC Health Check

ข้อ	ประเด็น	ใช่	ไม่ใช่
ส่วนของคณะกรรมการ (Board's Accountability)			
1	คณะกรรมการให้ความสำคัญและนำประเด็นความคาดหวังของผู้มีส่วนได้ส่วนเสียต่างๆ มาใช้ในการพิจารณาทบทวนความเหมาะสมของเป้าหมายระยะยาว กลยุทธ์ และรูปแบบการดำเนินธุรกิจขององค์กรอย่างสม่ำเสมอ		
2	คณะกรรมการมีความเข้าใจในมุมมองด้าน Risk Management ที่ครอบคลุมมากกว่าการดำเนินมาตรการที่มุ่งขจัดความเสี่ยง รวมถึงการใช้เป็น สัญญาณเตือนภัยล่วงหน้า ที่ทำให้เห็นถึงจุดอ่อนของการกำกับดูแลและมาตรการปฏิบัติตามกฎเกณฑ์ อันนำไปสู่การแก้ไขได้อย่างทันท่วงที		
3	คณะกรรมการมีความเข้าใจในมุมมองด้าน Compliance ที่ครอบคลุมมากกว่าการมุ่งปฏิบัติตามกฎเกณฑ์ภาคบังคับ รวมถึงการมุ่งตอบสนองความคาดหวังของผู้มีส่วนได้ส่วนเสียอย่างเป็นธรรม ตลอดจนการดำเนินงานตามหลักจริยธรรม แนวปฏิบัติที่ดี และมาตรฐานสากล		
4	คณะกรรมการมุ่งปลูกฝังให้เกิดวัฒนธรรมองค์กรที่ตระหนักถึงความเสี่ยง พร้อมส่งเสริม / ผลักดันให้หน่วยงานรับผิดชอบดำเนินการให้มีการบูรณาการ GRC อย่างเป็นรูปธรรม		
5	คณะกรรมการดูแลให้มั่นใจว่ากระบวนการวางแผนกลยุทธ์ได้ถูกดำเนินการควบคู่ไปกับการวางแผนบริหารความเสี่ยง		
6	คณะกรรมการติดตามดูแลการดำเนินงานตามแผนในข้อ 5 อย่างต่อเนื่อง โดยกำหนดเป็นวาระที่ชัดเจนในการประชุมคณะกรรมการ		
ส่วนของโครงสร้าง / นโยบาย / ระบบงานภายในองค์กร			
7	โครงสร้างด้านการกำกับดูแลกิจการ การบริหารความเสี่ยงและการกำกับการปฏิบัติตามกฎเกณฑ์มีความเชื่อมโยงกัน ไม่ได้ปฏิบัติงานแบบแยกกัน		
8	การกำหนดบทบาทและความรับผิดชอบด้าน GRC ในระดับกรรมการและหน่วยงานรับผิดชอบ		
9	การมอบหมายอำนาจหน้าที่และความรับผิดชอบด้าน GRC มีความเหมาะสมและชัดเจน		
ส่วนของโครงสร้าง / นโยบาย / ระบบงานภายในองค์กร			
10	การประเมินผลงานฝ่ายจัดการ การให้รางวัล และการชื่นชมช่วยส่งเสริมการปฏิบัติตามแนวทาง GRC		
11	การสื่อสารและการรายงานเกี่ยวกับ GRC เป็นช่องทางที่มีประสิทธิภาพและประสิทธิผล		
12	การปฏิบัติงานอย่างมีจรรยาบรรณและซื่อสัตย์ได้รับการมุ่งเน้นอย่างจริงจัง		
13	ระบบการบริหารความเสี่ยงได้รับการพัฒนาและปฏิบัติอย่างมีประสิทธิภาพและประสิทธิผลอย่างต่อเนื่อง		
14	ระบบการกำ กับการปฏิบัติตามกฎเกณฑ์ (Compliance) ได้รับการพัฒนาและปฏิบัติอย่างมีประสิทธิภาพและประสิทธิผล และปฏิบัติต่อเนื่องเป็นงานประจำ		
15	ระบบการตรวจสอบภายใน ได้รับการพัฒนาและปฏิบัติอย่างมีประสิทธิภาพและประสิทธิผล		
16	ระบบการบริหารจัดการเหตุทุจริตได้รับการพัฒนาและปฏิบัติอย่างมีประสิทธิภาพและประสิทธิผล ซึ่งครอบคลุมทั้งการค้นพบ การแก้ไข และการลงโทษ		
17	นโยบาย GRC ได้รับการสื่อสารไปยังบุคลากรทุกระดับ รวมถึงมีการติดตามและรายงานผลการปฏิบัติตามนโยบายอย่างสม่ำเสมอ		
18	ระบบเทคโนโลยีสารสนเทศได้ถูกนำ มาใช้ให้เป็นประโยชน์ต่อการบูรณาการ GRC		

)

เอกสารอ้างอิง

1. A Maturity Model for Integrated GRC, The Open Compliance and Ethics Group
2. Corporate Governance Code, The Office of Securities and Exchange Commission, 2017
3. Corporate Governance in the Boardroom – A Practical Perspective, Pricewaterhouse Coopers, 2015
4. Corporate Governance Health Check – Increasing the Value of Your Business, Pricewaterhouse Coopers, 2013
5. COSO Enterprise Risk Management 2017
6. Enterprise Risk Management – Integrating with Strategy and Performance, Committee of Sponsoring Organizations of the Treadway Commission (COSO), June 2017
7. Fundamentals of GRC : The Connected Roles of Internal Audit and Compliance, Thomson Reuters
8. GRC Capability Model version 3.0, The Open Compliance and Ethics Group
9. G20/OECD Principles of Corporate Governance, Organization for Economic Co-operation and Development (OECD), 2015
10. Guidance on Board Effectiveness, Financial Reporting Council (FRC), July 2018
11. Implement GRC Lines of Defense to Improve Your Business Processes, The Open Compliance and Ethics Group
12. Should your Board have a separate Risk Committee, Harvard Law School Forum, 2012
13. Striking a Balance – Whistleblowing arrangements as part of a speakup strategy, PwC,January 2011
14. The Building Blocks of GRC, The Open Compliance and Ethics Group, April 2016
15. The UK Corporate Governance Code, Financial Reporting Council (FRC), July 2018
16. The GRC Toolbox – the Use of Integrated Methods to Fight Fraud, Association of Certified Fraud Examiners, Fraud Magazine, September-October 201