



**ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ – IT Governance  
และการก้าวสู่แนวการบริหารแบบ GRC  
เพื่อขับเคลื่อน Integrity-Driven Performance**

**โดย : อาจารย์ เมธา สุวรรณสาร**

## ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ – IT Governance และการก้าวสู่แนวการบริหารแบบ GRC เพื่อขับเคลื่อน Integrity-Driven Performance

โดย : อาจารย์ เมธา สุวรรณสาร

### ความหมายของ IT Governance เพื่อการบริหารบางมุมมอง

ธรรมาภิบาลหรือการกำกับดูแลกิจการที่ดีทางด้านเทคโนโลยีสารสนเทศที่ดี (IT Governance) ไม่อาจแยกได้กับการกำกับดูแลกิจการที่ดีขององค์กร (Corporate Governance) ในการขับเคลื่อนองค์กรให้ก้าวไปสู่คุณภาพและศักยภาพของการจัดการที่ดี มีความสามารถในการแข่งขันขององค์กรและของประเทศโดยรวม ความหมายของ IT Governance ขึ้นกับมุมมอง การอธิบาย ดังต่อไปนี้

IT Governance หมายถึง การบริหารคุณภาพของการลงทุน การบริหารการจัดการอย่างเป็นกระบวนการ และการบริหารความเสี่ยงทางด้าน IT กับผลตอบแทนอย่างคุ้มค่าที่จะเกิดขึ้นในมุมมองของ Intangible Asset/Value และ Tangible Asset/Value หรือ

IT Governance หรือ ธรรมาภิบาลทางด้านเทคโนโลยีสารสนเทศ คือ รูปแบบโครงสร้างของความสัมพันธ์และกระบวนการจัดการและการปฏิบัติในองค์กร ที่กำกับและควบคุมองค์กรให้บรรลุถึงเป้าประสงค์ โดยการสร้างมูลค่าเพิ่มให้เกิดขึ้น ในขณะที่เดียวกันก็สามารถสร้างความสมดุลในการจัดการกับความเสี่ยงที่เกิดขึ้นเทียบกับสิ่งที่ได้รับจากเทคโนโลยีสารสนเทศและจากกระบวนการที่เกี่ยวข้อง หรือ

ธรรมาภิบาลทางด้านเทคโนโลยีสารสนเทศ (IT Governance) หมายถึงการใช้เทคโนโลยีสารสนเทศเพื่อจัดการที่ดี ผสมผสานอย่างลงตัวกับความสามารถในการประกอบธุรกิจและองค์ประกอบของการบริหาร โดยทั่วไป 5 ประการ คือ การวางแผน การจัดองค์กร การบริหารบุคลากร การดำเนินการ และการติดตามผล เพื่อเสริมสร้างการบรรลุเป้าหมายและวัตถุประสงค์อย่างมีคุณภาพในระดับประเทศ ในระดับองค์กรและในระดับสายงานต่างๆ อย่างสอดคล้องประสานและลงตัว หรือ

ธรรมาภิบาลทางด้านเทคโนโลยีสารสนเทศ (IT Governance) ก็คือ กระบวนการและการจัดการที่ดี มีคุณภาพและได้คุณภาพระหว่างองค์ประกอบของการบริหารองค์กร 5 ประการคือ การวางแผน การจัดองค์กร การบริหารทรัพยากร การดำเนินการ และการติดตามผลให้มีความสอดคล้องกับกระบวนการและศักยภาพของ

เทคโนโลยีสารสนเทศในมิติต่าง ๆ เพื่อสร้างมูลค่าเพิ่ม และความสามารถทางการแข่งขันในการบรรลุถึงนโยบาย พันธกิจ เป้าหมาย กลยุทธ์ แผนงานและโครงการต่าง ๆ ระดับองค์กรหรือระดับประเทศ

## หน้าที่การบริหาร IT Governance

IT Governance เช่นเดียวกับ Corporate Governance เป็นหน้าที่และความรับผิดชอบเกี่ยวกับการจัดการที่ดีทางด้านเทคโนโลยีสารสนเทศควบคู่กันไปกับความสามารถด้านอื่น ๆ ของคณะกรรมการและผู้บริหารระดับสูงที่ใช้เป็นกรอบ และองค์ประกอบของกระบวนการบริหารงานในการปฏิบัติตามนโยบาย กลยุทธ์เพื่อสร้าง ศักยภาพ คุณค่าเพิ่ม และการเติบโตอย่างยั่งยืนอย่างรู้คุณค่าให้กับองค์กรควบคู่กันไปกับหลักการกำกับดูแลกิจการที่ดีที่แยกกันไม่ได้ ในกระบวนการบริหารความเสี่ยงตามองค์ประกอบของการจัดการตั้งแต่ การวางแผน การจัดองค์กร การจัดพนักงาน การดำเนินการและการควบคุม

IT Governance ทำให้เกิดการบริหารและการบูรณาการที่เป็นระบบ มีระเบียบ เป็นขั้นตอน ลดความซ้ำซ้อน ลดความเสี่ยง เพิ่มศักยภาพโดยทำงานข้ามสายงานได้ และประสานงานระหว่างองค์กรได้อย่างรวดเร็วทันเวลา มีประสิทธิภาพสอดคล้องประสานกับ การดำเนินงานระดับต่าง ๆ จากการใช้ความสามารถและศักยภาพของเทคโนโลยีสารสนเทศ และทรัพยากรต่าง ๆ เพื่อการผลักดันความสำเร็จ ของการจัดการทั่วทั้งองค์กรอย่างเป็นกระบวนการ

เทคโนโลยีสารสนเทศสร้างความเสี่ยงใหม่ ๆ การสูญเสียโอกาสที่มีผลต่อประสิทธิภาพ ประสิทธิภาพในการดำเนินการ การปฏิบัติตามนโยบาย กฎหมาย ระเบียบ ประกาศ คำสั่ง ฯลฯ รวมทั้งผลกระทบต่อความน่าเชื่อถือและความถูกต้องของการตรวจสอบและการจัดทำรายงาน ซึ่งเป็นหัวใจของการบริหารและการควบคุมภายในอย่างคาดไม่ถึงในการบริหารงานระดับต่าง ๆ ขององค์กรควบคู่กันไปด้วย ดังนั้นการผสมผสานความสามารถด้านต่าง ๆ ขององค์กรกับศักยภาพของระบบงานและการจัดการเทคโนโลยีสารสนเทศที่ดี จึงเป็นทั้งหน้าที่ความรับผิดชอบที่ไม่อาจหลีกเลี่ยงได้ของคณะกรรมการและผู้บริหารระดับสูงขององค์กรในปัจจุบัน

สารสนเทศขององค์กรต้องสามารถตอบสนองความต้องการด้านคุณภาพ ความน่าเชื่อถือ และการรักษาความปลอดภัย เช่นเดียวกับสินทรัพย์อื่น ๆ ผู้บริหารควรเข้าใจถึงสถานะภาพของของระบบเทคโนโลยีสารสนเทศของตน และตัดสินใจว่าควรมีการดำเนินการควบคุมและสร้างศักยภาพอย่างไร จึงจะเหมาะสมอย่างผสมผสานกับธุรกิจเพื่อบรรลุเป้าหมายอย่างมีประสิทธิภาพสูงสุดขององค์กร ทั้งนี้โดยคำนึงถึงคุณลักษณะสารสนเทศที่ดีและความสามารถในการบริหารทรัพยากรเทคโนโลยีสารสนเทศ

การพัฒนาระบบงานต่าง ๆ ขององค์กรส่วนใหญ่จะมีเทคโนโลยีสารสนเทศเข้ามาเกี่ยวข้องด้วยเสมอ ในยุคของการค้าเสรีและเศรษฐกิจยุคใหม่ ซึ่งการมีการใช้เทคโนโลยีสารสนเทศได้เปลี่ยนโครงสร้างการดำเนินการ และการปฏิบัติงานในระดับหลัก ๆ ขององค์กรซึ่งทวีความซับซ้อนในการปฏิบัติงานตามหลักการกำกับดูแลกิจการที่ดี (Good Corporate Governance) ซึ่งในกระบวนการดังกล่าว มี IT Governance เป็นส่วนหนึ่งขององค์รวมในการบริหารความเสี่ยง การควบคุม และการตรวจสอบโดยใช้ฐานความเสี่ยง (Risk –Based Audit) อยู่ด้วย

ความสำเร็จในการดำเนินงานไปสู่เป้าหมายและวัตถุประสงค์หลักขององค์กรอย่างยั่งยืนนั้น ย่อมต้องการแนวความคิดในรูปแบบใหม่ที่ต้องอาศัยการปรับปรุงและพัฒนาองค์กรให้เหมาะสมกับสภาพแวดล้อมใหม่ของโลกแห่งการเปลี่ยนแปลงและความก้าวหน้าทางเทคโนโลยีสารสนเทศที่อาจจะเป็นปัญหาจากระบบงานมีจุดอ่อน และเป็นปัจจัยหนึ่งที่จะเกิดความเสียหายกับองค์กรจากการทุจริตได้

ศักยภาพที่เพิ่มขึ้นของเทคโนโลยีที่ขับเคลื่อนการเปลี่ยนแปลงกระบวนการทำงานที่เกิดขึ้นในองค์กรรวมทั้งปรับเปลี่ยนหลักการ การจัดการและการปฏิบัติงาน ซึ่งก่อให้เกิดโอกาสทางธุรกิจใหม่ ๆ และช่วยให้ต้นทุนและกระบวนการจัดการขององค์กรลดลงด้วย ดังนั้น ความเข้าใจในเรื่อง IT Governance และการบริหารความเสี่ยงที่เกี่ยวข้อง ที่มีผลโดยรวมต่อการบริหารทั่วทั้งองค์กร จึงเป็นสิ่งจำเป็นอย่างยิ่งในยุคของการแข่งขันที่รุนแรงซึ่งก่อให้เกิดการเปลี่ยนแปลงขององค์กรในด้านต่าง ๆ ไม่ว่าจะเป็นการปรับเปลี่ยนระบบและกระบวนการทำงานให้กระชับขึ้น โดยนำเทคโนโลยีสารสนเทศมาช่วยในการปรับปรุงเพื่อเพิ่มความสามารถในการแข่งขันมากขึ้น มีการปรับขนาดขององค์กรให้กระชับและมีความเหมาะสม มีการใช้บริการจากภายนอกมากขึ้น มีการกระจายอำนาจและปรับโครงสร้างองค์กรให้เป็นแนวราบมากขึ้น สิ่งเหล่านี้มีผลกระทบต่อการทำงานทั้งขององค์กรเอกชน และองค์กรของรัฐบาล โดยเฉพาะการเน้นไปที่การได้เปรียบในด้านการแข่งขัน และการเกิดประสิทธิภาพด้านต้นทุน ซึ่งเป็นผลให้แต่ละองค์กรจำเป็นต้องพึ่งพาเทคโนโลยีมากขึ้น และกลายเป็นยุทธศาสตร์ที่สำคัญขององค์กร

สิ่งเหล่านี้ทำให้หลายองค์กรมองเห็นความสำคัญของ Information และ เทคโนโลยีที่พัฒนา อันถือได้ว่าเป็นสินทรัพย์ที่มีค่ายิ่ง โดยเฉพาะในโลกของการแข่งขันที่รุนแรง ผู้บริหารจะให้ความสำคัญและความคาดหวังกับเทคโนโลยีมากยิ่งขึ้นโดยเฉพาะการตอบสนองที่รวดเร็ว มีคุณภาพ สามารถใช้งานได้หลากหลาย และสะดวกต่อการใช้งาน โดยใช้เวลาน้อยลง เพิ่มระดับการบริการให้ดียิ่งขึ้น โดยมีต้นทุนที่ต่ำลง

องค์กรที่มีการปฏิบัติงานในระบบอัตโนมัติจำเป็นต้องมีกลไกในการบริหารความเสี่ยงและการควบคุมที่ดี ยิ่งขึ้น โดยเฉพาะการควบคุมทั้งระบบคอมพิวเตอร์ และ ระบบเครือข่าย ทั้งในด้านของ Hardware และ Software ซึ่งระบบการควบคุมจำเป็นต้องพัฒนาไปพร้อมกับการพัฒนาของเทคโนโลยีที่เกิดขึ้นอย่างรวดเร็วและเป็นไปแบบก้าวกระโดด

หลายองค์กรได้สังเกตเห็นถึงประโยชน์ที่จะได้รับจากเทคโนโลยี และสำหรับองค์กรที่ประสบความสำเร็จก็มีความเข้าใจและสามารถบริหารความเสี่ยงที่มาพร้อมกับการนำเทคโนโลยีมาใช้ได้เป็นอย่างดี โดยเฉพาะการเปลี่ยนแปลงทางด้านเทคโนโลยีสารสนเทศได้เกิดมากขึ้นเป็นลำดับและรวดเร็ว จึงจำเป็นต้องมีการจัดการความเสี่ยงที่มาพร้อมกับการเปลี่ยนแปลงนี้ให้ดียิ่งขึ้น ไม่ว่าจะเป็นการจัดการกับข้อมูลที่เปิดเผย และข้อมูลที่เป็นความลับ รวมทั้งการนำข้อมูลไปใช้กระทำการที่ผิดกฎหมาย

*ดังนั้นการบริหารความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศจึงกลายมาเป็นส่วนสำคัญในการกำกับดูแลกิจการที่ดีขององค์กร (Corporate Governance) อย่างแยกกันไม่ได้ และความเข้าใจในเรื่อง Risk IT และ IT Risk ก็เป็นปัจจัยสำคัญยิ่งอย่างหนึ่งในการบริหาร Governance เพื่อการเติบโตอย่างยั่งยืนของทุกองค์กร ในภาพโดยรวมก่อนก้าวสู่ GRC*

ความต้องการในการมีกรอบมาตรฐาน สำหรับการจัดการเรื่องความปลอดภัย (Security) และการควบคุมทางด้านเทคโนโลยีสารสนเทศมีค่อนข้างมาก โดยเฉพาะองค์กรที่ประสบความสำเร็จต่างๆ ได้มีความเข้าใจ และประเมินค่าของความเสี่ยงเทียบกับข้อจำกัดในการใช้เทคโนโลยีสารสนเทศในทุกระดับขององค์กรเพื่อให้มั่นใจว่าองค์กรจะสามารถมีการกำกับดูแลที่มีประสิทธิผล และมีการควบคุมที่เพียงพอ

ถึงแม้การรักษาความปลอดภัยและการควบคุมทางด้านเทคโนโลยีสารสนเทศจะช่วยในการบริหารความเสี่ยงขององค์กรอย่างสำคัญ แต่ความเสี่ยงก็ยังคงมีอยู่ ไม่ได้ถูกขจัดออกไปทั้งหมดเพราะไม่มีใครสามารถกำหนดระดับความเสี่ยงได้ชัดเจนแน่นอน ดังนั้นผู้บริหารจึงต้องกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ในกระบวนการบริหาร โดยเปรียบเทียบกับต้นทุนที่ต้องลงทุน และผลประโยชน์ที่จะได้รับในมุมมองต่างๆ ซึ่งถือได้ว่าเป็นการตัดสินใจที่ค่อนข้างยาก เช่นมุมมองของการกำกับดูแลกิจการที่ดี การส่งเสริมการปฏิบัติที่ดี เป็นมาตรฐาน (Best Practice) ด้านต่างๆ เพื่อก้าวสู่มาตรฐานสากล การขับเคลื่อนองค์กรไปสู่เป้าประสงค์ของผู้กำกับต่างๆ เป็นต้น

ดังนั้น องค์กรจึงจำเป็นต้องมีกรอบมาตรฐาน เพื่อให้ทราบถึงระดับการยอมรับได้ในการรักษาความปลอดภัยและการควบคุมอย่างเป็นกระบวนการทางด้าน IT และ Non-IT ที่เกี่ยวข้อง ที่เป็นหลักปฏิบัติทั่วไป เพื่อเทียบวัดกับสถานะของเทคโนโลยีสารสนเทศในปัจจุบันและที่จะเป็นไปในอนาคต

ความก้าวหน้าของเทคโนโลยีในปัจจุบันไม่เพียงจะป้องกันการบุกรุกหรือการเข้าถึงข้อมูลจากบุคคลภายนอกเท่านั้น แต่ยังมีแนวทางใหม่ๆที่สามารถติดตามการกระทำ และป้องกันบุคคลากรจากภายในองค์กรที่สามารถสร้างปัญหาที่เกี่ยวข้องกับการทุจริต หรือกระทำผิดระเบียบได้เป็นการล่วงหน้า ก่อนองค์กรจะมีปัญหาและมีความเสียหายเกิดขึ้นจริง ตามที่ปรากฏเป็นข่าวอยู่เสมอ โดยเฉพาะสถาบันการเงิน เนื่องจาก การกระทำมิชอบต่างๆเกิดจากสาเหตุเพียง 3 ประการ คือ

- 1) ระบบงานมีจุดอ่อน และ
- 2) มีบุคลากรหรือพนักงานต้องการที่จะทุจริต หรือละเมิดกฎเกณฑ์ที่กำหนด และ
- 3) มีโอกาสที่จะดำเนินการมิชอบต่างๆได้

ดังนั้น ตามหลักการของการบริหารความเสี่ยงที่ดี คือ การป้องกันปัญหาก่อนที่จะเกิดปัญหา โดยการพิจารณาหรือชี้ปัญหาที่เป็นสาเหตุที่อาจจะเกิดขึ้นและออกระเบียบ กฎเกณฑ์ที่เหมาะสมมิให้มีการกระทำการละเมิดกฎเกณฑ์หรือสามารถที่จะรู้การละเมิดกฎเกณฑ์ได้อย่างเป็นรูปธรรม ถึงแม้หลายหน่วยงานจะมี Compliance Unit ดูแลในเรื่องนี้ แต่ก็ไม่มีศักยภาพเพียงพอที่จะติดตามรายการต่าง ๆ ผ่านระบบเทคโนโลยีสารสนเทศได้ทัน

