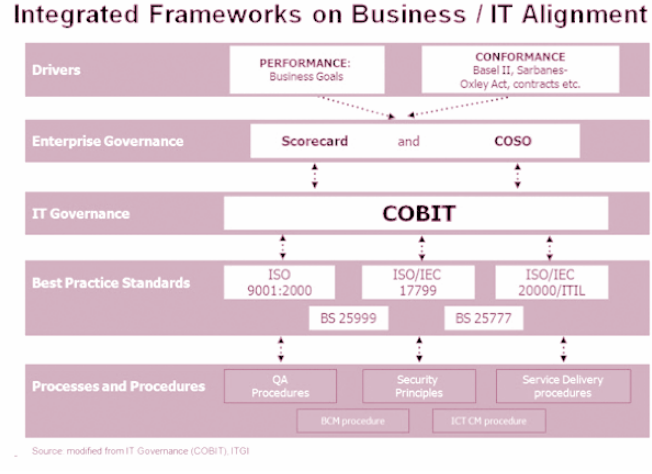
แนวคิด GRC กับการบริหารเทคโนโลยีสารสนเทศขององค์การ

วิชญ์ศุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

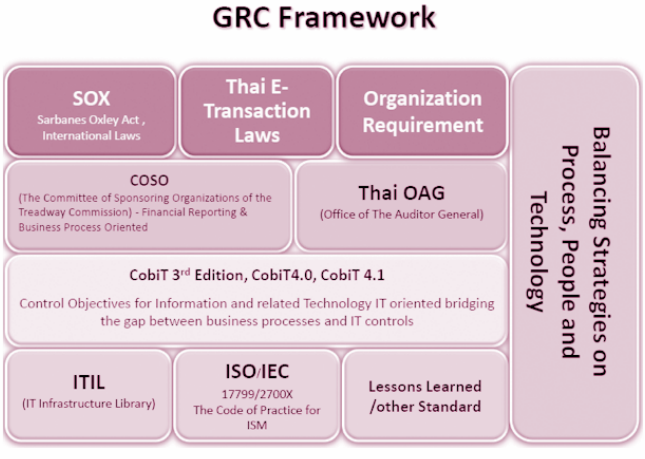
ต่อ จากฉบับที่แล้ว

GRC ถือว่าเป็นแนวคิดในเรื่องการจัดการแบบบูรณาการที่ผสมผสานการจัดการเชิงรุก ซึ่งใช้ประโยชน์เต็มที่จากโอกาส และทรัพยากรที่มีอยู่โดยเฉพาะอย่างยิ่งทรัพยากรด้าน IT และใช้กลไก หรือรูปแบบการบริหารอื่นๆ มาเป็นเครื่องมือสนับสนุนให้การบริหารมีความครบถ้วน ซึ่งเมื่อนำ GRC มาใช้งานได้อย่างมีประสิทธิผลแล้ว GRC จะช่วยให้มั่นใจได้ว่าระบบการควบคุมมีความเหมาะสม การปฏิบัติงานเป็นไปอย่างมีประสิทธิผล มีการระบุความเสี่ยงที่ยอมรับได้ และมีการใช้ทรัพยากรในการบริหารจัดการอย่างมีประสิทธิภาพ ประโยชน์ที่สำคัญมากกว่านั้น คือ GRC สามารถช่วยสร้างให้เกิดความเชื่อมั่นแก่คณะกรรมการ และผู้บริหารระดับสูงว่าระบบงานทั้งหมดที่อยู่ภายใต้การกำกับดูแล (Governance) ความเสี่ยง (Risk) และการปฏิบัติงานตามระเบียบ (Compliance) นั้นเป็นการดำเนินงานที่มีประสิทธิผล และมีคุณภาพ ส่งผลต่อการตัดสินใจเชิงนโยบายที่สามารถดำเนินการได้อย่างเป็นระบบมากขึ้นบนพื้นฐานของความชัดเจน และเป็นรูปธรรม รวมถึงการสร้างความมั่นใจให้กับผู้มีส่วนได้ส่วนเสีย (Stakeholders) ที่เกี่ยวข้องได้อย่างเหมาะสม



