GRC ควรมีความสำคัญต่อองค์กรของคุณอย่างไรบ้าง

ผู้แปล ศรรณ ทองประเสริฐ, CIA

หากคุณเป็นคนที่ติดตามอ่านข่าวสารธุรกิจทั้งทางหน้าหนังสือพิมพ์ และบล็อก (Blog) ต่างๆ อยู่เป็นประจำแล้ว โอกาสที่คุณจะพบตัวอักษรสามตัว คือ “GRC” นั้นมีบ่อยครั้งมากขึ้น

แนวคิดเรื่อง GRC Governance Risk และ Compliance นั้นไม่ใช่เรื่องใหม่ GRC ไม่ได้เป็นเพียงตัวอักษรสามตัวที่เรียงอยู่ติดกัน แต่อักษรสามตัวดังกล่าว เป็นสัญญลักษณ์ของแนวคิดที่สำคัญทางธุรกิจ ที่ควรอยู่ในใจของผู้บริหาร หรือผู้นำองค์กรที่ต้องรับผิดชอบในการขับเคลื่อนองค์กรที่นับวันยิ่งมีความซับซ้อนมากขึ้น

GRC คืออะไร?

ตามที่ Open Compliance and Ethics Group (OCEG) ได้ระบุความหมายของ GRC ว่าเป็นระบบที่เกี่ยวข้องกับคน (people) กระบวนการ (processes) และเทคโนโลยี (technology) ที่ช่วยขับเคลื่อนองค์กรให้

- มีความเข้าใจและจัดลำดับความสำคัญต่อความคาดหวังของผู้มีส่วนได้เสีย (Stakeholders)
- กำหนดวัตถุประสงค์ทางธุรกิจเพื่อให้สอดคล้องกับมูลค่าและความเสี่ยงที่เกี่ยวข้อง
- บรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนด และสามารถเพิ่มประสิทธิภาพในการเฝ้าระวังความเสี่ยง (Risk Profile) และปกป้องคุณค่าขององค์กร (Value)
- ดำเนินการภายใต้ขอบเขตของกฎหมาย สัญญา ระบบภายใน สังคม และจริยธรรม
- ให้ข้อมูลที่เกี่ยวข้อง เชื่อถือได้ และทันเวลา ต่อผู้มีส่วนได้เสีย
- ส่งเสริมการวัดผลของระบบการดำเนินงานและการมีประสิทธิผล

คาร์โรล์ สวิตเซอร์ ประธาน OCEG เชื่อว่าแนวคิด GRC มีศักยภาพที่จะจัดให้องค์กรมีข้อมูลที่นำมาใช้ในการจัดการบริหารความเสี่ยงให้สอดคล้องกับวัตถุประสงค์ ลดความซับซ้อนและความไม่สม่ำเสมอในการดำเนินงาน และควบคุมประสิทธิภาพการใช้เทคโนโลยีให้เหมาะสมที่สุด “*ทุกวันนี้ ผู้บริหารและฝ่ายจัดการระดับสูงต่างตระหนักถึงความต้องการความรู้ในวิธีการจัดการเชิงบูรณาการเชิงรุกที่มีประสิทธิภาพทั่วทั้งองค์กรมากขึ้น*” สวิตเซอร์ กล่าวว่า “*เมื่อดำเนินการได้อย่างเหมาะสมแล้ว GRC นี่แหละเป็นแนวคิดที่ตอบโจทย์ได้ทั้งหมด*” และเธอยังกล่าวต่ออีกว่า GRC เป็นตัวผลักดันให้เกิดการตัดสินใจในเรื่องความเสี่ยงอย่าง

ชาญฉลาด เพิ่มความคล่องตัวขององค์กร และลดค่าใช้จ่ายเกี่ยวกับระบบงาน "*เมื่อพิจารณาถึงผลประโยชน์เหล่านี้ แล้วทำไมจะไม่นำแนวคิดนี้มาใช้หล่ะ*" เธอกล่าวถาม

GRC กับ ERM

ความแตกต่างอยู่ที่ตรงไหน?