ผู้กำกับและผู้ดูแลการปฏิบัติตามกฎเกณฑ์ของหลายองค์กร จึงให้ความสนใจการใช้โปรแกรมเข้าช่วยควบคุม หรือช่วยกำกับดูแลการปฏิบัติที่ไม่อาจยอมรับได้นี้เป็นกระบวนการต่อเนื่อง ที่ช่วยฝ่ายบริหาร ฝ่ายปฏิบัติการ สายงาน Compliance Unit สายงานด้าน เทคโนโลยีสารสนเทศ และสายงานตรวจสอบภายในขององค์กรต่าง ๆ ปฏิบัติงานได้อย่างมีประสิทธิภาพมากขึ้น ทั้งนี้ รวมทั้งหน่วยงานที่เกี่ยวข้องกับการดูแลความมั่นคงของชาติ ก็ได้ใช้แนวทางนี้ในการติดตามพฤติกรรม ทั้งทางการเงินและมีช่องทางการเงิน ร่องรอย(Trail) ที่ช่วยวิเคราะห์ความผิดปกติ ที่อาจประเมินค่าหรือระบุความหมาย ที่มีนัยสำคัญ เพื่อการจัดการที่เหมาะสม เพื่อความเกี่ยวพันกับเสถียรภาพทางด้านต่าง ๆ ตามที่องค์กรหรือหน่วยงานกำหนดเป้าประสงค์ในลักษณะการบริหารเชิงรุก เพื่อการจัดการที่มีคุณภาพไว้ได้

ในระดับของผู้ใช้งาน ก็ต้องมีความมั่นใจว่ามีการรักษาความปลอดภัยและการควบคุม อย่างเพียงพอในการใช้งานด้านเทคโนโลยีสารสนเทศไม่ว่าจะเป็นการใช้บริการจากภายในองค์กร หรือจากผู้ให้บริการจาก

ภายนอก ซึ่งที่ผ่านมากการควบคุมทางด้านเทคโนโลยีสารสนเทศจะค่อนข้างซับซ้อนเนื่องจากมีการประเมินมาตรฐานหลายวิธีการจากหลายองค์กร การประเมินการควบคุมภายใน ดังนั้นผู้ใช้งจึงจำเป็นต้องมีหลักเบื้องต้นเพื่อยึดเป็นแนวทาง

ในส่วนของผู้ตรวจสอบ จำเป็นจะต้องมีมาตรฐานสากลในการตรวจสอบเนื่องจากจะต้องมีจุดยืนในการให้แนวคิดและเหตุผลเกี่ยวกับการตรวจสอบภายในกับระดับบริหาร ซึ่งถ้าปราศจากกรอบมาตรฐานแล้วจะหาจุดพิจารณาถึงระดับการรักษาความปลอดภัยและการควบคุม ด้านเทคโนโลยีสารสนเทศที่เหมาะสมได้ค่อนข้างยาก

### ความสำคัญของ IT Governance

IT Governance มีความสำคัญโดยสรุป ดังนี้

1. ความจำเป็นที่ต้องมีการควบคุมการจัดการ และการใช้เทคโนโลยีสารสนเทศ เพื่อการบรรลุกลยุทธ์และเป้าหมายขององค์กร

ความก้าวหน้าในการพัฒนาเทคโนโลยีสารสนเทศมาก ทำให้ข้อมูลสามารถส่งผ่านถึงผู้รับได้อย่างรวดเร็วโดยปราศจากข้อจำกัดด้านเวลา ระยะทางและความรวดเร็ว องค์กรที่มีการปฏิบัติงานในระบบอัตโนมัติ จำเป็นต้องมีกลไกในการควบคุมที่ดียิ่งขึ้น โดยเฉพาะการควบคุมทั้งระบบคอมพิวเตอร์ และระบบเครือข่าย ทั้งในด้านของ Hardware และ Software ซึ่งระบบการควบคุมจำเป็นต้องพัฒนาไปพร้อมกับการพัฒนาของเทคโนโลยีที่เกิดขึ้นอย่างรวดเร็วและเป็นไปแบบก้าวกระโดด จึงจำเป็นต้องมีการจัดการความเสี่ยงที่มาพร้อมกับการเปลี่ยนแปลงนี้ให้ดียิ่งขึ้น ไม่ว่าจะเป็นการจัดการกับข้อมูลที่เปิดเผย และข้อมูลที่เป็นความลับ รวมทั้งการนำข้อมูลไปใช้กระทำการที่ผิดกฎหมาย ดังนั้นการบริหารความเสี่ยงที่เกี่ยวข้องของเทคโนโลยีสารสนเทศจึงกลายมาเป็นส่วนสำคัญในการกำกับดูแลกิจการที่ดีขององค์กร (Corporate Governance)

ผู้บริหารจะต้องสามารถตัดสินใจได้ว่าควรจะลงทุน ณ ระดับใดในเรื่องการรักษาความปลอดภัยและการควบคุม และจะรักษาจุดสมดุลอย่างไรระหว่างความเสี่ยงที่รับได้กับการลงทุนในด้านการควบคุมและผลตอบแทน

## 2. ความจำเป็นของการควบคุมและกำกับทางด้าน เทคโนโลยีสารสนเทศ ตามกฎหมายที่ยอมรับในระดับสากลกับบริษัทในตลาดหลักทรัพย์

องค์กรต่าง ๆ ที่อยู่ในตลาดหลักทรัพย์ในสหรัฐฯ จำเป็นต้องให้ความสำคัญกับการควบคุมและการประมวลผลข้อมูลโดยมีการระบุในกฎหมาย Sarbanes-Oxley Act, 2002 ใน section 404 ที่กล่าวถึง “Management’s Report on Internal Controls over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports” ว่ารายงานของการควบคุมภายในจะต้องครอบคลุมเนื้อหา ดังนี้

2.1. การระบุความรับผิดชอบของผู้บริหารที่มีต่อการจัดการให้มีการควบคุมภายในในการจัดทำรายงานทางการเงินขององค์กร

2.2. การตรวจสอบของผู้บริหารถึงความถูกต้องและความมีประสิทธิภาพในการควบคุมภายในของการจัดทำรายงานทางการเงินขององค์กร ณ วันสิ้นสุดรอบการเงิน

2.3. การระบุถึงกรอบการจัดการในการประเมินความถูกต้องและความมีประสิทธิภาพในการควบคุมภายในของการจัดทำรายงานทางการเงินขององค์กร

2.4. การตรวจรับรองโดยบริษัทตรวจสอบบัญชีและรายงานถึงการตรวจสอบของผู้บริหารถึงความถูกต้อง และความมีประสิทธิภาพในการควบคุมภายใน ของการจัดทำรายงานทางการเงินขององค์กร ซึ่งการใช้ข้อมูลโดยพึ่งพาเทคโนโลยีสารสนเทศเป็นสิ่งจำเป็น การมีการควบคุมที่ดีในการจัดการข้อมูล รวมทั้งการควบคุมคุณภาพและการรักษาความปลอดภัยในการเข้าถึงข้อมูล จึงมีความสำคัญอย่างยิ่ง โดยปกติการเซ็นชื่อรับรองงบการเงินซึ่งมิใช่การสอบบัญชีนั้น จะกระทำโดย CEO และ CFO แต่ปัจจุบันเริ่มมีหลายองค์กรให้ CIO เซ็นชื่อร่วมด้วย โดยให้ความสำคัญกับ Technology Support เพื่อให้ได้มาซึ่งรายงานทางการเงินที่เชื่อถือได้ เป็นข้อหนึ่งของเป้าประสงค์หลักใน 4 ข้อ ในเรื่องการควบคุมทางด้าน Reporting ต่าง ๆ รวมทั้งรายงานที่เกี่ยวกับการเงิน (Financial – F) นั่นเอง

### การสร้างวิสัยทัศน์โดยการมองการสร้างมูลค่าเพิ่มในระยะยาว

#### 1. การสร้างมูลค่าเพิ่ม

การสร้างมูลค่าเพิ่มให้กับกิจการจะต้องเน้นไปในแนวทางการสร้างกำไรและเพิ่มมูลค่าให้กับกิจการ ทั้งนี้จะต้องกระทำภายใต้กรอบจริยธรรมที่ดี โดยคำนึงถึงผู้มีส่วนได้ส่วนเสียทุกฝ่าย เพื่อประโยชน์ส่วนรวม อีกทั้งต้องกระทำอย่างต่อเนื่อง เพื่อให้เจ้าของกิจการ/ผู้ถือหุ้น และนักลงทุน มีความเชื่อมั่นต่อผลการดำเนินงานในปัจจุบันและอนาคต

## 2. การมีวิสัยทัศน์

องค์ประกอบหนึ่งที่จะช่วยสร้างความเชื่อมั่นให้แก่ผู้ที่เกี่ยวข้อง ว่ากิจการมีการวางแผนสอดคล้องกับการเปลี่ยนแปลงในอนาคตเพื่อความมั่นคงและก้าวหน้าในระยะยาว สามารถแข่งขันได้ คือ การมีวิสัยทัศน์ของกิจการให้สอดคล้องกับเทคโนโลยีและสภาพเศรษฐกิจที่เปลี่ยนแปลงไป เมื่อมีวิสัยทัศน์ที่ถูกต้องแล้ว ก็จะส่งผลให้การลงทุน ทั้งในระยะยาวและระยะสั้นบรรลุตามเป้าหมาย เป็นเหตุให้การเพิ่มมูลค่ากิจการเป็นผลตามมา

การสร้างมูลค่าเพิ่มในระยะยาวและการสร้างวิสัยทัศน์ที่ดีจะต้องมีข้อปฏิบัติ ดังนี้

- 1) กำหนดทิศทางของกิจการในระยะเวลาหนึ่ง ๆ และประเมินผลอย่างต่อเนื่อง
- 2) ปรับเปลี่ยนกลยุทธ์อย่างรอบคอบโดยฉับพลัน เมื่อผลประกอบการไม่ประสบความสำเร็จดังที่วางแผนไว้

### ปัจจัยแห่งความสำเร็จและแนวความคิดทางด้าน IT Governance บางประการ

#### 1. จุดมุ่งหมายของการประกอบธุรกิจที่ดีด้วย Information Technology (IT)

- 1.1. สามารถลดต้นทุนและเพิ่มประสิทธิภาพในการดำเนินกิจการ
- 1.2. สร้างแนวทางในการหารายได้ใหม่ ๆ
- 1.3. สนองตอบความต้องการขององค์กร
- 1.4. สร้างมูลค่าเพิ่มให้กับองค์กร
- 1.5. สร้างรูปแบบใหม่ในการดำเนินธุรกิจขององค์กร
- 1.6. สร้างความสามารถในการแข่งขันด้วย IT Governance

#### 2. ปัจจัยแห่งความสำเร็จ

- 2.1. ควรคำนึงถึงตลอดเวลาว่า IT เป็นส่วนหนึ่งขององค์กรและในการกำหนดวิสัยทัศน์ พันธกิจ นโยบาย เป้าหมาย กลยุทธ์ แผนงาน โครงการและการติดตามผล
- 2.2. การดำเนินงานด้าน IT เป็นส่วนหนึ่งของการกำกับดูแลกิจการที่ดี (Good Corporate Governance)
- 2.3. รับรู้ปัญหาทางด้าน IT และวิธีการที่ฝ่ายจัดการว่าจ้างผู้เชี่ยวชาญจากภายนอกเข้ามาช่วยแก้ไขปัญหา รวมทั้งความเสี่ยงคงเหลือขององค์กรที่บุคลากรโดยเฉพาะผู้บริหารควรมีความรู้และศักยภาพทางด้าน IT
- 2.4. การกำหนดวัตถุประสงค์ รายละเอียด การนำ IT ไปใช้ ควรมีพื้นฐานมาจากความต้องการขององค์กร ด้วยความคิดที่เป็นระบบและมีขั้นตอน

- 2.5 ควรพิจารณาแต่งตั้งสมาชิกในคณะกรรมการตรวจสอบอย่างน้อย 1 คนที่มีความรู้การบริหารด้าน IT และความเสี่ยงด้าน IT รวมทั้ง IT Governance
- 2.6 ทรัพยากรทางด้าน IT ขององค์กรสามารถทำงานร่วมกับองค์กรอื่นได้เป็นอย่างดี องค์กรอาจถูกผลักดันจากพันธมิตร หรือคู่ค้าทางด้าน IT เพื่อการแลกเปลี่ยนและนำส่งข้อมูลระหว่างกันในระดับองค์กรและระดับประเทศ
- 2.7 เป้าหมายและการดำเนินการตามกลยุทธ์ ควรนำเทคโนโลยีมาใช้เพื่อเป็นการใช้ทรัพยากรที่มีอยู่อย่างคุ้มค่าและมีความสามารถที่จะตอบสนองของความต้องการขององค์กรได้อย่างมีคุณภาพสูงสุด
- 2.8 การสื่อสารระหว่างฝ่ายจัดการและผู้ตรวจสอบ เพื่อสร้างวัฒนธรรมการทำงานใหม่ ๆ ควรเป็นไปอย่างสะดวก ไม่มีขั้นตอนที่ยุ่งยากเพราะ IT สามารถเปลี่ยนวัฒนธรรมและสร้างความโปร่งใสที่ควบคุมและตรวจสอบได้ในระดับหนึ่งอย่างน่าพอใจ
- 2.9 ระเบียบวิธีปฏิบัติที่ถูกกำหนดขึ้น ควรเป็นความเห็นร่วมกันระหว่างฝ่ายจัดการและคณะกรรมการขององค์กรและเป็นไปตามกฎหมายที่เกี่ยวข้องและลงนามโดยฝ่ายจัดการ
- 2.10 กลยุทธ์การจัดการที่กำหนดให้มีขึ้น ควรคำนึงถึงวัตถุประสงค์ของ IT ได้แก่ กลยุทธ์ทางด้าน IT ที่ควรสอดคล้องกับกลยุทธ์สู่เป้าหมายต่าง ๆ ระดับต่าง ๆ ขององค์กรระหว่างองค์กรและระหว่างประเทศ ระยะเวลาการส่งมอบการบริหารความเสี่ยงและประสิทธิภาพการบริหาร โดยผู้บริหารและผู้ปฏิบัติงานควรมีความเข้าใจในเรื่อง IT
- 2.11 กลไกในการใช้ IT Governance เป็นตัวผลักดันประสิทธิภาพและการจัดการที่ดี
- 2.12 ความถี่ของการรายงานจุดควบคุมความเสี่ยงและข้อเสนอแนะต่อคณะกรรมการขององค์กร
- 2.13 การลดต้นทุนค่าใช้จ่าย การเพิ่มประสิทธิภาพของกระบวนการปฏิบัติงานทางด้าน IT โดยการเชื่อมโยงระบบต่าง ๆ เข้าด้วยกัน โดยมีมาตรฐานเดียวกัน
- 2.14 สร้างความหลากหลายและโอกาสใหม่ ๆ ในการประกอบธุรกิจโดยใช้ IT
- 2.15 เพิ่มอรรถประโยชน์ของทรัพยากรด้าน IT ที่มีอยู่
- 2.16 เพิ่มความพึงพอใจให้แก่พนักงานผู้มีประโยชน์ร่วมกันทุกฝ่าย
- 2.17 ปรับปรุงวิธีการทำงานและความรับผิดชอบของผู้ปฏิบัติงานที่มีส่วนเกี่ยวข้องกับ IT ทั้งทางตรงและทางอ้อม
- 2.18 เพิ่มพูนความรู้ด้าน IT ให้แก่ฝ่ายจัดการและผู้ปฏิบัติงาน
- 2.19 เพิ่มความเชื่อมโยงระหว่าง IT กับการกำกับดูแลกิจการที่ดี

2.20 เพิ่มศักยภาพของกระบวนการบริหาร (Management Process) และการปฏิบัติงานตามที่ได้รับวัดได้จาก Management Tools ต่าง ๆ

2.21 กำหนดมาตรฐานการปฏิบัติงาน และเปรียบเทียบกับมาตรฐานการกำกับดูแลกิจการที่ดี

### 3. กลไกในการใช้ IT Governance เป็นตัวผลักดันประสิทธิภาพและการจัดการที่ดี

3.1. ความถี่ของการรายงานจุดควบคุมความเสี่ยงและข้อเสนอแนะต่อคณะกรรมการขององค์กร

3.2. การลดต้นทุนค่าใช้จ่าย การเพิ่มประสิทธิภาพของกระบวนการปฏิบัติงานทางด้าน IT โดยการเชื่อมโยงระบบต่าง ๆ เข้าด้วยกัน

3.3. สร้างความหลากหลายในการประกอบธุรกิจด้วย IT

3.4. เพิ่มอรรถประโยชน์ของทรัพยากรทางด้าน IT ที่มีอยู่

3.5. เพิ่มความพึงพอใจให้แก่พนักงานผู้มีผลประโยชน์ร่วมทุกฝ่าย

3.6. ปรับปรุงวิธีการทำงานและความรับผิดชอบของผู้ปฏิบัติงานที่มีส่วนเกี่ยวข้องกับ IT ทั้งทางตรงและทางอ้อม

3.7. เพิ่มพูนความรู้ทางด้าน IT ให้แก่ฝ่ายจัดการและผู้ปฏิบัติงาน

3.8. เพิ่มความเชื่อมโยงระหว่าง IT กับการกำกับดูแลกิจการที่ดี

3.9. เพิ่มศักยภาพของกระบวนการบริหาร (Management Process) และการปฏิบัติงานตามที่ได้รับวัดได้จาก Management Tools ต่าง ๆ

3.10. กำหนดมาตรฐานการปฏิบัติงาน และเปรียบเทียบกับมาตรฐานการกำกับดูแลกิจการที่ดี

### 4. แนวความคิดที่ปฏิบัติจริงได้ จากการวัดประสิทธิภาพการบริหารด้าน IT และการใช้ IT Governance ในระดับสายงานต่าง ๆ อย่างสอดคล้องทั่วทั้งองค์กร

4.1. ทำอย่างไร IT จึงจะสามารถเพิ่มประสิทธิภาพและลดต้นทุนในการจัดการ

4.2. ทำอย่างไร IT จึงจะให้คำแนะนำเกี่ยวกับนวัตกรรมและการบริการใหม่ ๆ ได้อย่างรวดเร็ว และลดความซ้ำซ้อนในการปฏิบัติงาน

4.3. ทำอย่างไร IT จึงจะช่วยเพิ่มผลตอบแทนจากการลงทุนได้มากขึ้น

4.4. ทำอย่างไร IT จึงสามารถกำหนดมาตรฐานการปฏิบัติงานขององค์กรได้

4.5. ทำอย่างไร IT ช่วยองค์กรเพิ่มลูกค้าใหม่และสร้างความพอใจให้กับลูกค้าได้

4.6. ทำอย่างไร IT จึงจะสนองตอบความต้องการและความคาดหวังของผู้มีผลประโยชน์ร่วมขององค์กรได้ ภายใต้งบประมาณที่ได้รับและเวลาที่กำหนด

