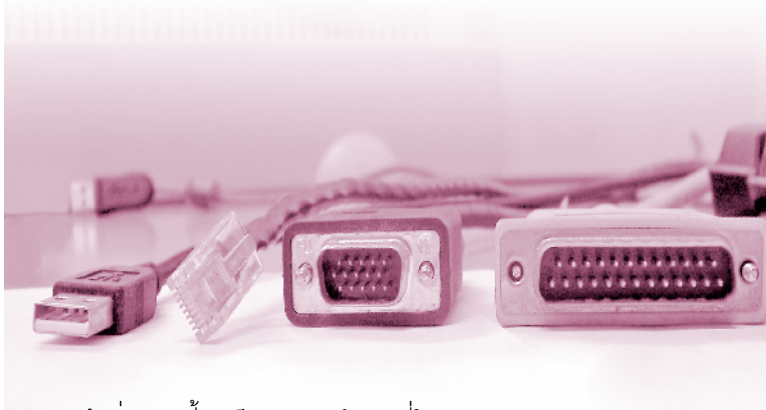
แนวคิด GRC กับการบริหารเทคโนโลยีสารสนเทศขององค์การ

วิชญ์ศุทธ์ เมาะพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ

ในบทความตอนที่ผ่านมา ผมมักจะกล่าวถึงสถานการณ์ แนวโน้มของเทคโนโลยีสารสนเทศที่มีบทบาทต่อองค์การในการพัฒนาศักยภาพ หรือสนับสนุนให้สามารถแข่งขันได้ในตลาดธุรกิจ ตลาดอุตสาหกรรมที่เปิดกว้างขึ้น มีผู้เล่นที่หลากหลาย มีความร่วมมือหรือแข่งขันในมิติของผลประโยชน์ร่วมที่สลับซับซ้อนซึ่งล้วนแล้วแต่ต้องคำนึงถึงปัจจัยต่างๆ ที่ส่งผลกระทบต่อกระบวนงานทางธุรกิจหลักขององค์การ จึงต้องเน้นไปที่การสร้างความเข้มแข็งของรากฐานการพัฒนาศักยภาพในการแข่งขัน โดยเฉพาะการนำเอาเทคโนโลยีสารสนเทศและการสื่อสาร หรือ IT มาใช้เป็นเครื่องมือสนับสนุนที่สำคัญซึ่งขาดไม่ได้ในปัจจุบัน รวมไปถึงแนวทาง และโอกาสในการเลือกใช้ IT อย่างเหมาะสม ตรงตามเป้าประสงค์ เพื่อไม่ให้กลายเป็นภาระขององค์การแทนที่จะใช้เป็นเครื่องมือสนับสนุน และสร้างความได้เปรียบ เหตุเพราะองค์การทางธุรกิจ หรืออุตสาหกรรมนั้น ส่วนใหญ่หากไม่ได้มีความชำนาญหรือเชี่ยวชาญด้าน IT มีการประกอบกิจการที่เกี่ยวข้องกับ IT มีการผลิตสินค้า ผลิตภัณฑ์ วัตถุดิบ ที่เข้าข่ายแล้วละก็ งานด้าน IT จะกลายเป็นภาระที่จำเป็นต้องพึ่งพา และใช้ประโยชน์ในกระบวนการทำงานหลักขององค์การ