ทั้ง Governance Risk and Compliance (GRC) และ Enterprise Risk Management (ERM) ต่างมีจุดมุ่งหมายเพื่อให้เกิดความเชื่อมั่นว่าองค์กรสามารถระบุความเสี่ยงทั้งหมดที่องค์กรเผชิญอยู่ (Identified) รวมทั้งการวิเคราะห์ (Analyzed)และบอกจำนวน (Quantified)ได้

อย่างไรก็ตาม ทั้งสองแนวคิดนี้มีความแตกต่างที่สำคัญ

ERM เป็นวิธีการจัดการความเสี่ยงทั่วทั้งองค์กร โดยมีการวัด และกำหนดลักษณะของความเสี่ยง รวมทั้งการกำหนดให้แต่ละส่วนงานเป็นเจ้าของความเสี่ยง (Risk Ownership) ในหน่วยงานของตนเอง

GRC มีกรอบโครงสร้างที่กว้างกว่า ซึ่งครอบคลุมถึงขอบข่ายของงาน และปรัชญาในการสื่อสาร ทั้งการกำกับดูแล และความเสี่ยงด้านการปฏิบัติตามระเบียบ ข้อบังคับ โดยใช้ประโยชน์จากเทคโนโลยีเพื่อการรายงานผล ซึ่งใช้เครื่องมือต่างในการควบคุมและจัดการสิ่งต่างๆ เช่น นโยบาย (Policies) ขั้นตอนการทำงาน (Procedures) เอกสารที่ต้องการ (Documentation Requirement) และการประเมินความเสี่ยง (Risk Assessments) โดยแก่นแท้แล้ว GRC ครอบคลุมเนื้อหาทั้งหมดของ ERM

แหล่งข้อมูล: Treasury & Risk, June 2007

ประโยชน์ของ GRC คืออะไร?

ในขณะที่องค์กรมีการเติบโตและมีพัฒนาการมากขึ้น บ่อยครั้งที่การพัฒนากระบวนการทำงานใหม่บนวิธีการเดิม โดยไม่ได้พิจารณาในรายละเอียดของการทำงานอีกครั้งว่าเป็นการทำงานที่เหมาะสม ซ้ำซ้อน หรือมีประสิทธิภาพหรือไม่ หน้าที่การทำงานในหลายเรื่องส่วนใหญ่เป็นการตอบสนองเพียงแต่ประเด็นปัญหาที่เข้ามา มากกว่าเป็นการแสวงหาวิธีการจัดการในเชิงรุก

อย่างไรก็ตาม "GRC" เป็นแนวคิดในเรื่องการจัดการแบบบูรณาการ (Integrated) ผสมผสานการจัดการเชิงรุกที่ใช้ประโยชน์เต็มที่จากโอกาส และทรัพยากรที่มีอยู่ โดยเฉพาะอย่างยิ่งทรัพยากรด้านเทคโนโลยีสารสนเทศ เมื่อนำ GRC มาใช้งานได้อย่างมีประสิทธิผลแล้ว GRC จะช่วยให้มั่นใจได้ว่าระบบการควบคุมมีความเหมาะสม การปฏิบัติงานเป็นไปอย่างมีประสิทธิผล มีการระบุความเสี่ยง และใช้ทรัพยากรในการจัดการอย่างมีประสิทธิภาพ ประโยชน์ที่สำคัญมากกว่านั้นคือ GRC สามารถช่วยให้เกิดความเชื่อมั่นแก่คณะกรรมการและผู้บริหารระดับสูงว่าระบบทั้งหมดในด้านการกำกับดูแล (Governance) ความเสี่ยง (Risk) และการปฏิบัติงานตามระเบียบ (Compliance) เป็นการปฏิบัติงานที่มีประสิทธิผล และมีคุณภาพสูง