- 4.7. ทำอย่างไร IT จึงจะช่วยองค์กรให้ปฏิบัติงานได้อย่างถูกต้องตามกฎหมายระเบียบ ข้อบังคับ หรือตามสัญญา
- 4.8. ทำอย่างไร IT จึงจะช่วยให้องค์กรบริหารความเสี่ยงที่มีอยู่อย่างโปร่งใส
- 4.9. ทำอย่างไร IT จึงจะช่วยองค์กรในการสร้างช่องทางการบริการใหม่ ๆ
- 4.10. ทำอย่างไร IT จึงจะช่วยฝ่ายจัดการสร้างผลตอบแทนให้แก่องค์กรในอัตราที่สูงขึ้น บริหารงาน และปฏิบัติงานได้รวดเร็วยิ่งขึ้น

### ความคาดหวังของคณะกรรมการและผู้บริหารต่อการมีการใช้ IT และ IT Governance

1. ปรับหรือปรับปรุง กระบวนการปฏิบัติงานระดับต่าง ๆ ให้สอดคล้องกับการทำงานของโปรแกรมประยุกต์ และประสิทธิภาพของ IT อย่างแท้จริง โดยเฉพาะอย่างยิ่ง การลดความซ้ำซ้อนในการปฏิบัติงาน และมีความสัมพันธ์กับโครงสร้างองค์กรอย่างเหมาะสม
2. จัดโครงสร้างขององค์กรให้มีขนาดกะทัดรัดในแนวราบให้มากและเหมาะสมกับ Organizational Governance Process<sup>1</sup> และโปรแกรมประยุกต์ทั่วทั้งองค์กร
3. จัดให้มีระบบที่มีลักษณะเป็น “Automated Solutions” เพราะผลของ IT Governance จะมีผลกระทบต่อเรื่องสำคัญมาก ในกระบวนการปฏิบัติงานและการบริหารทั่วทั้งองค์กร โดยเฉพาะผลที่จะกระทบกับประสิทธิภาพในการปฏิบัติงาน การบริหารความมั่นคงทางการเงินขององค์กร และความน่าเชื่อถือต่อองค์กรในที่สุดด้วย
4. ข้อมูลและสารสนเทศเป็นสินทรัพย์ที่มีค่าที่สุดขององค์กร ที่ต้องการความรู้ ความสามารถของผู้บริหาร และผู้ปฏิบัติงานที่เข้าใจกระบวนการบริหาร และองค์ประกอบในการจัดการด้าน IT และ IT Governance
5. กลยุทธ์ทางด้านเทคโนโลยีสารสนเทศ (IT) ต้องสอดคล้องกับกลยุทธ์ของธุรกิจและควรมีการพิจารณาร่วมกันตั้งแต่การกำหนดนโยบาย กลยุทธ์ และการถ่ายทอดไปสู่แผนปฏิบัติการและโครงการต่าง ๆ
6. กระบวนการทางธุรกิจ (Business Process) ต้องสัมพันธ์กับกระบวนการของเทคโนโลยีสารสนเทศ (IT) ระดับต่าง ๆ (IT Process) และสอดคล้องกับกระบวนการบริหาร (Management Process)

<sup>1</sup> Organizational Governance Process เป็นกระบวนการบริหารองค์กรที่ดี ที่เป็นส่วนหนึ่งของ Corporate Governance และ IT Governance ตั้งแต่การมีจิตทัศน์ การกำหนดวิสัยทัศน์ พันธกิจ คุณค่าขององค์กร นโยบาย กลยุทธ์ เป้าหมาย แผนงาน การปฏิบัติงาน การวัดผล การปรับปรุง โดยใช้องค์ประกอบในการบริหารงานทั้ง 5 คือ การวางแผน การจัดองค์กร การพนักงาน การกำกับ การติดตามประเมินผล โดยมุ่งหวังผลลัพธ์ ตามเป้าหมายอย่างมีคุณภาพ โดยเฉพาะการคำนึงถึงการใช้ทรัพยากรต่าง ๆ แบบไม่มีพรมแดน

7. จัดให้มีการประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ควบคุมและสอดคล้องกับการกำกับดูแลกิจการที่ดี และการประเมินความเสี่ยงด้านอื่น ๆ อย่างสอดคล้องประสานและลงตัวทั่วทั้ง องค์กรรวมทั้งจัดให้มีการติดตามสอบทาน ระบบการควบคุม การบริหาร IT และ IT Governance อย่างเหมาะสม
8. จัดให้มี Early Warning System และหลักฐานรูปแบบต่าง ๆ เพื่อป้องกันความเสี่ยงหลัก ๆ โดยจัดให้มี Management Trail เพื่อการติดตาม สอบทานแบบต่อเนื่องอย่างเหมาะสม ในการบริหารความเสี่ยงและการสร้าง IT Governance
9. ประเมินความต้องการจากเทคโนโลยีสารสนเทศเพื่อการจัดการอย่างต่อเนื่องทุกรูปแบบอย่างสอดคล้องทั่วทั้งองค์กรแล้ว กำหนดและสร้างระบบ หรือจัดหาระบบให้ทำงานแทนระบบ Manual อย่างอัตโนมัติให้มากที่สุด โดยลดกระบวนการทำงานซ้ำซ้อน และการ Re-key ข้อมูลใหม่ โดยเฉพาะอย่างยิ่ง การ Key หรือ Re-key ข้อมูลจากแหล่งที่มีใช้ เป็นแหล่งเกิดข้อมูล

#### กิจกรรมด้าน IT Governance จะประกอบด้วย

1. การกำหนด นโยบาย เป้าหมาย กลยุทธ์ แผนงาน การใช้เทคโนโลยีสารสนเทศที่ชัดเจนและผสมผสานกับการจัดการดูแลที่ดีเป็นลายลักษณ์อักษร
2. กำหนด IT Master Plan วิธีการปฏิบัติงานใหม่ที่ใช้ IT และผลกระทบทางด้าน IT ที่มีต่อองค์กร และวิธีทำงานใหม่ โดยใช้กระบวนการทางเทคโนโลยีสารสนเทศ รวมทั้งการเปลี่ยนแปลงที่เกี่ยวข้อง
3. กำหนดความคาดหวังและผลตอบแทนจากการใช้ IT อย่างคุ้มค่าและวัดผลสัมฤทธิ์ได้
4. การพิจารณา Physical Security, Logical Security, Information Security และ Security Governance ต่าง ๆ ที่เป็นรูปธรรม
5. กำหนดหน้าที่ ความรับผิดชอบ การประสานงาน การใช้ IT ของแต่ละสายงานทั่วทั้งองค์กร
6. การพิจารณาใช้ IT สนับสนุนกระบวนการปฏิบัติงาน ทั้งภายในภายนอกอย่างสอดคล้องและต่อเนื่อง ทั่วถึงกันทุกระบบที่สำคัญขององค์กร เพื่อให้ได้ข้อมูลและสารสนเทศที่ใช้ในการตัดสินใจที่ดี ทันเวลา
7. กำหนดจุดควบคุม กระบวนการสอบทาน ติดตามในกระบวนการปฏิบัติงาน ตามมาตรฐานที่ยอมรับได้และสอดคล้องกับหลักสากล
8. รวบรวมและบริหารอย่างผสมผสานของ 5 องค์ประกอบในการบริหาร ตั้งแต่ การวางแผน การจัดองค์กร การบริหารบุคลากร การดำเนินงานไปจนถึงการติดตามผล
9. การบริหารและจัดการกับความเสี่ยงที่เกี่ยวข้องทั่วทั้งองค์กรโดยใช้ IT เป็นเครื่องมือ
10. จัดให้ผลการวัดการปฏิบัติงานทุกสายงาน และภาพโดยรวมขององค์กร

11. สอบทานและรับรองคุณภาพของผลการปฏิบัติงานโดยรวมจากการมี การใช้ IT และ IT Governance (ITG)

12. การพิจารณาความดี ความชอบจากผลการบริหาร และการปฏิบัติงานด้าน ITG และด้านทั่วไป อย่างผสมผสานทั่วทั้งองค์กรในส่วนที่เกี่ยวข้อง

### ปัจจัยที่ใช้วัดความสำเร็จที่เกี่ยวกับ IT Governance โดยย่อ

ปัจจัยที่ใช้วัดความสำเร็จทางด้านเทคโนโลยีสารสนเทศ และ IT Governance ที่สำคัญ ซึ่งจะเชื่อมโยงนำไปสู่ความสำเร็จขององค์กรโดยรวม จะพิจารณาทางด้านกฎหมาย ด้านการจัดองค์กร และกระบวนการปฏิบัติงานทั่วทั้งองค์กร ไม่ว่าจะใช้โปรแกรมประยุกต์เพื่อการบริหารทรัพยากรทั่วทั้งองค์กรด้านเทคนิค ซึ่งอาจเป็นระบบ Enterprise Resource Planning (ERP) หรือไม่ก็ตาม การวางแผน การปฏิบัติ การสอบทาน และการแก้ไข เพื่อนำไปสู่ความคิดในการพัฒนางานด้าน IT Governance ให้เป็นส่วนหนึ่งของการกำกับดูแลกิจการที่ดี (GCG) นั้น เป็นทั้งหน้าที่และความรับผิดชอบของคณะกรรมการ และผู้บริหารระดับสูงของทุกองค์กร

สำหรับการบริหาร IT Governance เท่าที่เป็นอยู่ในปัจจุบันเมื่อเทียบกับมาตรฐานที่ใช้ในการประเมินผลการบริหารความเสี่ยงด้าน IT Governance ซึ่งเป็นส่วนหนึ่งของการประเมินระดับการบริหารความเสี่ยงขององค์กร นั้น มีข้อควรพิจารณาปรับปรุงบางประการ เช่น BCP-Business Continuity Plan การบริหารสภาพแวดล้อมของศูนย์คอมพิวเตอร์หลักโดยการจัดให้มี IT Security Room

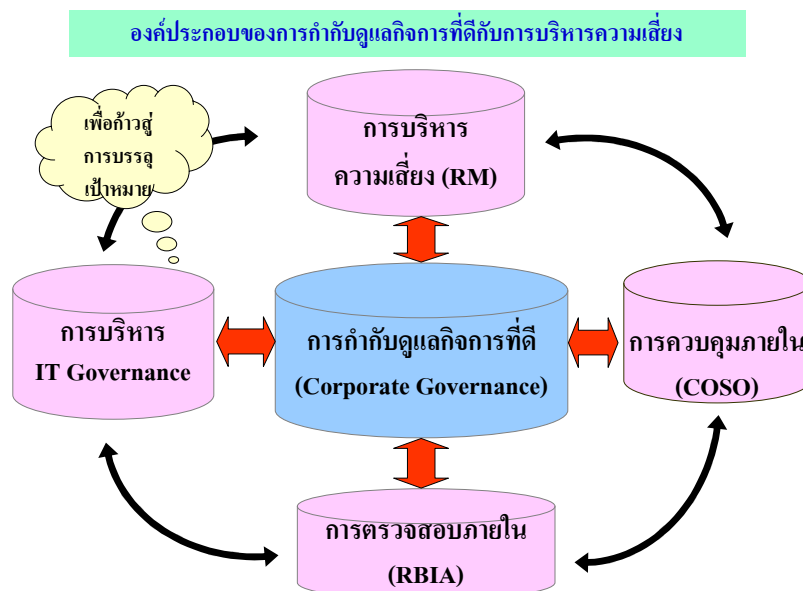
การจัดให้มีกระบวนการสร้างความมั่นใจถึงความสมดุลระหว่างผลตอบแทนจากการลงทุนและการจัดการด้าน เทคโนโลยีสารสนเทศ กับความเสี่ยงที่อาจเกิดขึ้น

การสร้างเกณฑ์วัดคุณภาพงานและผลสำเร็จของกลยุทธ์ หรือนโยบาย และการจัดการด้านเทคโนโลยีสารสนเทศตามที่กำหนดไว้ เช่น กลยุทธ์ หรือนโยบายด้านเทคโนโลยีสารสนเทศ ในการสนับสนุนให้องค์กรมีผลตอบแทนจากการลงทุนที่มากขึ้น กลยุทธ์หรือนโยบายด้านเทคโนโลยีสารสนเทศในการกำหนดมาตรฐานการปฏิบัติงานขององค์กร เป็นต้น

IT Governance เป็นส่วนหนึ่งขององค์ประกอบ Good Corporate Governance

Good Corporate Governance หรือ การกำกับดูแลกิจการที่ดี หรือ บรรษัทภิบาล เป็นเรื่องที่เราได้ยิน ได้เข้าใจกันในระดับหนึ่งแล้ว ถึงแม้ในทางปฏิบัติยังมีมาตรฐานที่แตกต่างกันค่อนข้างมากในองค์กรต่าง ๆ เพราะองค์ประกอบและปัจจัยหลายประการ ที่ต้องการสื่อสารประกอบความเข้าใจและมุ่งมั่นจากคุณลักษณะของผู้บริหารทุกระดับชั้น ทั้งในระดับประเทศ ระดับกระทรวง ระดับกรมระดับองค์กร และระดับสายงาน โดยเฉพาะอย่างยิ่ง การประสาน ความคิด ความเข้าใจและองค์ความรู้ จากสภาพแวดล้อมที่แตกต่างภายในองค์กร ไปสู่การปฏิบัติที่เป็นรูปธรรม วัดได้ พิสูจน์ได้ และตรวจสอบได้ ในการวัดคุณภาพการจัดการที่ดี ยังมีเรื่องที่ควรสนใจเพิ่มเติมที่สำคัญมากก็คือ IT Governance

องค์ประกอบของ Good Corporate Governance จะมีปัจจัยหลักและปัจจัยรองตามคุณลักษณะต่าง ๆ ที่เกี่ยวข้อง โยงใย และสัมพันธ์กันอย่างใกล้ชิด ซึ่งจะขึ้นกับว่าผู้บริหารกำลังพิจารณาในมุมมองใดเป็นเบื้องต้น แต่ทุกมุมมองจะเกี่ยวข้องกับองค์ประกอบและปัจจัยอื่น ๆ ด้วยเสมอ ตามที่ได้แสดงในภาพ จะมีรายละเอียดมากมายในแต่ละส่วนที่เกี่ยวข้องกับการบริหารเทคโนโลยีสารสนเทศ เพื่อการจัดการที่ดี (IT Governance) และการกำกับดูแลกิจการที่ดี (Good Corporate Governance) โดยเฉพาะอย่างยิ่ง การประเมินและการบริหารความเสี่ยง (Risk Management) ที่ต้องรวมความเสี่ยงทางด้าน IT และ IT Governance การควบคุมภายใน (Internal Control) ตามหลักการของ COSO<sup>2</sup> และการประเมินผลโดยการตรวจสอบตามฐานความเสี่ยง (Risk-based Audit) อย่างเหมาะสม



<sup>2</sup>COSO (Committee of Sponsoring Organizations of Treadway Commission) ทางด้าน IT จะเกี่ยวกับ COBIT (Control Objectives for Information and Related Technology) ซึ่งมีมุมมองทางด้าน Hard Controls (การควบคุมแบบทางการ) และ Soft Controls (การควบคุมแบบไม่เป็นทางการ) ที่น่าสนใจ และแตกต่างจากระบบทั่วไปมาก โดยเฉพาะ Soft Controls ที่ไม่เกี่ยวกับ Software และ Hard Controls สำคัญน้อยกว่า Soft Controls

หลายองค์กรให้ความสนใจเกี่ยวกับการบริหารความเสี่ยงทางด้าน IT และ IT Governance อย่างจำกัดมาก หลายองค์กรไม่เข้าใจและไม่มีการพิจารณารวมงานด้าน IT และหลักการบริหารด้าน IT Governance มาเป็นส่วนหนึ่งของหลักการ Good Corporate Governance เพื่อการจัดโครงสร้างการบริหารให้เกิดมูลค่าเพิ่ม และเป็นที่น่าเชื่อถือ อย่างเหมาะสม ด้วยการสร้างกลไก และกระบวนการทาง IT Governance เพื่อก่อให้เกิด Organizational Governance Process อย่างเหมาะสม ควบคู่กันไปกับ Good Corporate Governance เพื่อสร้างประสิทธิภาพ ประสิทธิผลในการดำเนินงาน อย่างเป็นกระบวนการทั่วทั้งองค์กร อย่างเป็นระบบ ตามหลักการกำกับดูแลกิจการที่ดี อย่างเป็นรูปธรรม ทั้งนี้เพราะความเข้าใจในการบูรณาการภาพโดยรวม และการใช้ศักยภาพ ของ IT และการบริหาร IT Governance ควบคู่กับ Good Corporate Governance ยังไม่มีการนำไปปฏิบัติ ตั้งแต่ระดับนโยบาย การกำหนดวัตถุประสงค์ รวมถึงการกำหนดกลยุทธ์ การมีการใช้ เทคโนโลยีสารสนเทศที่ดี เพื่อมุ่งไปสู่การบูรณาการ ในการบริหารอย่างเป็นรูปธรรม

**IT Governance เป็นส่วนหนึ่งของ Good Corporate Governance และต้องพิจารณาควบคู่กันไปใน การสร้างคุณค่าเพิ่มกับ E-Government<sup>3</sup>**

IT Governance กับ Good Corporate Governance หรือการใช้เทคโนโลยีสารสนเทศ ผสมผสานควบคู่กัน กับการบริหารการจัดการที่ดี เป็นสิ่งที่แยกกันไม่ได้เลยในทุกองค์กร นี่คือความจริง ที่ต้องการความเข้าใจในทุกะดับของการจัดการและการปฏิบัติ ทั้งในระดับประเทศ ระดับองค์กร ในทุกองค์ประกอบของการบริหาร เริ่มตั้งแต่การคิด การวางแผน การจัดองค์กร การพนักงาน การบริหาร และการติดตามผล โดยเฉพาะอย่างยิ่งการนำปัจจัยเรื่อง Risk IT และ IT Risk มาพิจารณาถึงผลกระทบต่อวัตถุประสงค์ระดับต่างๆ ขององค์กร เพราะ ใน COSO-ERM ยังไม่ได้กล่าวถึงเรื่องนี้

การบริหารทรัพยากรของประเทศและขององค์กรโดยรวม ต้องการจินตนาการและความคิดที่เป็นระบบ (Systematic Thinking) คิดให้ครบจนจบความ ในระดับประเทศ ระดับองค์กรให้ได้ก่อนจะแยกคิดให้ลึกเชิงวิเคราะห์ และคิดให้กว้างอย่างสร้างสรรค์เป็นเรื่อง และเป็นส่วน ๆ ต่อไปอย่างสัมพันธ์กันเป็นระบบโดยรวม (Total System) และเป็นขั้นตอนตามภาระหน้าที่ ที่ต้องระวางช่องว่างในการจัดการนั้น มีความสำคัญยิ่ง และสำคัญยิ่งกว่าความรู้และวิสัยทัศน์ ที่ยังเป็นคำถามสำหรับการจัดการที่ดีในหลายองค์กร ก่อนที่จะก้าวไปสู่การกำกับดูแล