GRC นั้นจะมุ่งเน้นที่การบริหารความเสี่ยง และกำกับควบคุมเพื่อนำไปสู่การสร้างธรรมาภิบาล ซึ่งโดยปกติในการปฏิบัติตามนโยบายการควบคุมภายในองค์การ และนโยบายด้านการรักษาความมั่นคงปลอดภัยขององค์การ รวมทั้งการดำเนินการเพื่อให้องค์การสามารถผ่านการตรวจสอบของผู้ตรวจสอบทั้งภายใน และภายนอกได้ ส่วนใหญ่จะเป็นไปตามหลักของ *"การกำกับดูแลกิจการที่ดี"* ซึ่งผู้บริหารระดับสูงมักนิยมประยุกต์ ใช้ "Balanced Scorecard" และ "COSO ERM" Framework ในการอ้างอิง โดยมี CobiT ที่กล่าวถึงข้างต้นเป็น IT Governance Framework ที่ควบคุมการดำเนินงานในส่วน IT อย่างเป็นขั้นตอนมีการตรวจสอบในทุกกระบวนงานที่สำคัญ คอยเชื่อมอยู่ตรงกลาง ซึ่งถูกนำมาใช้ในการเชื่อมโยง *"IT"* เข้ากับ *"Business"* เพื่อให้เกิดความสอดคล้องส่งผลให้เกิดประโยชน์สูงสุดต่อองค์การในการนำ IT มาใช้สนับสนุนการดำเนินงาน (IT benefit realization)

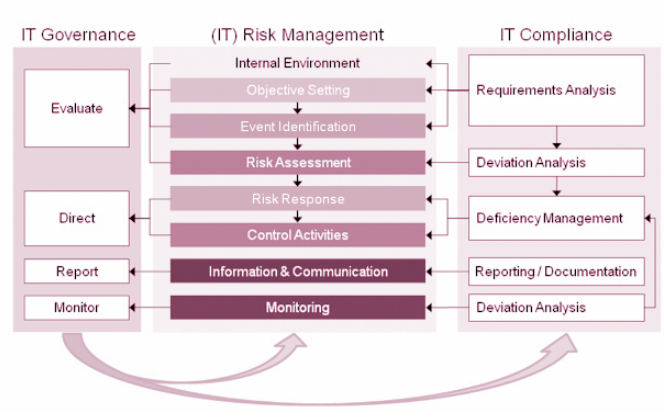
โดยภายใต้กรอบแนวคิด CobiT Framework (What to do) ก็คือ การนำเอารูปแบบการบริหารของกรณีศึกษาที่ประสบความสำเร็จ (Best Practices) หรือ Standard (How to do) ต่างๆ มาประยุกต์ใช้ในการพัฒนาขั้นตอนในการปฏิบัติงานภายในองค์การอาทิ มาตรฐาน ISO 9000, ISO/IEC27001, ISO/IEC 20000, ITIL และเพื่อให้สัมฤทธิ์ผลในทางปฏิบัติจริง ผู้บริหารระดับกลางต้องลงรายละเอียดในขั้นตอนการปฏิบัติงานอย่างเหมาะสม



สำหรับในมุมของ IT แล้วเมื่อนำเอามารวมเข้ากับ GRC เป็น IT GRC จะเป็นการเน้นที่ 3 เรื่องใหญ่ ได้แก่

1. IT Governance
2. IT Risk Management
3. IT Compliance

โดยการบริหารความเสี่ยง (Risk Management) ที่ถือได้ว่าเป็นแกนกลางที่สำคัญมากในการบริหารจัดการองค์การตามแนวคิด GRC มีความเกี่ยวข้องโดยตรงกับการบริหารความเสี่ยงสารสนเทศ (IT Risk Management) และ การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management)



โดยสรุป GRC เป็นแนวคิดที่ปรับทัศนะในการมองรูปแบบการบริหารจัดการองค์การ โดยอาศัยหลักของสิ่งที่ควรดำเนินการเพื่อการกำกับดูแลกิจการ 3 ประการ นั่นคือ

1. การบริหารความเสี่ยง หรือ บริหารการเปลี่ยนแปลง ซึ่งจำเป็นต้องอาศัยความร่วมมือของฝ่ายต่างๆ ในองค์การเพื่อระดมสมองสร้างจุดเริ่มในนโยบายการบริหารความเสี่ยงขององค์การร่วมกัน มีการจัดตั้งหรือกำหนดคณะทำงาน โดยอาศัยกรอบแนวคิด หรือรูปแบบการบริหารที่เกี่ยวข้องเป็นเครื่องมือสนับสนุนการดำเนินงานและนำเสนอนโยบายการบริหารความเสี่ยงแก่ผู้บริหารเพื่อขอความเห็นชอบ

2. การมีมาตรการเพื่อกำกับให้เกิดการปฏิบัติตามกฎระเบียบ ข้อบังคับ มาตรฐาน จากภายนอก หรือองค์การเป็นผู้กำหนดเป็นการภายในซึ่งมีสอดคล้อง และรองรับกับนโยบายการบริหารความเสี่ยงขององค์การ เพื่อควบคุมไม่ให้เกิดการดำเนินการที่จะก่อความเสียหายต่อองค์การ