จากคำกล่าวของสวิตเซอร์ GRC คือ วิธีการคิดและการปฏิบัติที่ช่วยปรับเปลี่ยนกระบวนทัศน์ภายในองค์กร "*เหตุผลที่ฉันหลงใหลใน GRC ก็คือ มันสามารถนำไปสู่การเปลี่ยนแปลงรูปแบบของการทำธุรกิจได้จริง*" เธอกล่าวต่อว่า "*...แนวทางที่เราเข้าใจและระบุความเสี่ยงได้ รวมถึงบรรลุหลักการกำกับที่ดีและมีคุณภาพทั้งในองค์กรขนาดใหญ่ และองค์กรขนาดเล็ก* " สิ่งเหล่านี้เป็นเรื่องเกี่ยวกับการบูรณาการ (Integrated) สร้างระบบที่ก่อให้เกิดความกลมกลืนระหว่างคน กระบวนการ และเทคโนโลยี ซึ่งระบบดังกล่าว ไม่เพียงแต่ใช้งานในสถานการณ์ปกติที่ไร้อุปสรรค แต่ยังมีความยืดหยุ่น ความรวดเร็ว และสามารถตอบสนองต่อสถานการณ์ต่างๆ ด้วยรูปแบบที่มีการควบคุมอย่างมีประสิทธิภาพ

ประโยชน์ของ GRC ยังรวมถึงการสร้างความมั่นใจให้กับผู้มีส่วนได้เสีย (Stakeholders) ปรับปรุงการตอบสนองและความพร้อมขององค์กรในการระบุความเสี่ยง และการลื่นไหลของข้อมูลอย่างสม่ำเสมอทั่วทั้งองค์กร

การปฏิบัติ GRC ที่ดีที่สุด

รางวัล GRC Achievement Award จัดขึ้นโดย OCEG เพื่อมอบรางวัลเกียรติยศให้กับองค์กรที่เป็นแบบอย่างในการบูรณาการธรรมาภิบาล การบริหารความเสี่ยง และการปฏิบัติตามระเบียบข้อบังคับ และเมื่อเร็ว ๆ นี้ รางวัลเกียรติยศประจำปี 2010 ได้มอบให้แก่ 6 บริษัทชั้นนำของโลก ได้แก่

1. Best Buy

   Best Buy ใช้สื่อสังคม (Social Media) ในการกระตุ้นให้เกิดประเด็นการสนทนาทางจริยธรรม โดยการใช้บล็อกที่มีเนื้อหาเกี่ยวกับจริยธรรมเป็นสื่อกลางจนกลายเป็นที่นิยมในกลุ่มคนทำงานรุ่นใหม่และลูกค้า

2. Capital One

   การนำหลักการง่ายๆ และกระบวนการบริหารความเสี่ยงอย่างที่มาตรฐานมาปรับปรุงระบบการควบคุมภายใน และเพิ่มระดับความสบายใจ (Comfort) และความเชื่อมั่นในการทำงาน (Assurance)

3. Carnival

   แม้ Carnival จะเป็นองค์กรที่มีอยู่ทั่วโลกที่ใช้การบริหารงานแบบกระจายอำนาจ บริษัทประสบความสำเร็จในการบูรณาการ (Integrated) GRC ซึ่งเป็นผลให้เกิดความสมดุลในโครงสร้างองค์กรและเสริมสร้างการควบคุมภายใน

4. DIRECTV

   หลังจากที่ได้มีการระบุความเสี่ยงตามลักษณะธุรกิจ (Inherent Risks) และความท้าทายในการจัดการข้อมูลบน Spreadsheet นั้น DIRECTV ได้ใช้วิธีการนี้ขยายผลไปทั่วทั้งองค์กร โดยออกแบบการใช้งานให้เป็นมาตรฐาน มีการดูแลรักษา และแบ่งปันข้อมูลระหว่างฝ่ายต่างๆ ในองค์กร

5. Tawuniya

   การเชื่อมโยงแนวคิดแบบ GRC กับผลการทำงานของฝ่ายจัดการ บริษัทตัวแทนประกันภัยชั้นนำจากซาอุดีอาระเบียบริษัทนี้ได้สร้างวัฒนธรรมองค์กรให้เกิดการบริหารความเสี่ยงที่มีประสิทธิผล