จุดสำคัญ คือ ทำอย่างไรให้สามารถบริหารจัดการงานด้าน IT ได้อย่างมีประสิทธิภาพ และไม่เป็นภาระขององค์การ บางกรณี Outsource อาจเป็นคำตอบ แต่บางกรณี การจ้างผู้เชี่ยวชาญ ที่ปรึกษา มีทีม IT ที่มีความสามารถขององค์การเป็นผู้กำกับดูแลเองก็อาจเป็นคำตอบที่เหมาะสม นั่นก็ขึ้นอยู่กับความสำคัญ อยากให้เน้นที่ข้อมูล เพราะระบบสารสนเทศทุกระบบมีพื้นฐานมาจากระบบข้อมูล หากสามารถบริหารจัดการได้อย่างชัดเจนในมิติของเจ้าของข้อมูล ผู้รับผิดชอบ เนื้อข้อมูล ทั้งที่เป็นเอกสาร (กระดาษ) และที่เป็นอิเล็กทรอนิกส์ รวมถึงอื่นๆ ที่เกี่ยวข้อง พร้อมทั้งกำหนดมาตรการกำกับดูแล และควบคุมที่เหมาะสม รวมทั้งสามารถระบุได้ว่าข้อมูลดังกล่าวถูกนำไปใช้ หรือเป็นผลผลิตที่ได้จากกระบวนงานใดขององค์การ จะทำให้สามารถบริหารจัดการข้อมูลขององค์การในทุกส่วนได้อย่างเป็นระบบมีระเบียบแบบแผนที่ชัดเจน หรือตามกลไกที่ควรจะเป็น ในกรณีนี้ อาทิ ข้อมูลบุคคล บุคลากร พนักงาน ข้อมูลด้านงบประมาณ การเงิน บัญชี ข้อมูลลูกค้า คู่ค้า พันธมิตร ข้อมูลการผลิต กระบวนการ เป็นต้น หากสามารถดำเนินการได้ดังที่กล่าวซึ่งเป็นแนวทางของ EA (Enterprise Architect) หรือสถาปัตยกรรมองค์การ ซึ่งมองเพียงผิวเผินแล้วสิ่งเหล่านี้จะเป็นวัตถุดิบสำคัญที่ในการพัฒนาระบบ ERP (Enterprise resource planning) ระบบ HRM (Human resource management) ระบบ CRM (Customer relationship management) ระบบ MIS (Management information system) หรือแม้กระทั่ง ระบบ DSS (Decision support system) ซึ่งมีความชัดเจน และมีเอกภาพ



ดังนั้น สิ่งที่องค์การควรดำเนินการก็คือ การสร้างความชัดเจนและเป็นรูปธรรม (จับต้องได้ สืบค้นได้ ระบุที่มาที่ไปได้) ของข้อมูลที่เกี่ยวข้องในกระบวนงานทางธุรกิจอย่างครบถ้วน และเหมาะสม ตามลำดับความสำคัญ และระดับชั้นความลับ ซึ่งในการบริหารจัดการดังกล่าวมีกรอบแนวในการดำเนินการหลากหลายรูปแบบซึ่งสามารถสืบค้น และอ้างอิงในระดับสากล โดยเฉพาะที่องค์การหลายแห่งทั้งภาครัฐ และเอกชน ทั้งใน และต่างประเทศนำมาใช้กำหนดกรอบการพัฒนา และบริหารจัดการ IT ซึ่งหลายท่านอาจจะมีความคุ้นเคย และเข้าใจในเนื้อหา อาทิ

- EA: Enterprise Architect สำหรับการจัดทำสถาปัตยกรรมองค์การเป็นรากฐานในการสร้างความชัดเจนในมิติต่างๆ โดยเฉพาะด้านข้อมูล และกระบวนงานทางธุรกิจ
- COBIT: Control Objectives for Information and Related Technology ใช้เป็นแนวทางในการกำหนดกรอบนโยบาย แนวทางปฏิบัติ และการควบคุม การพัฒนา และให้บริการด้าน IT ขององค์การ
- COSO: Committee of Sponsoring Organizations of the Tread way Commission ใช้เป็นกลไกในการประเมินและควบคุมการพัฒนาและให้บริการด้าน IT ขององค์การ
- ITIL: IT Infrastructure Library / IT Service Management ใช้เป็นกรอบการบริหารจัดการ การให้บริการงานด้าน IT ขององค์การ
- **มาตรฐาน** ISO/IEC 20000 Series ที่เกี่ยวข้องโดยตรงกับการควบคุมคุณภาพของการพัฒนา และให้บริการด้าน IT ขององค์การ รวมถึงการมีกลไกการรักษาความมั่นคงปลอดภัยในด้านดังกล่าว