<sup>3</sup> แนวความคิด E-Government และการจัดให้มีศูนย์ประมวลผลแห่งรัฐโดยรวม อย่างเป็นระบบ เป็นขั้นตอน โดยแบ่งตามคุณลักษณะแห่งงาน จะเปลี่ยนแปลงไปตามการพัฒนาเทคโนโลยีที่เหมาะสม และมีความสะดวกมากขึ้นในปัจจุบัน โดยผ่าน Network อาศัยความสามารถในการใช้ทรัพยากรด้าน IT โดยไม่คำนึงถึงและไม่ยึดติดกับโครงสร้างทางกายภาพของ IT นั่นคือ การใช้ Network ในการเชื่อมโยงทรัพยากรด้าน IT เข้าด้วยกัน อย่างมีคุณภาพสูงสุด (Virtual Network) เพื่อลดความสูญเสียในการใช้ทรัพยากรต่าง ๆ เท่าที่เป็นไปได้

กิจการที่ดี และการเติบโตอย่างยั่งยืนของผู้มีผลประโยชน์ร่วม นั่นคือ ต้องมีความเชื่อร่วมกันเป็น Core Value ขององค์กรกว่า IT Governance เป็นมากกว่าการใช้ IT เป็นเพียง Tool ในการบริหารและการจัดการ ภายในองค์กร และระหว่างองค์กร

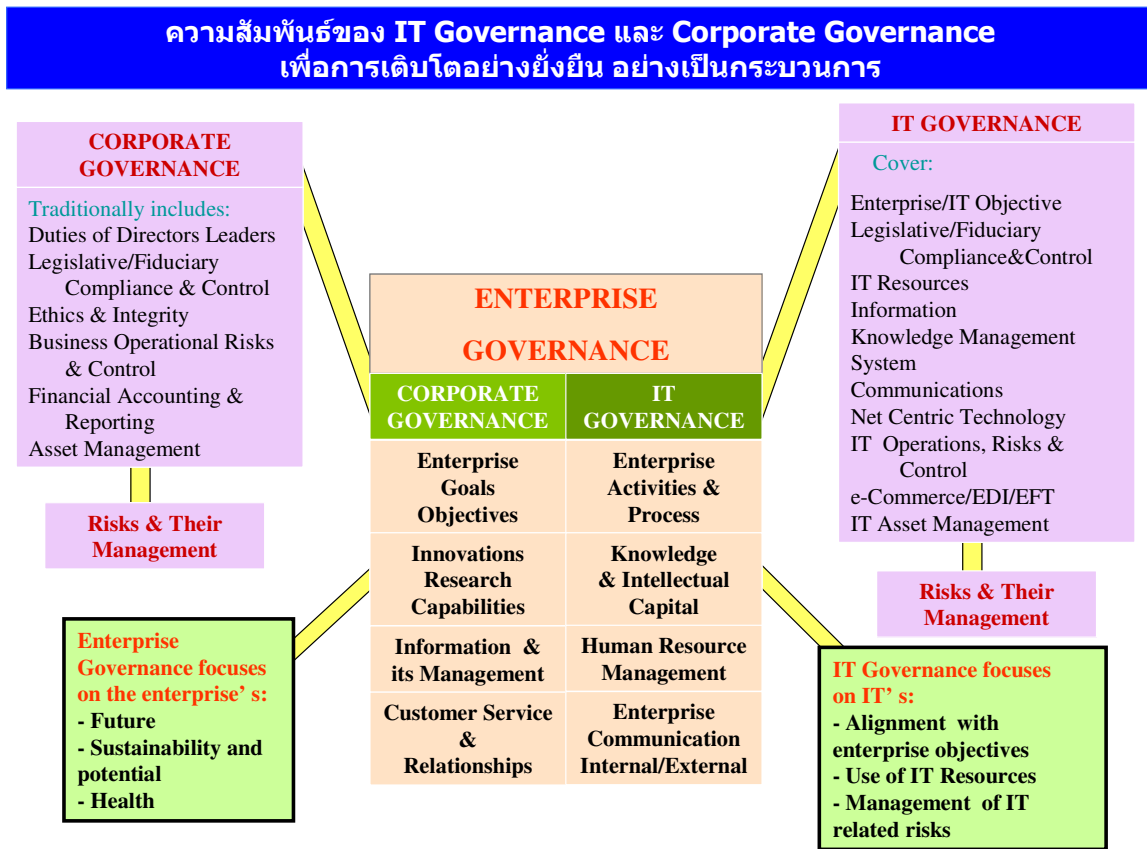
ตัวอย่างในเรื่องนี้จะชัดเจนยิ่งขึ้นเมื่อรัฐบาลนำระบบ Zero-Based มาใช้ในการจัดทำงานประมาณประจำปี งบประมาณทางด้าน IT ของหน่วยงานต่างๆ จะสูงขึ้นอย่างมีนัยสำคัญ ทั้งทางด้าน Hardware, Software และ Network ซึ่งจะตามมาด้วยค่าบำรุงรักษาเป็นจำนวนมาก และงบประมาณจากระบบใหม่โดยรวมก็จะไม่ลดลง หรืออาจเพิ่มขึ้นอย่างมีนัยสำคัญ จึงน่าจะมีคำถามและคำตอบที่ดีว่า หน่วยงานของรัฐและรัฐวิสาหกิจควรจัดสรรทรัพยากรร่วมกันอย่างไรดี จึงจะสามารถลดความซ้ำซ้อน และสร้างมูลค่าเพิ่ม คุ่มค่าเงินของประเทศ และองค์กรมากที่สุด ประเทศไทยควรมีหน่วยงานที่ทำหน้าที่กำกับ IT Governance ระดับชาติ โดยการร่วมกันใช้ทรัพยากรทางด้าน IT และทรัพยากรอื่นๆ ที่เกี่ยวข้องอย่างเป็นระบบ

ในภาคปฏิบัติอาจกำหนดให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารให้ข้อเสนอแนะและเสนอคณะรัฐมนตรีเพื่อพิจารณากำกับการปรับปรุงแผนแม่บทเป็นรายปี เพื่อให้ทำใหักระบวนการวางแผนในระดับชาติเกี่ยวกับการพัฒนา ICT มีการขับเคลื่อนอย่างต่อเนื่อง (Rolling Plan) ทุกปี ซึ่งเรื่องนี้ทราบว่า เป็นสิ่งที่กระทรวง ICT ได้มีแนวทางเรื่องนี้ชัดเจนอยู่แล้ว หากการปฏิบัติใช้รูปแบบการบูรณาการระดับชาติที่เกี่ยวข้องกับ IT Governance ทั้งทางด้าน Hardware Software และ Network รวมทั้งบุคลากรเป็นไปอย่างสอดคล้องประสานกันอย่างแท้จริงทุกระดับอย่างได้ผลแล้ว จะทำให้งบประมาณในการพัฒนาทางด้าน IT ของชาติและขององค์กรต่าง ๆ จะมีประสิทธิภาพเพิ่มขึ้นมาก

### ความสัมพันธ์ของ IT Governance กับ Corporate Governance

IT Governance เป็นส่วนสำคัญที่รวมอยู่ในความสำเร็จของ Corporate Governance โดยจะเป็นจุดวัดของการปรับปรุงในด้านประสิทธิผล และประสิทธิภาพของกระบวนการปฏิบัติงานขององค์กร โดยธรรมาภิบาลขององค์กร จะเป็นกรอบในการกำหนดแนวทางสำหรับธรรมาภิบาลทางด้านเทคโนโลยีสารสนเทศ ส่วนกิจกรรม / กระบวนการต่าง ๆ ขององค์กรจะต้องใช้ข้อมูลจาก กิจกรรม / กระบวนการของเทคโนโลยีสารสนเทศ ดังนี้

## Enterprise Governance = IT Governance + Corporate Governance



Corporate Governance จะกำกับ ควบคุม เป็นผู้ขับเคลื่อน และกำหนดรูปแบบของ IT Governance ในขณะเดียวกัน เทคโนโลยีสารสนเทศก็ได้สนับสนุนข้อมูลที่เป็นต่าง ๆ เพื่อใช้ในการวางแผนด้านกลยุทธ์ และในบางครั้งยังเป็นส่วนที่มีอิทธิพลในการสร้างโอกาสใหม่ ๆ ให้กับองค์กร จึงถือได้ว่าเทคโนโลยีสารสนเทศและการวางแผนด้านกลยุทธ์มีความสัมพันธ์แบบพึ่งพากัน โดยกิจกรรมในองค์กร จำเป็นต้องใช้ข้อมูลจาก IT Activities เพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจ โดย IT Activities จะต้องสอดคล้องกับกิจกรรมในองค์กรและช่วยให้องค์กรสามารถใช้ประโยชน์จากข้อมูลอย่างเต็มที่ในการสร้างประโยชน์สูงสุด และได้ผลตอบแทนจากการลงทุนจากโอกาสทางธุรกิจต่าง ๆ รวมทั้งสามารถเพิ่มความได้เปรียบในการแข่งขันมากขึ้น

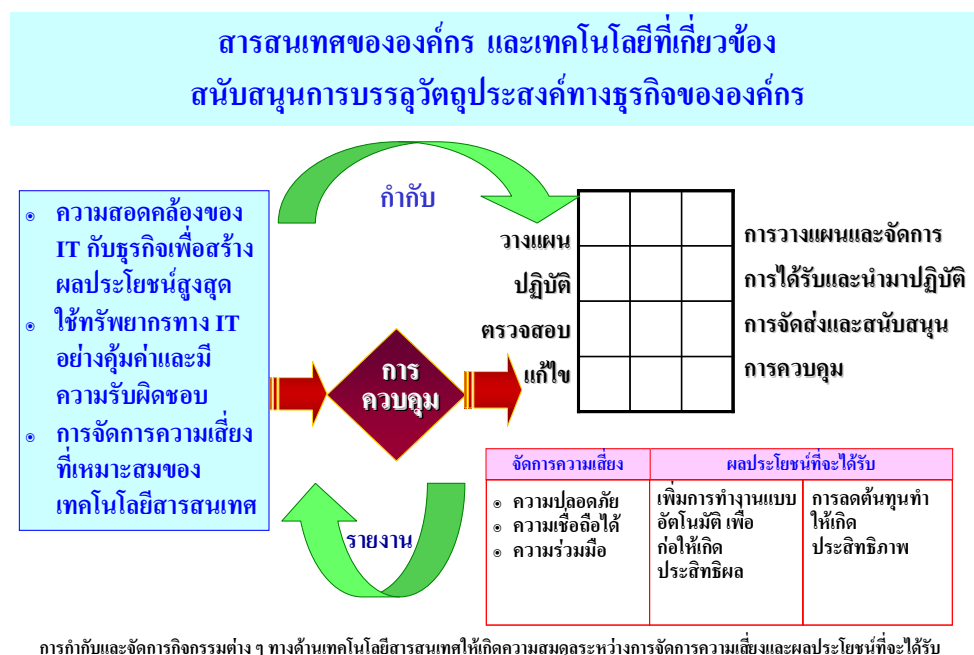
โดยปกติแล้วองค์กร จะมีการกำกับ บริหาร และควบคุมโดยใช้หลักการจัดการและการปฏิบัติที่เหมาะสมหรือที่ดีที่สุด เพื่อให้มั่นใจว่าองค์กรจะสามารถบรรลุเป้าประสงค์ ที่ต้องการ โดยต้องมีการควบคุมที่ดีด้วยเช่นกัน

ในขณะเดียวกันเทคโนโลยีสารสนเทศก็จำเป็นต้องมีการกำกับ บริหาร และควบคุมที่ดี โดยยึดหลักการของ Good Practices หรือ Best Practices เช่น เดียวกัน เพื่อให้ข้อมูลและเทคโนโลยีที่ใช้ในองค์กร สามารถช่วยให้องค์กรบรรลุวัตถุประสงค์ทางธุรกิจได้ รวมทั้งการใช้ทรัพยากรต่าง ๆ อย่างมีประสิทธิภาพ และมีการบริหารความเสี่ยงที่เหมาะสม

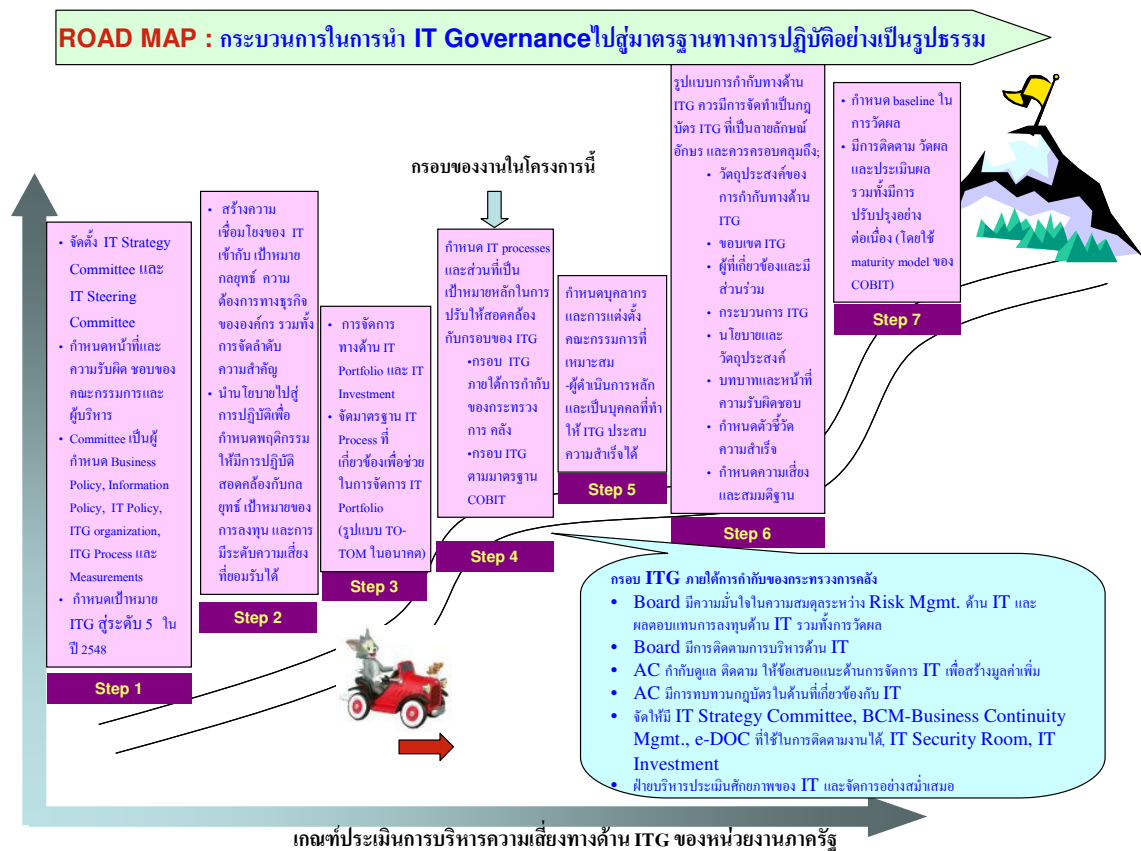
จากประเด็นดังกล่าวจะเป็นพื้นฐานสำคัญในการกำหนดแนวทางของกิจกรรมทางด้านเทคโนโลยีสารสนเทศซึ่งสามารถสรุปลักษณะของกิจกรรมหลักจาก 4 Domains ได้ดังนี้

1. การวางแผนและการจัดการองค์กร (Planning & Organization - PO)
2. การจัดหาและการนำระบบออกใช้งานจริง (Acquisition & Implementation - AI)
3. การส่งมอบและการบำรุงรักษา (Delivery & Support - DS)
4. การติดตาม (Monitoring - M)

โดยมีวัตถุประสงค์ควบคู่ไปกับการบริหารความเสี่ยง (ในด้านความปลอดภัย ความเชื่อมั่น และความสอดคล้อง ของ IT Activities) และการได้มาซึ่งประโยชน์สูงสุด (ในด้านการเพิ่มประสิทธิภาพ และประสิทธิผล) ผลลัพธ์ที่ได้ในรูปแบบของรายงาน จะบอกถึง IT Activities ว่าสามารถสอดคล้อง และสนับสนุนองค์กรให้บรรลุวัตถุประสงค์และเป้าหมายขององค์กรหรือไม่ และทำได้ดีเพียงใดและอย่างไรตามภาพโดยย่อ ดังนี้



## ROAD MAP : กระบวนการในการนำ IT Governance ไปสู่มาตรฐาน ทางการปฏิบัติอย่างเป็นรูปธรรม



### บทบาทและความสัมพันธ์กับการบริหารความเสี่ยงโดยรวม

การบริหารเทคโนโลยีสารสนเทศที่ดี (IT Governance) มีความสำคัญมาก และเป็นมิติสำคัญในการบริหารความเสี่ยงในภาพโดยรวมของทุกองค์กร ซึ่งหน่วยงานกำกับภาครัฐ ก็ได้นำ IT Governance มาเป็นปัจจัยวัดคุณภาพการบริหารความเสี่ยงโดยรวมด้วยการรื้อปรับระบบ (Reengineering) ไม่จำเป็นต้องปรับระบบให้เป็นอัตโนมัติ หรือการปรับโครงสร้าง (Restructuring) การลดขนาดองค์กร (Downsizing) การจัดองค์กรใหม่ (Reorganizing) หรือการลดชั้น (Delay ring) ในองค์กร แต่เมื่อระบบงานหลักเปลี่ยนเป็นระบบอัตโนมัติมากขึ้น การเปลี่ยนแปลงจำเป็นต้องเกิดขึ้นอย่างสอดคล้องกันในเวลาที่เหมาะสม

1. การรื้อปรับระบบจากซอฟต์แวร์สำเร็จรูปจะช่วยให้งานหลัก ๆ ปฏิบัติได้อย่างมีประสิทธิภาพ ช่วยให้มีการประสานการทำงาน และกระบวนการทำงานให้มีประสิทธิภาพ รวมทั้งยังเพิ่มความสามารถในการตัดสินใจของผู้บริหารและผู้เกี่ยวข้อง เพื่อสร้างคุณค่าเพิ่มให้องค์กรได้มาก