6. VISA

   รวบรวมความต้องการที่มีมากกว่า 3,400 ความคิดเห็น มาเป็นข้อมูลใช้ในระบบเพื่อการสนับสนุนการวิเคราะห์ข้อมูลสำคัญที่มีความน่าสนใจ และเพื่อสร้างความเชื่อมั่น บริษัทVISA ได้ดำเนินการบริหารความเสี่ยงในแบบองค์รวมทั่วทั้งองค์กร

บทบาทของงานตรวจสอบภายใน

ผู้ตรวจสอบภายในมีบทบาทสำคัญในการเป็นที่ปรึกษา ให้คำแนะนำแก่องค์กรเรื่องแนวทางการบริหารเชิงรุกที่ผสมผสานการกำกับดูแล ความเสี่ยง และการปฏิบัติตามระเบียบ แก่ผู้บริหารระดับสูงมากกว่าที่จะมองในเรื่องของการบริหารความเสี่ยงแบบเดิมๆ อาจกล่าวได้ว่า ไม่มีหน้าที่ใดในหน่วยงานของบริษัทที่เหมาะสมในการประเมินประสิทธิผลของการดำเนินงาน GRC ได้ดีเท่ากับงานตรวจสอบภายใน

เมื่อคณะกรรมการและผู้บริหารระดับสูงตัดสินใจที่จะนำแนวคิด GRC มาปรับใช้กับองค์กร การวัดผลเกี่ยวกับประสิทธิผลในการดำเนินการนั้น จึงนับเป็นโอกาสที่ดีสำหรับ ผู้ตรวจสอบภายในที่จะสร้างความเชื่อมั่นว่าการดำเนินงานนั้น มีการวางระบบ ที่มีความโปร่งใส และมีแบบแผน สำหรับใช้ในการตัดสินใจซึ่งได้ตระหนักถึงความเสี่ยงที่อาจเกิดขึ้น

"*คณะกรรมการของบริษัทไม่สามารถที่จะทำหน้าที่เพียงแต่มอบอำนาจให้ฝ่ายจัดการในการวางแผนกลยุทธ์และการตัดสินใจว่าองค์กรจะดำเนินการไปในทิศทางไหน*" สวิตเซอร์กล่าวต่อว่า "*จะให้หลับหูหลับตาตัดสินใจ หรืออนุมัติอะไรจากการฟังรายงานเท่านั้นไม่ได้*" เธอกล่าวถึงบทบาทหน้าที่ของคณะกรรมการในปัจจุบันที่จะต้องกำหนดขอบเขตหรือกรอบในการทำงานของแต่ละหน้าที่ในองค์กร "*สำหรับการกำกับดูแลอย่างแท้จริงนั้น พวกเขาควรจะต้องกำหนดวิสัยทัศน์ ภารกิจ และให้ความเชื่อมั่นว่าระบบ GRC สามารถวัดผลการดำเนินงานได้อย่างชัดเจน*" เธอกล่าวเสริมว่า "*การมีส่วนร่วมอย่างเหมาะสมของผู้ตรวจสอบภายในจะช่วยให้คณะกรรมการมั่นใจได้ว่าพวกเขาได้ทราบถึงสิ่งที่จำเป็นต้องรู้เพื่อการกำกับดูแลอย่างแท้จริง*"

แน่นอนว่า ไม่มีวิธีการใดที่จะให้ความเชื่อมั่นต่อการกำกับดูแลว่ามีประสิทธิผล100 เปอร์เซ็นต์ แต่สิ่งที่เราต้องการคือ ให้ความเสี่ยงในแต่ละส่วนงานลดลง และมีการปฏิบัติตามกฎระเบียบข้อบังคับ อย่างไรก็ตาม แนวคิด GRC ให้แนวคิดอย่างเป็นระบบในการระบุความเสี่ยงและปัญหาในการปฏิบัติงาน