นอกจากนี้ยังมีกรอบแนวทางที่ใช้ในทางการบริการจัดการองค์การ อาทิ Balanced Scorecard ที่หลายๆ ท่านมีความคุ้นเคยเป็นอย่างดี การทำ TQM, PMQA เพื่อประเมินคุณภาพ เหล่านี้หากนำมาใช้กับแง่มุมของ IT ดูจะเป็นเรื่องยุ่งยากมีรายละเอียดที่มากมาย และคงเป็นงานที่ไม่ถนัดนักสำหรับนัก IT ขององค์การหรือแม้แต่ผู้บริหารเองก็ตาม ซึ่งบางครั้งอาจคิดว่าต้องทำถึงขนานนั้นด้วย หรือสำหรับองค์การขนาดใหญ่ที่พึ่งพา IT เป็นหลักมีความจำเป็นต้องดำเนินการวางแผนการพัฒนา IT ในระยะ 4-8 ปี เป็นช่วงๆ เพื่อกำหนดทิศทางที่สอดรับกับยุทธศาสตร์ และกลยุทธ์ขององค์การที่ต้องการก้าวไปให้ถึงเป้าประสงค์ และวิสัยทัศน์ โดยมีการนำเอาแนวทาง มาตรฐาน หรือรูปแบบต่างๆ ข้างต้นมาใช้ประกอบการบริหารจัดการเชิงนโยบาย

แล้วแบบนี้พอจะมีแนวคิดการบริหารจัดการงานด้าน IT ที่สามารถทำความเข้าใจได้ง่ายมุ่งเน้นไปที่เฉพาะประเด็นสำคัญที่ต้องดำเนินการ เช่น งานด้านการควบคุมกำกับดูแล มีการสร้างหรือพัฒนาการปฏิบัติที่หยั่งรากลึกลงไปในแง่ของวัฒธรรมองค์การเพื่อให้เกิดการพัฒนาที่ยั่งยืนบ้างหรือไม่ คำตอบคือเมื่อประมาณ 6-7 ปีที่ผ่านมามีการพัฒนาแนวคิดใหม่ที่รวมเอาสิ่งที่ถือว่าเป็นปัจจัย และเป้าประสงค์ที่บ่งชี้ความสำเร็จในการบริหารซึ่งจะเกิดผลอันเป็นรูปธรรม ประกอบด้วย

➲ Governance **หรือธรรมาภิบาล** คือ ความรับผิดชอบของผู้บริหารระดับสูงในการสร้างความโปร่งใสในการดำเนินงานให้สอดคล้องกับนโยบาย โดยกำหนดขั้นตอนการดำเนินงานที่ชัดเจน มีกลไกที่ทำให้สามารถปฏิบัติได้ตามที่กำหนด หากมีข้อผิดพลาดสามารถรู้ได้โดยเร็วสามารถดำเนินการแก้ไขทันท่วงที และสามารถรู้ได้เมื่อมีการละเว้นไม่ดำเนินการ

➲ Risk Management **หรือ การบริหารความเสี่ยง** คือ กระบวนการกำหนดประเด็นความเสี่ยง กำหนดสินทรัพย์เสี่ยง ประเมินค่าความเสี่ยง ระบุค่าความเสี่ยงที่องค์การยอมรับได้ กำหนดกิจกรรมควบคุม และจัดลำดับความสำคัญของกิจกรรมควบคุม เพื่อ “ลด ละ เลิก” ความเสี่ยงในการดำเนินงานขององค์การ

➲ Compliance **หรือ การปฏิบัติตามกฎ กติก** คือ การดำเนินงานให้สอดคล้องกับข้อกำหนดของกฎหมาย และกฎระเบียบต่างๆ ทั้งของหน่วยงานที่กำกับดูแล (ภาครัฐ) และกฎระเบียบขององค์การเอง