3. จากข้อที่ 1 และ 2 นำไปสู่การสร้างความเชื่อมั่นให้กับผู้บริหารในการกำหนดนโยบายการบริหารที่มีความโปร่งใส สามารถตรวจสอบได้ การปฏิบัติที่เหมาะสมกับองค์การ สร้างให้เกิดวัฒนธรรมในการปฏิบัติงานขององค์การที่ดีส่งเสริมภาพลักษณ์ขององค์การ

โดย GRC ที่ครอบคลุมงานด้าน IT นั้น สามารถดำเนินการได้ง่าย และมีความชัดเจนเนื่องจากมีเครื่องมือบริหารที่หลากหลายและมีประสิทธิภาพในระดับสากลให้เลือกใช้เป็นบรรทัดฐานในการดำเนินการ

การบูรณาการแนวคิด “GRC” สู่ภาคปฏิบัติในองค์การนั้นจะสำเร็จไม่ได้เลย ถ้าไม่ได้รับความร่วมมือ และการสนับสนุนจากผู้บริหารระดับสูง หากแต่ความยากนั้นอยู่ที่จะทำอย่างไรให้ผู้บริหารระดับสูงเข้าใจในประโยชน์ของการนำแนวคิด GRC มาใช้ ซึ่งเป็นหน้าที่ของ CIO หรือ CISO/CSO ในการนำเสนอแนวคิดดังกล่าวให้

ผู้บริหารระดับสูงมองเห็นประโยชน์อย่างชัดเจน และจับต้องได้ เสียก่อน กล่าวคือ บริหารและกำกับดูแล “IT” อย่างไรให้ยังประโยชน์ถึง “Business” จากนั้นจึงค่อยลงรายละเอียดในเรื่องของการบริหารความเสี่ยง และลงรายละเอียดในกระบวนการขั้นตอนการปฏิบัติงานด้วยมาตรฐาน กฎ ระเบียบ ข้อบังคับต่างๆ ที่เหมาะสม

แนวคิด “GRC” ไม่ได้เป็นเพียง “G” “R” และ “C” หากแต่มีความหมายลึกซึ้งในการเชื่อมโยงและบูรณาการอยู่ในตัวเอง มีการเชื่อมโยงไปถึงเรื่องของภาวะผู้นำ และวัฒนธรรมภายในองค์การ อย่างหลีกเลี่ยงไม่ได้ ดังนั้นเรื่องของความร่วมมือ และความเข้าใจของผู้ปฏิบัติในองค์การจึงเป็นเรื่องสำคัญที่เป็นปัจจัยแห่งความสำเร็จ ของ GRC

สิ่งสำคัญที่กล่าวถึงเสมอ คือ การทำศึกนั้น “รู้เขารู้เรา รบร้อยครั้งชนะร้อยครั้ง” สิ่งสำคัญไม่ใช่ ***“รู้เขา”*** แต่เป็น ***“รู้เรา”*** กล่าวคือ การสร้างความชัดเจนให้กับองค์การเองในเรื่องต่างๆ เพื่อเป็นจุดเริ่มทั้งในแง่การพัฒนาศักยภาพ การปรับปรุงประสิทธิภาพ การซ่อมแซมส่วนสึกหรอ การมองให้เห็นถึงอาวุธที่เรามี และวิธีการใช้ประโยชน์เหล่านี้ อาจใช้ EA ในการจัดการ และสำหรับ GRC นั้น คือแนวทางการการบริหารเพื่อสร้างความยืดหยุ่น ปกปิดจุดอ่อน (จำกัด และกำจัดความเสี่ยงที่มี) สร้างความเข้มแข็ง ความเป็นระเบียบขององค์การ และบุคลากรในองค์การ รวมถึงการก้าวเดินไปข้างหน้าอย่างมีธรรมาภิบาลโปร่งใสตรวจสอบได้ สร้างความเชื่อมั่นให้กับผู้มีส่วนได้ส่วนเสีย และภาพลักษณ์ที่ดีขององค์การ ซึ่งปัจจุบันมีบริษัทชั้นนำของโลกที่นำเอา GRC ไปประยุกต์ใช้แล้วประสบความสำเร็จ อาทิ Best Buy, Capital One, DIRECTV, VISA เป็นต้น TPA news

แหล่งข้อมูลอ้างอิง

1. www.grc-resource.com
2. www.acisonline.net
3. กลยุทธ์ GRC เพื่อการพัฒนา IT ขององค์การ, กำพล ศรธนะรัตน์
4. สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย (The Institute of Internal Auditors of Thailand (IIA))