2. การจัดการเทคโนโลยีสารสนเทศที่ดี (IT Governance) จะมีประโยชน์ในการผลักดันประสิทธิภาพขององค์กรได้อย่างจำกัด ถ้าทรัพยากรบุคคลก้าวไม่ทันกับระบบงานใหม่ ดังนั้นจึงมีความจำเป็นที่จะต้องทำการพัฒนาบุคลากรอย่างเหมาะสม ให้สอดคล้องกับแผนงานด้านเทคโนโลยีสารสนเทศขององค์กรในอนาคต

3. ปัจจุบันกรรมการ และผู้บริหารขององค์กร มีวิสัยทัศน์ที่ดีในด้านการวางแผนการใช้เทคโนโลยีสารสนเทศเพื่อการจัดการที่ดี ซึ่งผู้บริหารเป็นเจ้าภาพในการปรับเปลี่ยนกระบวนการทัศน์สู่การจัดการใหม่ได้ โดยสร้างกลยุทธ์ที่เหมาะสมให้สามารถมองเห็น และประยุกต์ใช้เทคโนโลยีที่ดีเป็นขั้นตอนอย่างเหมาะสม ซึ่งจะมีประโยชน์อย่างยิ่งในการประเมินระดับการบริหาร โดยการเตรียมการ และพัฒนาพนักงานอย่างเหมาะสมเป็นสำคัญ

### บทบาทของฝ่ายตรวจสอบที่เกี่ยวข้องกับ IT Governance

ฝ่ายตรวจสอบควรมีบทบาทในฐานะเป็นผู้ให้คำแนะนำและสร้างคุณค่าเพิ่มในการปฏิบัติหน้าที่ตามมาตรฐานการตรวจสอบภายในของทุกสายงาน และในฐานะผู้ประเมินคุณภาพการบริหารความเสี่ยง การควบคุมภายในทางด้านต่างๆ เช่น

1. คุณภาพของการปฏิบัติงาน (Operational)
2. คุณภาพทางการปฏิบัติตามนโยบาย กฎเกณฑ์ ระเบียบ คำสั่ง (Compliance)
3. คุณภาพด้านการเงิน และการรายงาน (Financial) รวมทั้งการให้คำแนะนำด้านเทคโนโลยี

สารสนเทศ และ IT Governance

4. การตรวจสอบทางด้านเทคโนโลยีสารสนเทศตามระเบียบของบริษัทฯ ตรวจสอบแผ่นดินข้อที่ 6 รวมทั้งการใช้ Outsource เพื่อเป้าหมายดังกล่าว รวมทั้งมุมมองที่กว้างกว่านั้น บริษัทฯ ควรวางกรอบความต้องการของตนให้ชัดเจนเพื่อความคุ้มค่าในการดำเนินงาน เพราะการตรวจสอบด้านเทคโนโลยียุคใหม่จะเป็นการตรวจสอบการจัดการความเสี่ยงทางด้าน IT Governance

### ความสำคัญของการจัดให้มีหลักเกณฑ์และแนวทางการกำกับดูแลที่ดี

ภาครัฐได้กำหนดให้มีระเบียบสำนักนายกรัฐมนตรีว่าด้วยการสร้างระบบการบริหารกิจการบ้านเมืองและสังคมที่ ปี พ.ศ. 2542 โดยมีจุดมุ่งหมายเพื่อ

1. สร้างกฎเกณฑ์และกลไกที่ดีในการบริหารกิจการบ้านเมืองและสังคม
2. พัฒนาศักยภาพของนักวิชาการให้สามารถศึกษา ค้นคว้า และเสนอแนะแนวทางแก้ไขปัญหาต่าง ๆ ที่จำเป็นต่อการบริหารกิจการบ้านเมือง
3. ปรับปรุงระบบการบริหารจัดการของภาครัฐและธุรกิจให้รวดเร็ว ชัดเจน และเป็นธรรม

4. ขยายโอกาสของประชาชนในการรับรู้ข้อมูลข่าวสารของภาครัฐ
5. จัดการทุจริตประพฤติมิชอบและการหลีกเลี่ยงกฎหมาย เพื่อแสวงหาประโยชน์ส่วนตน ทั้งในภาครัฐและเอกชน

### ประโยชน์ของการกำกับดูแลที่ดี

1. สร้างความโปร่งใส และมีมาตรฐานการปฏิบัติที่เป็นสากล
2. เป็นการเพิ่มความน่าเชื่อถือ และความมั่นใจแก่สาธารณชน เจ้าของกิจการ/ผู้ถือหุ้น นักลงทุนทั้งในและต่างประเทศ
3. สร้างความมั่นใจในการลงทุน และทำให้มูลค่ากิจการสูงขึ้น
4. ทำให้เกิดรูปแบบกิจการที่เป็นที่ยอมรับ และสามารถแข่งขันได้ในสภาพตลาดการแข่งขันเสรี
5. ทำให้เกิดการสร้างพันธมิตรผูกพัน เพื่อให้ผู้บริหารใช้อำนาจภายในขอบเขต รวมถึงการสร้างกรอบความรับผิดชอบของคณะผู้บริหาร และคณะกรรมการต่อผู้มีส่วนได้ส่วนเสีย และสังคมส่วนรวมทำให้เกิดระบบความรับผิดชอบของผู้บริหารต่อกรรมการ และกรรมการต่อเจ้าของกิจการ/ผู้ถือหุ้น เป็นลำดับขึ้นไป
6. เป็นเครื่องมือการตรวจสอบการทำงานด้านต่าง ๆ ขององค์กร เพื่อปรับปรุงแก้ไขการดำเนินงานให้มีประสิทธิผลและประสิทธิภาพดียิ่งขึ้น
7. ป้องกันการแสวงหาประโยชน์จากการเป็นกรรมการหรือการบริหาร และเสริมสร้างความโปร่งใสในการบริหารจัดการ

### หลักสำคัญสำหรับจัดทำกำกับการกำกับดูแลที่ดี

- หลักสำคัญในการจัดทำกำกับการกำกับดูแลที่ดีมีหลักสำคัญอันเป็นหลักสากลที่เป็นมาตรฐาน 6 ประการ ดังนี้
1. Accountability หรือความรับผิดชอบต่อผลการปฏิบัติหน้าที่ (ซึ่งอาจเป็นทั้งบวกและลบ)
  2. Responsibility หรือความสำนึกในหน้าที่ด้วยขีดความสามารถและประสิทธิภาพที่เพียงพอ
  3. Equitable Treatment หรือการปฏิบัติต่อผู้มีส่วนได้เสียอย่างเท่าเทียมกัน กล่าวคือ ผู้มีส่วนได้เสียโดยสุจริตจะต้องได้รับการพิจารณาให้เกิดความเท่าเทียมกัน เช่น การจัดซื้อจัดจ้างต้องให้ทุกคนได้รับความยุติธรรมและเท่าเทียมกัน หากมีการร้องเรียนต้องมีคำอธิบายได้
  4. Transparency หรือความโปร่งใส กล่าวคือ ต้องมีความโปร่งใสใน 2 ลักษณะดังนี้
    - 4.1. ความโปร่งใสในการดำเนินงานที่สามารถตรวจสอบได้

4.2. มีการเปิดเผยข้อมูลอย่างโปร่งใส (Transparency of Information Disclosure) คือมีการแสดงผลประกอบการอย่างโปร่งใสแก่ผู้ที่เกี่ยวข้องทุกฝ่าย

5. Vision ที่จะ Create Long Term Value หรือการมีวิสัยทัศน์โดยการมองการสร้างมูลค่าเพิ่มแก่กิจการในระยะยาว ที่จะสนองภารกิจโดยไม่ทำลายขีดความสามารถในระยะสั้น ซึ่งการเปลี่ยนแปลงหรือเพิ่มมูลค่าใด ๆ นั้น จะต้องเป็นการเพิ่มความสามารถในทุกด้านเพื่อการแข่งขัน

6. Ethics คือ การส่งเสริมพัฒนาการกำกับดูแล และจรรยาบรรณที่ดีในการประกอบธุรกิจ



อธิบายเบื้องต้นจากรูปภาพประกอบ โดยเพิ่มส่วนที่เกี่ยวข้องกับการบริหารความเสี่ยง ในมุมมองกว้างๆ เพื่อนำไปสู่จินตนาการ ความคิด ความเข้าใจ การสื่อสาร และการปฏิบัติที่เกี่ยวข้องกับการโยงโยงของ IT และ IT Governance ระดับระหว่างประเทศ ภายในประเทศ ระหว่างองค์กรของภาครัฐ และภาคเอกชน ในส่วนที่เกี่ยวข้องเพียงเป็นพื้นฐานได้ระดับหนึ่ง

ตามภาพ ธรรมภิบาล (Good Governance) ประกอบด้วย บรรษัทภิบาล (Corporate Governance) โลกภิบาล (Global Governance) รัฐบาล (Public Governance) และสังคมภิบาล (Social Governance) โดยมีปัจจัยแต่ละ Governance แตกต่างกันไปตามคุณลักษณะของ Governance แต่ละประเภทดังที่ได้สรุปไว้ในภาพแล้ว

ทุกความแตกต่างไม่ว่าจะเป็นแบบใด ระดับใด ความแตกต่างของลักษณะงานโดยเฉพาะความแตกต่างเรื่องสถานที่ และความแตกต่างเรื่องเวลา การทำงานข้ามสายงาน การทำงานข้ามองค์กร สามารถเชื่อมโยงและสื่อถึงกันได้ด้วยเทคโนโลยีสารสนเทศ (IT) จากความคิดเรื่องเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดี (ITG) ที่นำไปสู่การปฏิบัติที่เป็นรูปธรรมได้ จัดการได้ ควบคุมได้ วัดได้ ตรวจสอบได้ ทั้งในระดับประเทศและระดับองค์กร รวมทั้งระดับสายงาน ถ้าพิจารณาจากรูปภาพต่อไปก็จะพอเข้าใจเบื้องต้นได้ว่า การวัดประสิทธิผล ประสิทธิภาพ ในการดำเนินงาน ไม่ว่าจะใช้ Management Tools ใด ๆ เป็นตัววัด เช่น BSC (Balanced Scorecard) KPI (Key Performance Indicator) EVA (Economic Value Added) ฯลฯ ก็สามารถดำเนินการได้ นอกเหนือจากการใช้ IT เพื่อการควบคุม เพื่อการบริหาร เพื่อการจัดการ และเพื่อการตรวจสอบตามฐานความเสี่ยงทางด้าน IT และ IT Governance ที่เกี่ยวข้อง

## ก้าวสู่...การกำกับดูแลกิจการที่ดีขององค์กร

การกำกับดูแลกิจการที่ดีขององค์กรมีบทบาทในการเพิ่มศักยภาพการแข่งขันทางด้านกาบริการ ให้บริการ สร้างความไว้วางใจในด้านความโปร่งใสและการปฏิบัติที่เป็นธรรม

ความเข้าใจของคำว่า การกำกับดูแลกิจการที่ดี (Good Corporate Governance) มีความเข้าใจที่แตกต่างกันค่อนข้างมาก ในบรรดาผู้บริหารและผู้ปฏิบัติงานบางส่วน การสร้างความเชื่อมั่นในการนำองค์กรไปสู่เป้าหมายที่กำหนดได้อย่างยั่งยืนนั้น จำเป็นอย่างยิ่งที่จะต้องร่วมมือร่วมใจกันสร้างและจัดให้มีวิธีการกำกับดูแลกิจการที่ดี เพื่อสร้างโอกาส ศักยภาพ โดยความร่วมมือ ร่วมใจของบุคลากรทุกระดับ

การกำกับดูแลกิจการที่ดี เป็นการบริหารจัดการโดยกำหนดบทบาทและวิธีปฏิบัติงานเพื่อก่อให้เกิดประโยชน์ต่อการบริหาร การให้บริการและเพิ่มมูลค่าในทุกระดับขององค์กร ตามหลักการสากลของการกำกับดูแลกิจการที่ดีที่ใช้อยู่ในปัจจุบันนี้และสอดคล้องกับพระราชกฤษฎีกา พ.ศ.2546 ว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดีในมิติต่าง ๆ ซึ่งจะประกอบด้วย

### 1. Responsibility

มีความเข้าใจและมีขีดความสามารถในการประพฤติปฏิบัติได้ตามหน้าที่ และความรับผิดชอบให้บรรลุวัตถุประสงค์และเป้าหมายที่กำหนด

### 2. Accountability

แสดงความรับผิดชอบและรับผิดชอบต่อผลการปฏิบัติหน้าที่ถึงแม้จะไม่ได้ปฏิบัติงานนั้นด้วยตนเอง

### 3. Equitable Treatment

ปฏิบัติต่อผู้มีส่วนได้ส่วนเสียทุกกลุ่มอย่างเท่าเทียมและเป็นธรรม

### 4. Transparency

แสดงความโปร่งใสในการดำเนินงาน สามารถอธิบายและตรวจสอบได้

### 5. Creation of Long Term Value

แสดงกลยุทธ์และขีดความสามารถในการสร้างมูลค่าเพิ่มให้กับกิจการในระยะยาว

### 6. Promotion of Best Practices

ส่งเสริมการปฏิบัติอันเป็นเลิศ และการมีจรรยาบรรณที่ดีในการประกอบธุรกิจ

## 7. Social and Environmental Awareness

มีความสำคัญที่ต้องรับผิดชอบต่อสังคม และสิ่งแวดล้อม

ความตื่นตัวขององค์กรกำกับดูแลกิจการที่ดี ได้เกิดมากขึ้นหลังจากที่ประเทศไทยได้ประสบวิกฤติการณ์เศรษฐกิจที่ผ่านมา เชื่อว่าวิกฤติที่เกิดขึ้นนั้น ส่วนหนึ่งมาจากการขาดการบริหารจัดการที่ดีทั้งในภาครัฐและเอกชน โดยเฉพาะอย่างยิ่งการละเลยไม่ปรับตัวให้สอดคล้องกับความเปลี่ยนแปลง การไม่สร้างมาตรฐานให้ทัดเทียมเพื่อการแข่งขันกับคนอื่น โดยเฉพาะในเวทีของโลก จึงต้องมีการปรับปรุงการบริหารจัดการ ทั้งในภาครัฐและเอกชน พัฒนารูปแบบการดำเนินงานเพื่อสามารถแข่งขันกับผู้อื่นได้ สามารถยกระดับมาตรฐานให้เป็นสากล เป็นที่ยอมรับ เป็นที่น่าเชื่อถือและน่าไว้วางใจต่อผู้ที่เกี่ยวข้อง เพราะธุรกิจต่าง ๆ และหน่วยงานของรัฐ ต้องติดต่อและมีความสัมพันธ์ระหว่างประเทศมากขึ้น ไม่ทางตรงก็ทางอ้อม

หน่วยงานภาครัฐของไทยจึงเล็งเห็นถึงความสำคัญของการกำกับดูแลกิจการที่ดีและประโยชน์ที่คาดว่าจะได้รับจากการนำการกำกับดูแลกิจการที่ดีมาใช้ จึงได้มีการประยุกต์หลักการสากลทั้ง 7 ประการข้างต้นให้มีความเป็นรูปธรรมและเหมาะสมกับประเทศไทยมากขึ้น โดยรัฐบาลได้ออกมาเป็น พระราชกฤษฎีกาว่าด้วยหลักเกณฑ์ และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ. 2546 เมื่อวันที่ 9 ตุลาคม 2546 โดยสาระสำคัญประกอบด้วย

1. การเกิดประโยชน์สุขของประชาชน
2. การเกิดผลสัมฤทธิ์ต่อภารกิจของรัฐ
3. มีประสิทธิภาพและเกิดความคุ้มค่าในเชิงภารกิจของรัฐ
4. ไม่มีขั้นตอนการปฏิบัติงานเกินความจำเป็น
5. มีการปรับปรุงภารกิจของส่วนราชการให้ทันต่อสถานการณ์
6. ประชาชนได้รับการอำนวยความสะดวก และได้รับการตอบสนองความต้องการ
7. มีการประเมินผลการปฏิบัติราชการสม่ำเสมอ

สาระสำคัญของพระราชกฤษฎีกาฯ ข้างต้นทำให้ทางหน่วยงานภาครัฐต่าง ๆ ให้ความสำคัญในเรื่องการกำกับดูแลกิจการที่ดีกันมากขึ้น โดยได้มีการนำเอาพระราชกฤษฎีกาฯ นั้นมาใช้ในการกำหนดออกมาเป็นกรอบของ กพร. ซึ่งสามารถแบ่งออกเป็นมิติต่าง ๆ 4 ด้าน

#### มิติตั้ง 4 ด้าน ตามกรอบของกพร. ประกอบด้วย

##### มิติตั้งที่ 1 ประสิทธิภาพตามพันธกิจ

1. การประเมินผลตามแผนยุทธศาสตร์ของหน่วยราชการ
2. ผลสำเร็จในการพัฒนาการปฏิบัติราชการ

##### มิติตั้งที่ 2 ประสิทธิภาพของการปฏิบัติราชการ

1. คุณภาพการให้บริการ
2. การให้บริการผ่านทางระบบอิเล็กทรอนิกส์
3. การสำรวจและรับฟังความคิดเห็นของประชาชน และจัดให้มีคณะที่ปรึกษาภาคประชาชน

##### มิติตั้งที่ 3 คุณภาพการให้บริการ

1. การลดค่าใช้จ่าย
2. การลดระยะเวลาการให้บริการ
3. การนำระบบอิเล็กทรอนิกส์มาใช้กับงานบางส่วน
4. การวัดต้นทุนต่อหน่วย
5. การบริหารสินทรัพย์ให้เกิดประสิทธิภาพ

##### มิติตั้งที่ 4 การพัฒนาองค์กร

1. การลดอัตรากำลังหรือการจัดสรรอัตรากำลังให้ทำงานคุ้มค่า
2. การมอบอำนาจการตัดสินใจ การอนุมัติ อนุญาตไปยังระดับปฏิบัติการ
3. การกำหนดเป้าหมายและตัวชี้วัดระดับบุคคลให้สอดคล้องกับระดับองค์กร
4. การพัฒนาระบบการควบคุมภายใน
5. นวัตกรรม