ตามที่สวิตเซอร์กล่าวข้างต้นนั้น แนวคิด GRC กำหนดระดับในการดำเนินการที่สามารถปฏิบัติงานได้ซ้ำเหมือนเดิม มีการจัดระบบเอกสาร มีความสม่ำเสมอ และความสอดคล้องกลมกลืนกับกระบวนการทำงาน "*ประเด็นมันไม่ได้อยู่ที่ว่า จะต้องลดความเสี่ยงให้หมดในทุกส่วนงาน แต่ต้องระบุให้ได้ก่อนว่าความเสี่ยงนั้นคืออะไร และมีความเข้าใจวิธีการจัดการภายใต้สถานการณ์ที่มีความแตกต่างกันนั้นอย่างไร*" เธอกล่าวว่า "*มันเกี่ยวกับการสร้างระบบควบคุมที่สำคัญบนพื้นฐานของการวิเคราะห์ถึงผลกระทบจากความเสี่ยงอย่างแท้จริง ไม่ใช่การคาดเดา และการใส่แนวคิดลงในกระบวนการให้กลมกลืนกับระบบการปฏิบัติงาน จะช่วยให้เกิดผลลัพธ์ที่ต้องการมากกว่าที่จะเกิดความเสียหายต่อธุรกิจ*"

การนำแนวคิด GRC มาปรับใช้นั้น ไม่ได้หมายความว่าต้องยกเลิกกระบวนการทำงานและเทคโนโลยีเดิมที่ใช้อยู่ และเริ่มต้นใหม่ หรือการทุ่มใช้งบประมาณมากมายในการสร้างขั้นตอนการทำงานซับซ้อน ทุกองค์กรควรประเมินระดับขั้นการทำงานในปัจจุบัน รวมทั้งพิจารณาจุดสำคัญที่ต้องการจะทำให้ประสบผลสำเร็จ โดยการจัดลำดับความสำคัญของงานในการปรับปรุง

ในปัจจุบัน คณะกรรมการบริษัท โดยเฉพาะบริษัทมหาชนที่มีกิจการทั่วโลก จะอยู่ภายใต้การพิเคราะห์อย่างที่ไม่เคยมีมาก่อน เพราะว่าไม่ใช่เป็นเพียงแค่การได้รับมอบหมายให้กำหนดกลยุทธ์ในการกำกับดูแลและตัดสินใจในนามของผู้มีส่วนได้เสีย แต่การตัดสินใจดังกล่าวยังส่งผลกระทบต่อสังคมโดยรวม เพราะในบางกรณี การตัดสินใจของพวกเขาสามารถเปลี่ยนแปลงทิศทางของตลาดเศรษฐกิจและสภาพแวดล้อมทางกายภาพ หน้าที่ความรับผิดชอบของคณะกรรมการบริษัท คือทำให้แน่ใจว่า พวกเขามีความเข้าใจอย่างแท้จริงถึงผลลัพธ์ของการตัดสินใจที่เกิดขึ้นที่มีความสำคัญร้ายแรง และที่ก่อให้เกิดความกังวลใจ

ในกรณีที่ไม่มีการบูรณาการ (Integrated) ระบบ GRC ใช้ในการปฏิบัติงาน ซึ่งเป็นระบบที่ช่วยให้มีความชัดเจนถูกต้องแม่นยำของข้อมูล และเป็นฐานในการตัดสินใจเรื่องความเสี่ยงได้อย่างชาญฉลาด คณะกรรมการบริษัทอาจมีข้อจำกัดในการตัดสินใจอย่างหลีกเลี่ยงไม่ได้ ในกรณีที่มีการพัฒนาระบบ GRC ให้มีความสมบูรณ์เต็มที่ ซึ่งเป็นการบูรณาการ (Integrated) ของระบบงาน การจัดการความเสี่ยงให้มีความสมดุล และมีกระบวนการปฏิบัติงานที่มีความสอดคล้องและโปร่งใสทั่วทั้งองค์กรนั้น ดังนั้นการพัฒนาจึงจะต้องให้ความสำคัญในการปรับปรุงระบบเทคโนโลยีสารสนเทศเป็นอันดับแรก