เหล่านี้เรียกโดยรวมว่า GRC ซึ่งจะก่อให้เกิดประโยชน์ในมุมของ

➢ การทำให้องค์การแสดงถึงความเป็น *“Good Governance”* หรือมีธรรมาภิบาลในการบริหาร หรือแม้กระทั่งภาพรวมของการประกอบการ

➢ การสร้างความน่าเชื่อถือให้กับองค์การ สินค้า และบริการ

➢ การทำให้องค์การสามารถสร้างคุณค่าเพิ่มในสินค้า และบริการ

➢ การสร้างความได้เปรียบในการแข่งขัน อย่างสร้างสรรค์

➢ การส่งเสริมภาพลักษณ์ที่ดีให้กับองค์การ

➢ การสร้างจิตสำนึกในการปฏิบัติงานที่ดีให้กับพนักงานทุกคน ซึ่งหมายถึงวัฒนธรรมองค์การ

GRC เป็นระบบที่เกี่ยวข้องกับกลยุทธ์ (Strategy) คน (people) กระบวนการ (processes) และเทคโนโลยี (technology) ที่ช่วยขับเคลื่อนองค์การให้

➢ มีความเข้าใจ และจัดลำดับความสำคัญต่อความคาดหวังของผู้มีส่วนได้เสีย (Stakeholders)

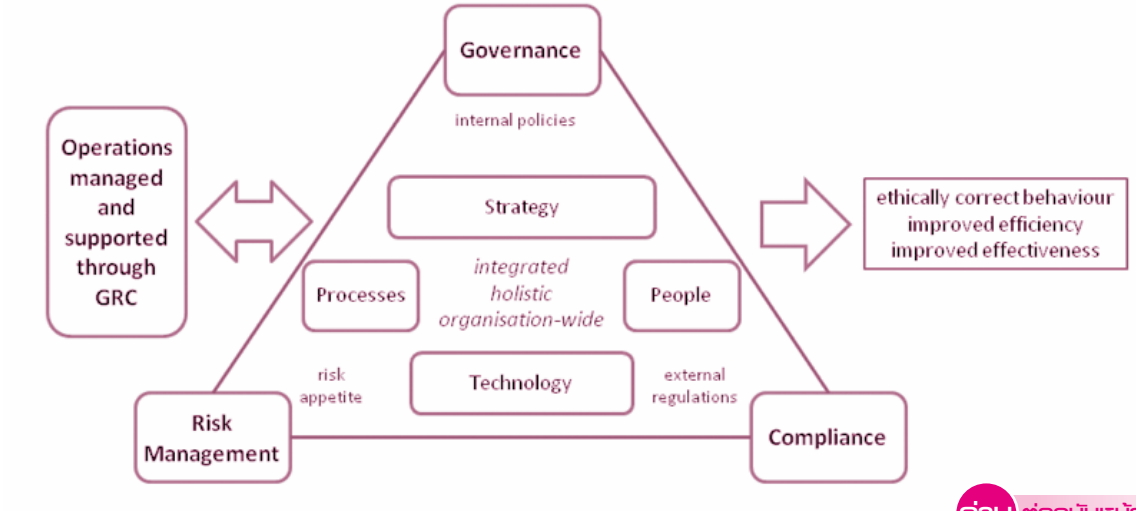
➢ กำหนดวัตถุประสงค์ทางธุรกิจเพื่อให้สอดคล้องกับมูลค่าและความเสี่ยงที่เกี่ยวข้อง

➢ บรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนด และสามารถเพิ่มประสิทธิภาพในการเฝ้าระวังความเสี่ยง (Risk Profile) และปกป้องคุณค่าขององค์การ (Value)

➢ ดำเนินการภายใต้ขอบเขตของกฎหมาย สัญญา ระบบภายใน สังคม และจริยธรรม

➢ ให้ข้อมูลที่เกี่ยวข้อง เชื่อถือได้ และทันเวลา ต่อผู้มีส่วนได้เสีย

➢ ส่งเสริมการวัดผลของระบบการดำเนินงาน และการมีประสิทธิผล



อ่านต่อฉบับหน้า