จากหลักสากลของการกำกับดูแลที่ดีแปลงมาสู่พระราชกฤษฎีกาฯ องค์กรสามารถนำมาประยุกต์ปฏิบัติให้เป็นรูปธรรม เพื่อให้สามารถวางเป็นกรอบการดำเนินงานในการกำกับดูแลองค์กรที่ดีขององค์กร เป็นหลักเกณฑ์และมาตรฐานที่กำหนดขึ้น เพื่อให้คณะผู้บริหารและพนักงานขององค์กร ใช้เป็นแนวทางในการกำกับดูแลการบริหารงานและปฏิบัติงานให้มีคุณภาพ มีความโปร่งใส และมีประสิทธิภาพในภาระหน้าที่ความรับผิดชอบในการบริหารงานทุกขั้นตอน โดยการกำหนดรูปแบบและอำนาจหน้าที่ ตลอดจนแนวปฏิบัติที่ดีของคณะกรรมการฝ่ายบริหารและพนักงาน เพื่อให้เกิดกระบวนการกำกับดูแล มีการตรวจสอบและพัฒนาการ และระบบการควบคุม

ภายในที่ดีเป็นมาตรฐาน โดยมีการบริหารและจัดการกับขนาดของความเสี่ยงด้านต่าง ๆ ที่มีโอกาสที่จะสร้างความเสียหายให้กับองค์กร ทั้งในปัจจุบันและอนาคตได้อย่างมีประสิทธิภาพและเหมาะสมเป็นที่ยอมรับของทุก ๆ ฝ่ายที่เกี่ยวข้อง

**กรอบการดำเนินงานข้างต้น สามารถแสดงออกมาเป็นภาพที่ชัดเจนและสื่อได้ดังนี้**



รากฐานของการบริหารเพื่อสร้างศักยภาพการแข่งขันและความน่าเชื่อถือ  
 สู่การเติบโตอย่างยั่งยืนจากหลักสากลสู่รูปแบบไทย

## การกำกับดูแลกิจการที่ดี (Good Governance) และการนำไปสู่การปฏิบัติ

### 1. การกำกับดูแลกิจการที่ดีขององค์กร (Good Corporate Governance หรือ GCG) คืออะไร

ความเข้าใจในที่มาของหลักการจากความเชื่อ สู่วิธีการปฏิบัติที่เป็นรูปธรรมเป็นเรื่องสำคัญมาก Good Corporate Governance - GCG คือ วิธีแห่งการนำองค์กรสู่ความรุ่งเรืองมั่นคงยั่งยืน ซึ่งกล่าวถึง ปรัชญา คุณธรรม และจริยธรรมแห่งองค์กรในการบริหารและจัดการที่ดี อันเป็นปัจจัยสำคัญของการสร้างคุณค่าและเพิ่มพลังแห่งความเจริญเติบโตรุ่งเรือง เพื่อให้องค์กรบรรลุวัตถุประสงค์หลักภายใต้การเปลี่ยนแปลงที่รวดเร็วในด้านต่างๆ ของประเทศและของโลกธุรกิจปัจจุบัน ที่เกี่ยวข้องกับการบริหารการควบคุมและจัดการกับความเสี่ยงและการตรวจสอบภายใน โดยใช้ฐานความเสี่ยงเป็นหลัก

### 2. ประโยชน์ของการกำกับดูแลกิจการที่ดี

เพื่อให้องค์กรบรรลุวัตถุประสงค์หลักในเรื่องการบริหารและจัดการความเสี่ยงที่ดี โดยมีปรัชญาทางด้านคุณธรรมเป็นแกนนำในการทำงานที่ดี เพื่อให้ได้รับความเชื่อถือ ซึ่งจะช่วยให้องค์กรก้าวไปข้างหน้าได้อย่างมั่นคงและยั่งยืน ซึ่งเป็นแนวทางที่สำคัญยิ่งของการบริหารองค์กรต่าง ๆ ในยุคปัจจุบัน

### 3. ปรัชญา หลักการ และวิธีการ ของการกำกับดูแลกิจการที่ดี

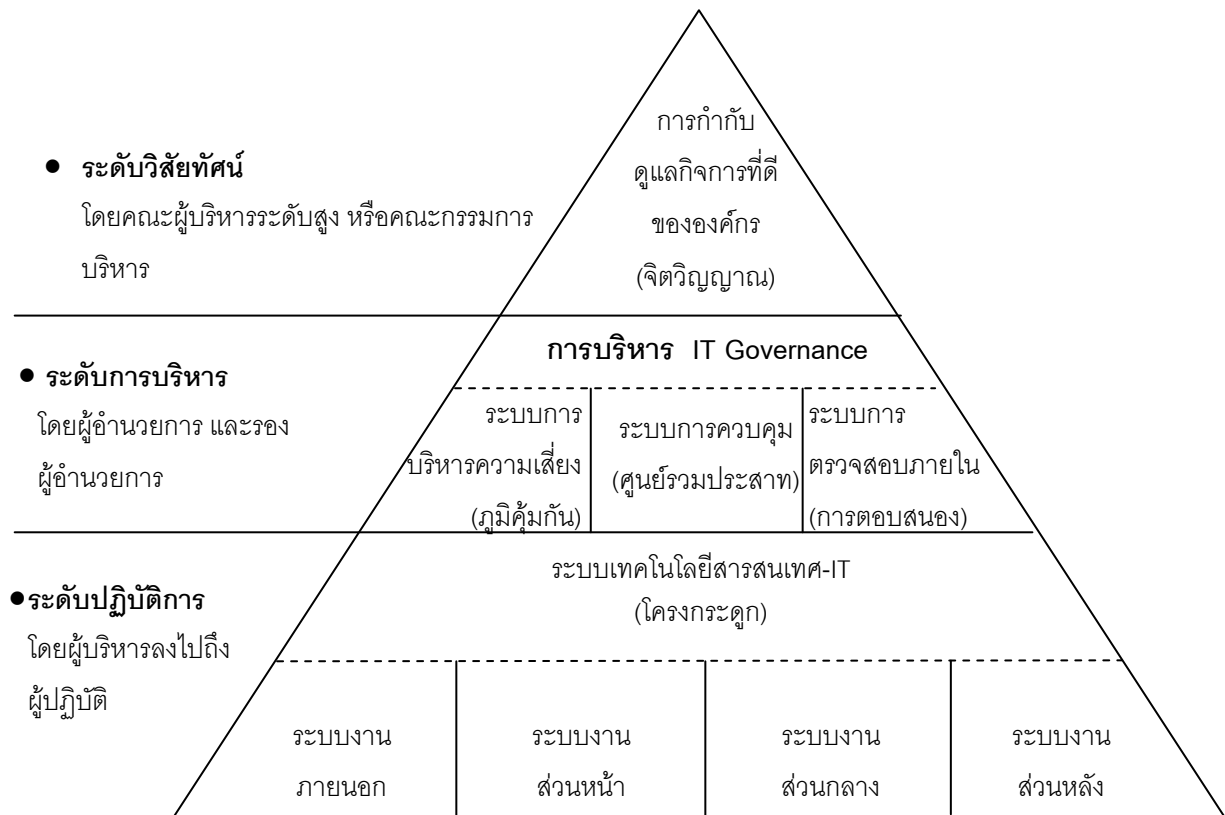
**ปรัชญา** คือ ความเชื่อที่มาจากรากฐานแห่งความจริงที่ว่า การบริหารและการจัดการที่ดีคือ ความยุติธรรม ความโปร่งใส ความสามารถในการบริหาร การจัดการความเสี่ยงต่าง ๆ ที่มีต่อองค์กรได้อย่างเป็นรูปธรรมเป็นที่ยอมรับของผู้ที่เกี่ยวข้อง ความชัดเจนในภาระหน้าที่ความรับผิดชอบ และดุลอำนาจในองค์กรเพื่อนำองค์กรไปสู่เป้าหมายและวัตถุประสงค์ที่กำหนด

**หลักการ** คือ มาตรฐานของกฎเกณฑ์ที่ตั้งไว้เพื่อเป็นแก่นหรือเป็นโครงสร้างของความคิดและรูปแบบ (Model) ต่างๆ ที่ถูกพัฒนาต่อมาจากปรัชญาเพื่อก้าวต่อไปสู่วิธีปฏิบัติที่เป็นรูปธรรม

**วิธีการ** คือ รายละเอียดแห่งการปฏิบัติที่เป็นไปตามหลักการที่กำหนดขึ้นเพื่อที่ นำไปสู่กระบวนการแห่งความสำเร็จของการบริหารงานความเสี่ยงต่าง ๆ ซึ่งจะนำไปสู่เป้าหมายและวัตถุประสงค์ที่กำหนดขึ้นขององค์กร

โดยรวมแล้ววิธีการต้องอาศัยหลักการทำให้ทุกองค์ประกอบเกื้อกูลกัน อันเป็นแนวความคิดใหม่ในการบริหารองค์กร ซึ่งเป็นที่ยอมรับกันทั่วไปในโลกธุรกิจและการบริหารในปัจจุบันที่ว่าด้วย Good Corporate Governance การบริหารความเสี่ยง และการตรวจสอบภายในตามฐานความเสี่ยง

## กรอบการกำกับดูแลกิจการที่ดีขององค์กร



การขับเคลื่อนเพื่อให้เกิดการปฏิบัติตามหลักการการกำกับดูแลกิจการที่ดีนี้ขึ้นกับพลังร่วม (Synergy) จากค่านิยมใหม่โดยมีความซื่อสัตย์ต่อตนเองและวิชาชีพภายใต้การกำกับของคณะผู้บริหารระดับสูง คณะกรรมการบริหาร ผู้อำนวยการ รองผู้อำนวยการ และพนักงานทุกระดับ ตามบทบาทของตนเองดังนี้

- คณะผู้บริหารและคณะทำงานชุดต่าง ๆ ขององค์กร เป็น “เจ้าภาพ (Ownership)” ของการกำกับดูแลกิจการที่ดีโดยรวมในภาพกว้างและลึกทั่วทั้งองค์กร
- ผู้อำนวยการและ/หรือรองผู้อำนวยการเป็น “ผู้นำ (Leadership)” ของการกำกับดูแลกิจการที่ดีสำหรับทุกสายงานทั้งองค์กร
- ผู้บริหารและพนักงาน เป็น “หุ้นส่วน (Partnership)” ของการกำกับดูแลกิจการที่ดี
- องค์กรเป็น “ผู้สนับสนุน (Sponsorship)” ของการกำกับดูแลกิจการที่ดี
- สังคมไทย เป็น “ผู้มีผลประโยชน์ (Stakeholder)” ของการกำกับดูแลกิจการที่ดี

แต่กลไกที่สำคัญที่สุดที่จะนำไปสู่การแปลงรูปให้เกิดการกำกับดูแลกิจการที่ดีในองค์กรนั้นคือ บทบาท และความเป็นผู้นำของคณะผู้บริหารในระดับกรรมการบริหารในการกำหนดวิสัยทัศน์และพันธกิจ เพื่อให้คณะผู้บริหารโดยการนำของผู้อำนวยการและรองผู้อำนวยการ สามารถกำหนดนโยบายบริหารคุณค่าร่วม จัดทำ แผนการพัฒนาทรัพยากรบุคคล ระบบงาน และระบบข้อมูลสารสนเทศอย่างต่อเนื่อง เพื่อนำพาองค์กรไปสู่ ความสำเร็จในการบรรลุวัตถุประสงค์หลักขององค์กรต่อไป

### กระบวนการขับเคลื่อนการกำกับดูแลกิจการที่ดีขององค์กร

กระบวนการขับเคลื่อนการกำกับดูแลกิจการที่ดีขององค์กร ให้เกิดเป็นรูปธรรม บรรทัดฐาน (Norm) วัฒนธรรม (Culture) และจิตวิญญาณ (Spiritual) ในที่สุดนั้นประกอบด้วย

#### 1. กำหนดโครงสร้าง รูปแบบของการกำกับดูแลกิจการที่ดี

โดยความเห็นชอบของคณะผู้บริหารองค์กร พร้อมจัดทำเส้นทางขับเคลื่อน (Roadmap) จากคณะผู้บริหารองค์กร

#### 2. ระบบการวัดผล

คณะผู้บริหาร และคณะทำงานฯ ขององค์กร ร่วมกันกำหนดวิธีการวัดผลการขับเคลื่อนการกำกับดูแลกิจการที่ดีขององค์กร

#### 3. การวิเคราะห์

คณะผู้บริหารองค์กร วิเคราะห์ถึงเหตุและปัจจัยที่ทำให้การขับเคลื่อนการกำกับดูแลกิจการที่ดีขององค์กร คลาดเคลื่อนจากเป้าหมายที่ได้ตั้งไว้

#### 4. การพัฒนา

คณะผู้บริหาร นำการพัฒนากระบวนการปฏิบัติตามการกำกับดูแลกิจการที่ดีขององค์กรให้บังเกิดผลดีอย่างต่อเนื่อง และมีขีดความสามารถในการสนองตอบต่อความเป็นพลวัตของสภาพแวดล้อม

#### 5. การควบคุม

คณะผู้บริหารองค์กร มีกลไกและกระบวนการที่จะเกิดความแน่ใจว่ากระบวนการควบคุมยังเกิดประสิทธิผลอยู่ เพื่อบรรลุเป้าหมายที่ดี และที่ต้องได้รับมอบหมายในอนาคต

### การกำกับและบริหารงานที่ดีควรเข้าใจความเสี่ยงขององค์กร

1. ประสิทธิภาพ ประสิทธิภาพ ขององค์กร จะประสบความสำเร็จได้ดีเป็นที่ยอมรับต่อผู้ที่มีผลประโยชน์ร่วม (Stakeholders) ทุกฝ่ายได้ ก็ต่อเมื่อองค์กรมีหลักการกำกับและบริหารงานที่ดี ซึ่งเป็นแม่บทของการบริหารความเสี่ยง (Risk Management) อันประกอบไปด้วย การควบคุมความเสี่ยง (Risk control) และการตรวจสอบโดยใช้ฐานความเสี่ยง (Risk-based Audit Approach) เป็นสำคัญและเป็นสากล

2. การบริหาร คือ การทำสิ่งที่เป็นไปไม่ได้ให้เป็นไปได้ แต่สิ่งที่สำคัญสำหรับผู้บริหารคือการครอง “ใจ” ผู้ร่วมงานและผู้เกี่ยวข้อง ด้วยการชี้แนะของผู้นำด้านต่าง ๆ และการบริหารความเสี่ยงต่าง ๆ ทุกระดับของสำนักงานบุคลากรอย่างมีประสิทธิภาพ เพื่อสร้างศรัทธา และจิตวิญญาณในการทำงานอย่างผู้เป็นเจ้าของร่วมจากพนักงานทุกคนทุกระดับ

3. องค์กรควรสร้างจิตสำนึกในจริยธรรม ความมุ่งมั่น ความรู้ความสามารถในการควบคุมความเสี่ยง ด้วยความเสียสละและความกล้าหาญให้เกิดขึ้นกับพนักงานทุกระดับ เพื่อสร้างจิตวิญญาณของความรู้สึกในการทุ่มเทการทำงาน เสมือนหนึ่งเป็นเจ้าของสำนักงานบุคลากรร่วมกันเพื่อความสำเร็จและความยอมรับของกรมบุคลากรและผู้ที่เกี่ยวข้อง

4. ควรพิจารณาสร้างหลักเกณฑ์และแนวทางการกำกับดูแลที่ดี ทั้งนี้ ควรจัดให้มีคณะกรรมการต่าง ๆ ให้ครบถ้วน

5. ความหมายของคำว่า “ความเสี่ยง” ขององค์กร ก็คือเหตุการณ์/การกระทำใด ๆ รวมทั้งกิจกรรมที่อาจเกิดขึ้นจากการดำเนินงาน บริหารงาน ที่จะส่งผลหรือโอกาสที่เกิดความเสียหายหรือกระทบต่อประสิทธิผล และประสิทธิภาพหรือความล้มเหลวให้กับเป้าหมายขององค์กรหรือวัตถุประสงค์ขององค์กรได้

6. การบริหารความเสี่ยง คือ “การควบคุมและบริหารกิจกรรมรวมทั้งกระบวนการปฏิบัติงานและลดโอกาสที่องค์กรจะเกิดความเสียหาย ให้มีระดับของความเสี่ยงและขนาดของความเสียหายต่อวัตถุประสงค์และเป้าหมายที่จะเกิดขึ้นในอนาคตให้อยู่ในระดับที่องค์กรยอมรับได้ ประเมินได้ และตรวจสอบได้”

7. การประเมินความเสี่ยง การบริหารความเสี่ยง ตลอดจนการควบคุมและการตรวจสอบ ซึ่งเป็นกระบวนการหนึ่งของการวิเคราะห์ความเสี่ยง เป็นการวิเคราะห์ถึงมูลเหตุที่อาจนำไปสู่ความเสียหาย หรือความสำเร็จของงาน หรือกิจกรรมอย่างเป็นระบบ ประกอบไปด้วยตัวแปรของ ความเสี่ยง 2 อย่างคือ มูลเหตุที่นำไปสู่ความเสียหาย และโอกาสที่จะเกิดเหตุการณ์นั้น

8. ความเข้าใจในบทบาทการกำกับและบริหารงานที่ดีควบคู่กับการวิเคราะห์ความเสี่ยงอย่างเป็นระบบ จึงเป็นสิ่งที่ไม่อาจแยกจากกันได้ นั่นคือผู้บริหารที่ดีต้องเข้าใจถึงความสัมพันธ์และความโยงใยระหว่างปัจจัยต่อไปนี้

- การกำกับดูแลกิจการที่ดี กับ
- การวิเคราะห์และบริหารความเสี่ยง และ
- การควบคุมการบริหารและจัดการกับกิจกรรมที่ก่อให้เกิดความเสี่ยง และ
- การตรวจสอบภายในโดยใช้ฐานความเสี่ยงเป็นหลักในกระบวนการปฏิบัติงาน

## การจัดตั้ง IT Strategy Committee และ IT Steering Committee

การจัดตั้งคณะกรรมการทางด้านกลยุทธ์เทคโนโลยีสารสนเทศ IT Strategy Committee ถือได้ว่าเป็นความสำคัญในการเริ่มต้นกระบวนการบริหารเทคโนโลยีสารสนเทศตามแนวทาง IT Governance โดยความรับผิดชอบหลักคือการมุ่งไปที่การเพิ่มคุณค่าในการใช้เทคโนโลยีสารสนเทศ (IT Value) การบริหารความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT Risk) และผลการปฏิบัติงานอันเนื่องมาจากการใช้เทคโนโลยีสารสนเทศ (IT Performance)

1. IT Governance ได้ระบุถึงความสำคัญของเทคโนโลยีสารสนเทศที่มีต่อการดำเนินธุรกิจในปัจจุบันว่า
  - 1.1. องค์กรส่วนใหญ่ในปัจจุบันไม่สามารถจะดำรงอยู่ได้ถ้าไม่มีเทคโนโลยีสารสนเทศโดยเฉพาะในกลุ่มที่ดำเนินธุรกิจ ด้านการสื่อสาร ธุรกิจการบิน ธนาคาร พลังงาน ตลาดหลักทรัพย์ เป็นต้น
  - 1.2. รูปแบบทางธุรกิจในปัจจุบันที่สามารถกำหนดขนาดได้ด้วยเทคโนโลยีสารสนเทศ
  - 1.3. ต้นทุนทางเทคโนโลยีสารสนเทศที่มีความสำคัญต่อผลกำไรของธุรกิจ อันเนื่องมาจากการลงทุนทางด้านเทคโนโลยีสารสนเทศ
  - 1.4. การดำเนินธุรกิจอาจไม่สามารถทำได้อย่างเต็มที่ในการบรรลุเป้าหมายทางธุรกิจถ้าขาดการสนับสนุนการทำงานจากระบบเทคโนโลยีสารสนเทศอัตโนมัติ
  - 1.5. ความจำเป็นในการตอบสนองระดับการบริการ ที่ได้มีการตกลงกับลูกค้ารวมทั้งการปฏิบัติให้สอดคล้องกับข้อบังคับต่าง ๆ

ผู้บริหารระดับสูงขององค์กรต่าง ๆ ในฐานะกรรมการขององค์กร ซึ่งถือได้ว่าเป็นตัวแทนของผู้ถือหุ้นได้ตระหนักถึงแนวโน้มและความจำเป็นของการสร้างคุณค่าในการใช้งานเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยเฉพาะความสำคัญของข้อมูลที่ผู้บริหารใช้ในการตัดสินใจซึ่งจำเป็นจะต้องเชื่อถือได้ และมีการรักษาความปลอดภัยของข้อมูลที่เหมาะสม และจุดนี้ที่ทำให้ข้อมูลที่ดีว่าเป็น Intangible Asset สามารถสร้างคุณค่าให้แก่ธุรกิจในการเพิ่มมูลค่าในตลาด และการมุ่งไปสู่การดำเนินงานที่มีศักยภาพอย่างเต็มที่ไม่ใช่เพียงแค่อพยรรอดเท่านั้น

IT Governance ไม่สามารถจะจัดการแยกมาโดดเดี่ยวได้แต่ควรจะต้องรวมเป็นส่วนหนึ่งของการบริหาร และจัดการที่ดี หรือ ธรรมชาติขององค์กร (Enterprise Governance) โดยจำเป็นต้องให้คณะกรรมการบริหาร เน้นย้ำและให้ความสำคัญเพื่อให้มั่นใจว่า ผลตอบแทนจากการลงทุนทางด้านเทคโนโลยี

สารสนเทศสามารถสร้างคุณค่าได้สูงสุด และและมีการบริหารความเสี่ยงที่เหมาะสม เพื่อให้ตอบสนองความต้องการทางธุรกิจและบรรลุเป้าหมาย

## 2. บทบาทของคณะกรรมการบริหารที่เกี่ยวข้องกับ IT Governance

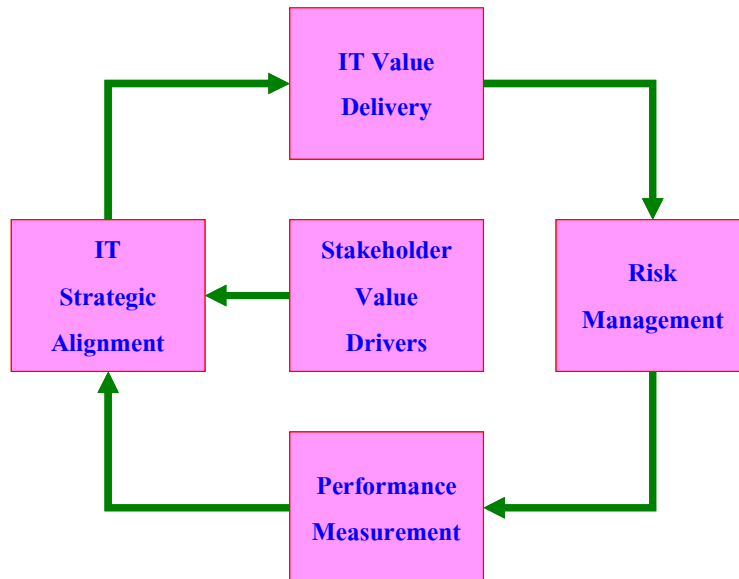
บทบาทของคณะกรรมการบริหารที่เกี่ยวข้องกับ IT Governance จึงสามารถทำงานผ่านทาง IT Strategy Committee และ IT Steering Committee และเป็นผู้กำหนด Business Policy, Information Policy, IT Policy, IT Governance Organization, IT Governance Process และ Measurements ดังรายละเอียดของระดับที่เกี่ยวข้องและหน้าที่ความรับผิดชอบดังนี้

IT Strategy Committee ตัวแทนของคณะกรรมการบริหารองค์กร (Board)	IT Steering Committee CIO และ C-Level ขององค์กร
<ol style="list-style-type: none"> <li>1. กำหนดทิศทาง ทางด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับกลยุทธ์ทางด้านเทคโนโลยีสารสนเทศให้แก่ผู้บริหาร</li> <li>2. เป็นผู้ผลักดัน IT Governance ในระดับคณะกรรมการบริหาร (Board)</li> <li>3. ให้คำปรึกษาแก่คณะกรรมการบริหารองค์กร และผู้บริหารในด้านกลยุทธ์เทคโนโลยีสารสนเทศ</li> <li>4. รับมอบหมายจากคณะกรรมการบริหารองค์กรให้เป็นผู้ชี้แนะกลยุทธ์ด้านเทคโนโลยีสารสนเทศและเตรียมขออนุมัติ</li> <li>5. เน้นประเด็นที่เกี่ยวข้องกับกลยุทธ์ ทั้งในปัจจุบันและอนาคต</li> <li>6. ให้คำแนะนำและข้อมูลเชิงลึกในด้านเทคโนโลยีสารสนเทศแก่ Steering Committee และผู้ที่เกี่ยวข้องในประเด็นที่เกี่ยวข้อง               <ol style="list-style-type: none"> <li>6.1. การพัฒนาของเชิงลึกในด้านเทคโนโลยีสารสนเทศในมุมมองทางด้านธุรกิจที่เกี่ยวข้อง</li> <li>6.2. การพิจารณาถึงความสอดคล้องของเชิงลึกในด้านเทคโนโลยีสารสนเทศกับทิศทางของธุรกิจ</li> </ol> </li> </ol>	<ol style="list-style-type: none"> <li>1. อนุมัติแผนโครงการและงบประมาณ รวมทั้งจัดลำดับความสำคัญและ Milestones</li> <li>2. กำหนดและจัดหา ทรัพยากรที่ต้องใช้</li> <li>3. คอยพิจารณาอย่างต่อเนื่องว่าโครงการที่ทำนั้นสามารถบรรลุตามความต้องการขององค์กร รวมทั้งมีการประเมิน Business Case อีกครั้ง เพื่อว่าต้องมีการปรับเปลี่ยน</li> <li>4. พิจารณาติดตามแผนงานของโครงการว่าให้ผลตามที่คาดหวังในระยะเวลาและงบประมาณที่กำหนด</li> <li>5. ตัดสินใจการลงทุนทางด้านเทคโนโลยีสารสนเทศโดยรวมและจะจัดสรรต้นทุนอย่างไร</li> <li>6. อนุมัติรูปแบบ IT Architecture ขององค์กรและทำให้เกิดความสอดคล้องกัน</li> <li>7. พิจารณาติดตามการใช้ทรัพยากรและความขัดแย้งในการจัดลำดับความสำคัญที่เกิดขึ้นระหว่างหน่วยงานเทคโนโลยีสารสนเทศกับส่วนงานต่าง ๆ</li> <li>8. ให้คำแนะนำและความจำเป็นในการปรับเปลี่ยนแผนกลยุทธ์ เช่น การจัดลำดับความสำคัญงบประมาณ แนวทางการใช้เทคโนโลยี</li> </ol>

<p>6.3. การบรรลุวัตถุประสงค์ทางด้านกลยุทธ์ของเชิงลึกในด้านเทคโนโลยีสารสนเทศ</p> <p>6.4. การมีทรัพยากรทางด้านเทคโนโลยีสารสนเทศที่เพียงพอและเหมาะสม รวมทั้งทักษะที่จำเป็นและ IT Infrastructure เพื่อให้สามารถบรรลุเป้าหมายขององค์กร</p> <p>6.5. การรักษาระดับทางด้านเทคโนโลยีสารสนเทศให้อยู่ในระดับที่เหมาะสม ซึ่งรวมถึงบทบาท คุณค่าและประโยชน์ที่ได้รับจากการใช้บริการด้านเทคโนโลยีสารสนเทศจากการลงทุนทางด้านเทคโนโลยีสารสนเทศ</p> <p>6.6. พิจารณาความก้าวหน้าของโครงการเชิงลึกในด้านเทคโนโลยีสารสนเทศขนาดใหญ่</p> <p>6.7. พิจารณาความก้าวหน้าของโครงการเชิงลึกในด้านเทคโนโลยีสารสนเทศขนาดใหญ่</p> <p>6.8. ผลของธุรกิจที่ได้รับจากการใช้เชิงลึกในด้านเทคโนโลยีสารสนเทศ (สามารถสร้างคุณค่าให้แก่องค์กรได้ตามที่คาดไว้)</p> <p>6.9. พิจารณาความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ รวมทั้งความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามนโยบายด้านเทคโนโลยีสารสนเทศ</p> <p>6.10. พิจารณาถึงการจำกัดความเสี่ยงทางด้านเทคโนโลยีสารสนเทศผสมผสานกับความเสี่ยงอื่นที่เกี่ยวข้อง</p>	<p>การใช้ทรัพยากร เป็นต้น</p> <p>9. สื่อสารเป้าหมาย/ กลยุทธ์ ให้แก่ project team ต่างๆ</p> <p>10. เป็นผู้รับผิดชอบหลักและผลักดันด้าน IT Governance</p> <p>11. ให้ความช่วยเหลือแก่ทีมผู้บริหารในการพัฒนากลยุทธ์ด้านเทคโนโลยีสารสนเทศ</p> <p>12. ติดตามการบริหารงานด้านเทคโนโลยีสารสนเทศ (Day-to-Day) และโครงการด้านเทคโนโลยีสารสนเทศ</p> <p>13. เน้นประเด็นที่เกี่ยวข้องกับการปฏิบัติงานเพื่อให้เกิดรูปธรรมทางด้านประสิทธิผลและประสิทธิภาพ โดยเปรียบเทียบกับตัวชี้วัดที่เหมาะสม</p>
---	--

สามารถอธิบายด้วยภาพและแจกแจงรายละเอียดถึงหน้าที่ความรับผิดชอบของแต่ละระดับในแต่ละบทบาทได้ดังนี้

### บทบาทหน้าที่ของคณะกรรมการองค์กรเกี่ยวกับ ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ



#### 1. Board of directors

##### 1.1. Board of Directors

###### ความสอดคล้องของกลยุทธ์ (Strategic Alignment)

- 1) กำกับฝ่ายบริหารว่าได้มีการกำหนดกระบวนการในการวางแผนกลยุทธ์ที่ดี
- 2) เห็นชอบและอนุมัติกลยุทธ์ทางด้าน IT ที่สอดคล้องกับความต้องการขององค์กร และ

ของธุรกิจ

- 3) ให้การรับรองว่าโครงสร้างของ IT Organization สามารถรองรับและตอบสนอง

รูปแบบของธุรกิจ และทิศทางในอนาคต

###### การได้ผลลัพธ์ที่เพิ่มคุณค่าให้ธุรกิจ (Value Delivery)

- 1) กำกับฝ่ายบริหารว่าได้มีการกำหนดกระบวนการ และแนวทางในการปฏิบัติที่ช่วยให้

IT สามารถสร้างคุณค่าให้แก่ธุรกิจ

- 2) กำกับดูแลเพื่อให้มั่นใจว่าการลงทุนทางด้าน IT (IT Investment) ที่ยอมรับได้นั้น มี

ความสมดุลในการบริหารความเสี่ยงเทียบกับประโยชน์ที่ได้รับตามงบประมาณ

การจัดการทรัพยากรด้าน IT (IT Resource Management)

- 1) ติดตามฝ่ายบริหารว่ามีจัดการทรัพยากรทางด้าน IT อย่างไรเพื่อให้สามารถบรรลุเป้าหมายได้
- 2) กำกับดูแลความสมดุลในการจัดการด้านการลงทุนทางด้าน IT ที่ทำให้องค์กรสามารถดำเนินธุรกิจได้พร้อมกับการสร้างความเติบโตด้วย

การบริหารความเสี่ยง (Risk Management)

- 1) ตระหนักถึงความเสี่ยงที่มากับ IT และการจำกัดความเสี่ยงให้อยู่ระดับที่ยอมรับได้
- 2) ประเมินผลฝ่ายจัดการในการติดตามความเสี่ยงทางด้าน IT

การวัดผลการดำเนินงาน (Performance Management)

- 1) ประเมินผลการดำเนินงานของผู้บริหารระดับสูงในด้านของกลยุทธ์ IT ในทางปฏิบัติ
- 2) ทำงานร่วมกับผู้บริหารในการกำหนดและติดตามผลการดำเนินงานด้าน IT ใน

ระดับบน

## 1.2. IT Strategy Committee

ความสอดคล้องของกลยุทธ์ (Strategic Alignment)

- 1) กำหนดทิศทางกลยุทธ์ทางด้าน IT และความสอดคล้องกับกลยุทธ์ของธุรกิจ
- 2) ให้แนวทางในการกำหนดนโยบาย เช่น ด้านความเสี่ยง ด้านงบประมาณ การสร้าง

พันธมิตร/คู่สัญญา เป็นต้น

- 3) ตรวจสอบว่ามีการปฏิบัติตามกลยุทธ์ เช่น การบรรลุเป้าหมาย/วัตถุประสงค์ทางกล

ยุทธ์ที่กำหนด

การได้ผลลัพธ์ที่เพิ่มคุณค่าให้ธุรกิจ (Value Delivery)

- 1) ยืนยันได้ว่า IT/ business architecture มีความเหมาะสมในการสร้างคุณค่าทางธุรกิจได้สูงสุด
- 2) กำกับการใช้ IT ในการสร้างคุณค่าให้แก่องค์กร
- 3) พิจารณาผลตอบแทนจากการลงทุนทางด้าน IT และศักยภาพในการแข่งขัน

การจัดการทรัพยากรด้าน IT (IT Resource Management)

- 1) ให้คำชี้แนะในการกำหนดทิศทางในการจัดหา และการใช้ทรัพยากรทางด้าน IT
- 2) พิจารณาการจัดหา/จัดสรรเงินทุนสำหรับ IT ในภาพรวมทั้งหมดขององค์กร

การบริหารความเสี่ยง (Risk Management)

## เสี่ยงด้าน IT

- 1) กำกับฝ่ายบริหารในการกำหนดให้มีทรัพยากรที่เหมาะสมเพื่อใช้ในการบริหารความเสี่ยงด้าน IT
- 2) พิจารณาความเสี่ยงในด้านการลงทุนทางด้าน IT
- 3) ยืนยันได้ว่าสามารถจัดการความเสี่ยงวิกฤตต่างๆได้

### การวัดผลการดำเนินงาน (Performance Management)

## ยุทธศาสตร์ที่กำหนด

- 1) ตรวจสอบว่ามีการปฏิบัติตามกลยุทธ์ เช่น การบรรลุเป้าหมาย/วัตถุประสงค์ทางกลยุทธ์ที่กำหนด
- 2) ทบทวนการวัดผลทางด้าน IT และผลของการใช้งานทางด้าน IT ที่ส่งผลต่อธุรกิจ

## 2. Executive Management

### 2.1. CEO

#### ความสอดคล้องของกลยุทธ์ (Strategic Alignment)

- 1) ประสานเชื่อมโยงกลยุทธ์ IT
- 2) ประสานเชื่อมโยงการดำเนินงานด้าน IT เข้ากับการดำเนินงานทางธุรกิจ
- 3) สื่อสารเชื่อมโยงกลยุทธ์และเป้าหมายลงไปตามลำดับชั้นในองค์กร
- 4) เป็นสื่อเชื่อมโยงความจำเป็นทางธุรกิจเข้ากับความจำเป็นทางเทคโนโลยี

#### การได้ผลลัพธ์ที่เพิ่มคุณค่าให้ธุรกิจ (Value Delivery)

- 1) กำกับการมีต้นทุนทางด้าน IT ที่เหมาะสม
- 2) กำหนดความรับผิดชอบร่วมของธุรกิจในการลงทุนทางด้าน IT
- 3) กำกับเพื่อให้มั่นใจว่างบประมาณทางด้าน IT และแผนการลงทุนสอดคล้องกับความเป็นจริงและบรรจุอยู่ในแผนการเงิน

## เป็นจริงและบรรจุอยู่ในแผนการเงิน

#### การจัดการทรัพยากรด้าน IT (IT Resource Management)

## ที่สุด

- 1) กำกับเพื่อให้มั่นใจว่าบริษัทมีการใช้ประโยชน์ของข้อมูลและความรู้ได้คุ้มค่ามากที่สุด
- 2) กำหนดลำดับความสำคัญของธุรกิจ (business priorities) และจัดสรรทรัพยากรเพื่อให้การใช้งานทางด้าน IT เกิดผลสูงสุด
- 3) จัดโครงสร้างองค์กร และกำหนดความรับผิดชอบ เพื่อให้สามารถนำพากลยุทธ์ทางด้าน IT ไปสู่การปฏิบัติได้

4) กำหนดบทบาทของ CIO และให้การสนับสนุนเพื่อให้มั่นใจว่า CIO จะต้องเป็นส่วนสำคัญในการดำเนินธุรกิจและเป็นผู้บริหารที่มีส่วนร่วมในการตัดสินใจ

#### การบริหารความเสี่ยง (Risk Management)

1) ให้การยอมรับในกรอบของการบริหารความเสี่ยง และการควบคุม รวมทั้งการกำกับดูแลที่ดี (governance)

2) ให้ความรับผิดชอบทางด้านการจัดการความเสี่ยงเข้าไปฝังตัวอยู่ในองค์กร

3) ติดตามความเสี่ยงทางด้าน IT และให้การยอมรับความเสี่ยงทางด้าน IT ที่ยอมรับได้ (residual IT risks)

#### การวัดผลการดำเนินงาน (Performance Management)

1) ให้การรับรองผลของการดำเนินงานด้าน IT การควบคุมและความเสี่ยงของ IT รวมทั้งการยอมรับการตัดสินใจที่เป็นอิสระทางด้าน IT ในเรื่องสำคัญๆ

2) ทำงานร่วมกับ CIO ในการกำหนด IT Balanced Scorecard เพื่อให้มั่นใจว่ามีการเชื่อมโยงกับเป้าหมายทางธุรกิจ

## 2.2. Business Executive

#### ความสอดคล้องของกลยุทธ์ (Strategic Alignment)

1) เข้าใจถึงรูปแบบ IT organization ขององค์กร รวมทั้งรูปแบบ infrastructure และความสามารถ (capabilities) ทางด้าน IT

2) ผลักดันการกำหนดความต้องการทางธุรกิจและเป็นเจ้าของ

3) สนับสนุนและเป็น project sponsor ในโครงการ IT ที่มีความสำคัญ

#### การได้ผลลัพธ์ที่เพิ่มคุณค่าให้ธุรกิจ (Value Delivery)

1) อนุมัติและควบคุม service levels

2) เป็นลูกค้าที่รับบริการทางด้าน IT

3) กำหนดและนำการบริการทางด้าน IT ใหม่ๆมาใช้

4) ประเมินผลถึงประโยชน์ที่ได้รับจากการลงทุนทางด้าน IT ที่รับผิดชอบอยู่ และเผยแพร่ให้ทราบทั่วกัน

#### การจัดการทรัพยากรด้าน IT (IT Resource Management)

1) จัดสรรทรัพยากรที่จำเป็นในการควบคุมและกำกับการดำเนินงานด้าน IT (IT Governance) ในการจัดการโครงการและในการดำเนินงานต่างๆ

### การบริหารความเสี่ยง (Risk Management)

- 1) ประเมินผลกระทบทางธุรกิจและนำเสนอเข้าสู่กระบวนการจัดการความเสี่ยงขององค์กร

### การวัดผลการดำเนินงาน (Performance Management)

- 1) ให้การยอมรับและอนุมัติ IT Balanced Scorecard
- 2) ติดตาม/พิจารณา service levels
- 3) ให้ความสำคัญกับการจัดการปัญหาการดำเนินงานทางด้าน IT ทั้งในการระบุปัญหาและการแก้ไข

## 2.3. CIO

### ความสอดคล้องของกลยุทธ์ (Strategic Alignment)

- 1) ผลักดันการพัฒนากลยุทธ์ทางด้าน IT และการนำไปปฏิบัติ รวมทั้งให้สามารถสร้างคุณค่าตามที่มีการวัดผลได้ตรงตามเวลา ในงบประมาณที่มีอยู่ ทั้งในปัจจุบัน และอนาคต
- 2) นำนโยบายและมาตรฐานทางด้าน IT ไปสู่การปฏิบัติ
- 3) ให้ความรู้ความเข้าใจแก่ผู้บริหารอื่นๆในเรื่องของระดับการพึ่งพาของ IT ที่มีต่อธุรกิจ ต้นทุนทางด้าน IT ที่เกี่ยวข้อง ประเด็นและมุมมองต่างๆทางเทคโนโลยี รวมทั้งความสามารถของ IT ที่มีอยู่ (IT Capabilities)

### การได้ผลลัพธ์ที่เพิ่มคุณค่าให้ธุรกิจ (Value Delivery)

- 1) ชี้แจงและแสดงให้เห็นถึงคุณค่าที่ IT สร้างให้แก่องค์กร
- 2) หาแนวทางในการเพิ่มคุณค่าจากการใช้ IT โดยใช้วิธีแบบเชิงรุก
- 3) เชื่อมโยงงบประมาณทางด้าน IT เข้ากับวัตถุประสงค์และเป้าหมายเชิงกลยุทธ์
- 4) สามารถจัดการกับความคาดหวังทางธุรกิจ และของผู้บริหารที่มีต่อ IT
- 5) กำหนดระเบียบปฏิบัติที่เข้มงวดในการบริหารโครงการ

### การจัดการทรัพยากรด้าน IT (IT Resource Management)

- 1) กำหนด IT Infrastructure ที่ส่งเสริมให้มีการใช้ข้อมูลทางธุรกิจร่วมกันในระดับต้นหน้าที่เหมาะสม
- 2) สามารถจัดให้มีทรัพยากรทางด้าน IT ที่เหมาะสม รวมทั้งความรู้ความชำนาญ และโครงสร้างพื้นฐาน (infrastructure) ที่จะสามารถทำให้บรรลุวัตถุประสงค์ตามกลยุทธ์ที่กำหนดได้

3) มีการกำหนดบทบาท และการจัดการบุคลากรที่มีความสำคัญในการสร้างคุณค่าสูงสุดจากการใช้ IT ได้อย่างเหมาะสม

4) กำหนดมาตรฐานของ architecture และ เทคโนโลยี

การบริหารความเสี่ยง (Risk Management)

1) ประเมินความเสี่ยง และมีการลดความเสี่ยงได้อย่างมีประสิทธิภาพ และสามารถแจ้งความเสี่ยงให้ผู้เกี่ยวข้องหรือมีส่วนได้ส่วนเสียได้รับทราบ

2) มีการกำหนดบทบาท และการจัดการบุคลากรที่มีความสำคัญในการจัดการกับความเสี่ยงด้าน IT ได้อย่างเหมาะสม

การวัดผลการดำเนินงาน (Performance Management)

1) รับผิดชอบการดำเนินงานทางด้าน IT ในแต่ละวัน (day-to-day management) และ ทบทวนกระบวนการทางด้าน IT และการควบคุมทางด้าน IT อยู่เสมอ

2) นำ IT Balanced Scorecard ไปสู่การปฏิบัติโดยมีตัวชี้วัดผลการดำเนินงานที่ไม่มากนัก แต่มีความละเอียดและชัดเจนโดยมีการประสานเชื่อมโยงโดยตรงกับกลยุทธ์

### 3. Committees ที่ประสานงานและสนับสนุนการทำงานของ Executive และ CIO

#### 3.1. Steering Committee

ความสอดคล้องของกลยุทธ์ (Strategic Alignment)

1) จัดลำดับความสำคัญของโครงการต่าง ๆ

2) ประเมินแต่ละโครงการว่ามีความสอดคล้องและเหมาะสมกับกลยุทธ์หรือไม่

3) พิจารณา/ทบทวน IT portfolio เพื่อให้เกิดความต่อเนื่องกับกลยุทธ์

การได้ผลลัพธ์ที่เพิ่มคุณค่าให้ธุรกิจ (Value Delivery)

1) พิจารณานุมัติและให้เงินทุนกับแนวคิดการพัฒนาปรับปรุงใหม่ ๆ และประเมินว่าจะช่วยพัฒนากระบวนการทางธุรกิจได้อย่างไร

2) ให้มั่นใจว่าได้มีการระบุต้นทุนที่เกี่ยวข้องกับ IT ทั้งหมด รวมทั้งมีการวิเคราะห์ต้นทุนเทียบกับประโยชน์ที่ได้รับ (cost/benefit analysis)

3) มีการพิจารณาทบทวน IT Portfolio เพื่อการจัดการต้นทุนที่เหมาะสม

การจัดการทรัพยากรด้าน IT (IT Resource Management)

1) จัดการสมดุลของการลงทุนระหว่างการลงทุนเพื่อสนับสนุนกิจกรรมในปัจจุบันกับการลงทุนเพื่อสร้างความเติบโตให้ธุรกิจ

#### การบริหารความเสี่ยง (Risk Management)

1) กำกับให้มีการจัดการความเสี่ยงในทุกๆโครงการ  
2) สนับสนุนและเป็น sponsor ที่เกี่ยวข้องกับการบริหารความเสี่ยง และการควบคุม รวมทั้งการกำกับดูแลที่ดี (governance)

3) เป็นผู้ตัดสินใจในเรื่องของ IT Governance ที่สำคัญ

#### การวัดผลการดำเนินงาน (Performance Management)

- 1) กำหนดการวัดผลสำเร็จของโครงการ
- 2) ติดตามผลและความคืบหน้าของโครงการ IT ที่สำคัญต่าง ๆ
- 3) ติดตามและกำกับกระบวนการของ IT Governance

### 3.2. Technology Council

#### ความสอดคล้องของกลยุทธ์ (Strategic Alignment)

- 1) ให้แนวทางเกี่ยวกับการเปลี่ยนแปลงของเทคโนโลยี
- 2) ติดตามการเปลี่ยนแปลงของเทคโนโลยีที่เกี่ยวข้องและมีผลต่อธุรกิจ

#### การได้ผลลัพธ์ที่เพิ่มคุณค่าให้ธุรกิจ (Value Delivery)

- 1) ให้คำปรึกษาแนะนำในการเลือกเทคโนโลยีในกรอบมาตรฐานที่มีอยู่
- 2) ให้ความช่วยเหลือในการพิจารณาการเปลี่ยนแปลงต่าง ๆ

#### การจัดการทรัพยากรด้าน IT (IT Resource Management)

- 1) ให้คำแนะนำในด้านผลิตภัณฑ์ของ infrastructure
- 2) กำกับมาตรฐานทางเทคโนโลยี และข้อปฏิบัติ

#### การบริหารความเสี่ยง (Risk Management)

- 1) พิจารณาว่ามีการประเมินจุดอ่อนของเทคโนโลยีใหม่ ๆ ที่เกิดขึ้น

#### การวัดผลการดำเนินงาน (Performance Management)

- 1) ตรวจสอบการปฏิบัติที่สอดคล้องกับแนวทางและมาตรฐานของเทคโนโลยี

### 3.3. IT Architecture Review Board

#### ความสอดคล้องของกลยุทธ์ (Strategic Alignment)

- 1) เสนอแนะแนวทางด้าน IT Architecture

#### การได้ผลลัพธ์ที่เพิ่มคุณค่าให้ธุรกิจ (Value Delivery)

- 1) ให้คำปรึกษาแนะนำในการนำแนวทางด้าน IT Architecture ไปใช้

#### การจัดการทรัพยากรด้าน IT (IT Resource Management)

- 1) กำกับการออกแบบ IT Architecture

#### การบริหารความเสี่ยง (Risk Management)

- 1) กำกับเพื่อให้มั่นใจว่า IT Architecture มีความสอดคล้องกับกฎหมาย ข้อบังคับ

หลักการในการใช้ข้อมูล และการดำเนินธุรกิจอย่างต่อเนื่อง

#### การวัดผลการดำเนินงาน (Performance Management)

- 1) ตรวจสอบการปฏิบัติที่สอดคล้องกับแนวทาง Architecture

### ปัจจัยสู่ความสำเร็จ

ความสำเร็จขององค์กรจะเกิดขึ้นได้ต่อเมื่อมีกระบวนการวางแผนที่ดี มีการตัดสินใจในการใช้ทรัพยากรที่เหมาะสมและมีการกำหนดแผนงาน โครงการและงบประมาณที่ก่อให้เกิดผล โดยมีการทำงานแบบสอดคล้องประสานข้ามสายงานในแต่ละฝ่าย ซึ่งจะทำให้กิจกรรมทางด้าน IT ที่ได้กำหนดขึ้นนั้นสามารถก่อให้เกิดประสิทธิผลรวมทั้งสามารถครอบคลุมต้นทุน และวัดถึงผลตอบแทนทางธุรกิจที่เกิดขึ้นได้ อย่างไรก็ตามสิ่งเหล่านี้จะเกิดขึ้นได้ก็ขึ้นอยู่กับ กระบวนการดำเนินงานและวัฒนธรรมของการจัดการด้วย

ผลลัพธ์ที่ดีนั้นประกอบด้วย

1. การมีโครงการที่ดีขึ้นกว่าเดิม
2. การคัดเลือกโครงการที่ดี
3. มีการลดค่าใช้จ่ายในส่วนที่ไม่ก่อให้เกิดผล
4. การใช้จ่ายในปัจจุบันก่อให้เกิดผลที่ดีขึ้น
5. มีการจัดการที่ถูกต้องเหมาะสม

โดยสามารถดูได้ว่าบริษัท / องค์กรสามารถสร้างผลลัพธ์ได้ดีเพียงใด โดยพิจารณา

1. กระบวนการวางแผนทางธุรกิจและ IT มีการเชื่อมโยงและสอดคล้องประสานกัน

2. นวัตกรรมใหม่ ๆ ทางด้าน IT มีส่วนอยู่ในการวางแผนของธุรกิจ และสร้างให้เกิดกลยุทธ์ธุรกิจใหม่ ๆ รวมทั้งพัฒนาการนำกลยุทธ์ของธุรกิจในปัจจุบันไปดำเนินการให้เกิดผล
3. การลงทุนทางด้าน IT มีการจัดลำดับความสำคัญ โดยพิจารณาจากกลยุทธ์ของธุรกิจ
4. การใช้จ่ายทางด้าน IT ไม่ว่าจะเป็นการพัฒนา การปฏิบัติการ การดูแล และบำรุงรักษาและการให้บริการ มีความสอดคล้องกับกลยุทธ์ของธุรกิจ
5. มีการวัดผลการดำเนินงานของ IT ทั้งในด้านผลทางธุรกิจ และด้านเทคนิค
6. ทีมผู้บริหารทั้งด้านการจัดการ และด้าน IT มีกระบวนการดำเนินงานที่สอดคล้องกันเพื่อให้ IT สามารถเพิ่มคุณค่าและก่อให้เกิดผลตอบแทน / กำไรที่ดีขึ้น
7. กระบวนการวางแผนและการจัดการ มุ่งเน้นไปถึงการลงทุนทางด้าน IT ทั้งในด้านการบำรุงรักษา / ให้บริการของระบบในปัจจุบัน และในโครงการต่าง ๆ ด้วย
8. ผู้บริหารทั้งทางด้าน IT และในส่วนของธุรกิจ มีส่วนร่วมในการปฏิบัติตามกระบวนการต่าง ๆ ที่กล่าวมานี้อย่างเต็มที่

จุดต่าง ๆ นี้ถือได้ว่าเป็นปัจจัยสู่ความสำเร็จในการจะทำให้มีการตัดสินใจที่เหมาะสม และก่อให้เกิดผลลัพธ์ที่ดี ทั้ง 5 ประการดังที่กล่าวมาข้างต้น ซึ่งจะเป็นผลให้ต้นทุนทางด้าน IT ลดลงและยังช่วยหลักการในการจัดการ เพื่อสร้าง Value Chain ในการนำกลยุทธ์ไปสู่การเพิ่มคุณค่าให้ผลตอบแทนทาง IT

หลักการนี้ถือได้ว่าเป็นเครื่องมือสำหรับผู้บริหารทั้งในด้าน IT และในส่วนของธุรกิจ ในการพัฒนาระบบการจัดการ เพื่อนำกลยุทธ์ขององค์กร ไปกำหนดโปรแกรมและแผนงานที่ IT นำไปปฏิบัติได้ ดังนี้

#### 1. การวางแผนในการกำหนด Strategic demand / supply

ต้องกำหนดให้ชัดเจนว่าบริษัท / องค์กรต้องการจะทำอะไรหรือที่เรียกว่า Strategic intents (ความต้องการทางธุรกิจ) โดยผู้บริหารทางด้านธุรกิจและ IT จะต้องเข้าใจในภาพเดียวกันว่า องค์กรกำลังจะไปทิศทางใด และ IT สามารถช่วยเสริมในด้านใดได้บ้าง โดยความต้องการทางธุรกิจนี้จะกำหนด “ตัวขับเคลื่อนทางธุรกิจ” (business drivers) ซึ่งจะใช้เป็นตัวกำหนดกลยุทธ์ทางด้าน IT (Strategic IT requirements) เพื่อให้บรรลุถึงความต้องการทางธุรกิจนั้น ๆ

กลยุทธ์ทางด้าน IT จะเป็นแนวทางในการกำหนดความต้องการทางด้าน IT (Strategic demand for IT) โดยการวางแผนทางด้าน IT (IT Strategic planning) จะบ่งบอกถึงเทคโนโลยีใด (Strategic supply) ที่

สามารถเสริมให้กลยุทธ์ IT บรรลุได้ สิ่งที่ได้ลำดับความสำคัญก่อนหลังซึ่งเป็นแผนงาน IT และแผนการปฏิบัติงาน

## 2. นวัตกรรม

เป็นไปได้ว่า IT สามารถสร้างโอกาสทางธุรกิจ โดยทิศทางของ IT อาจช่วยก่อให้เกิดโอกาสทางธุรกิจใหม่ ๆ และถูกนำไปกำหนดเป็นกลยุทธ์ขององค์กรและแผนการดำเนินงานได้ ผลที่เกิดขึ้นคือ จะช่วยให้องค์กรสามารถสร้างความได้เปรียบในการแข่งขันได้ดียิ่งขึ้น

## 3. การจัดลำดับความสำคัญ

การประเมินโครงการ IT ที่มีการนำเสนอและมีการจัดลำดับความสำคัญ มีการกำหนดทรัพยากรที่ต้องใช้ให้กับโครงการที่สร้างคุณค่าได้สูงสุด ทำให้บริษัท / องค์กร สามารถบริหารจัดการว่าจะใช้เงินไปกับโครงการใดที่ก่อให้เกิดผลที่ดีที่สุดกับกลยุทธ์ขององค์กร และจัดลำดับของโครงการตามผลที่ประเมิน ซึ่งจะช่วยให้มีการใช้เงินอย่างถูกต้องคุ้มค่า โดยผู้บริหารทั้งด้านธุรกิจและ IT ได้มีการตัดสินใจร่วมกัน

## 4. ความสอดคล้อง

ประเมินผลที่ได้รับจากกิจกรรมที่มีอยู่ในปัจจุบันว่ากิจกรรมใด ควรได้รับการจัดสรรทรัพยากรให้แทนที่จะคิดว่ากิจกรรม IT ทุกอย่างที่ทำอยู่จะต้องได้รับการสนับสนุน โดยพิจารณาว่ากิจกรรมใดที่ไม่ก่อให้เกิดผลหรือไม่สอดคล้องกับกลยุทธ์ของธุรกิจ ก็ควรขจัดออกไปเพื่อที่จะได้จัดสรรทรัพยากรไปให้กับ กิจกรรม IT ใหม่ ๆ ที่ช่วยพัฒนาให้องค์กรสามารถบรรลุกลยุทธ์ทางธุรกิจได้ และถือได้ว่าเป็นการจัดการการใช้เงินที่มีเหตุผล เนื่องจากรับการพัฒนาใหม่ ๆ ที่เกิดขึ้นด้วย

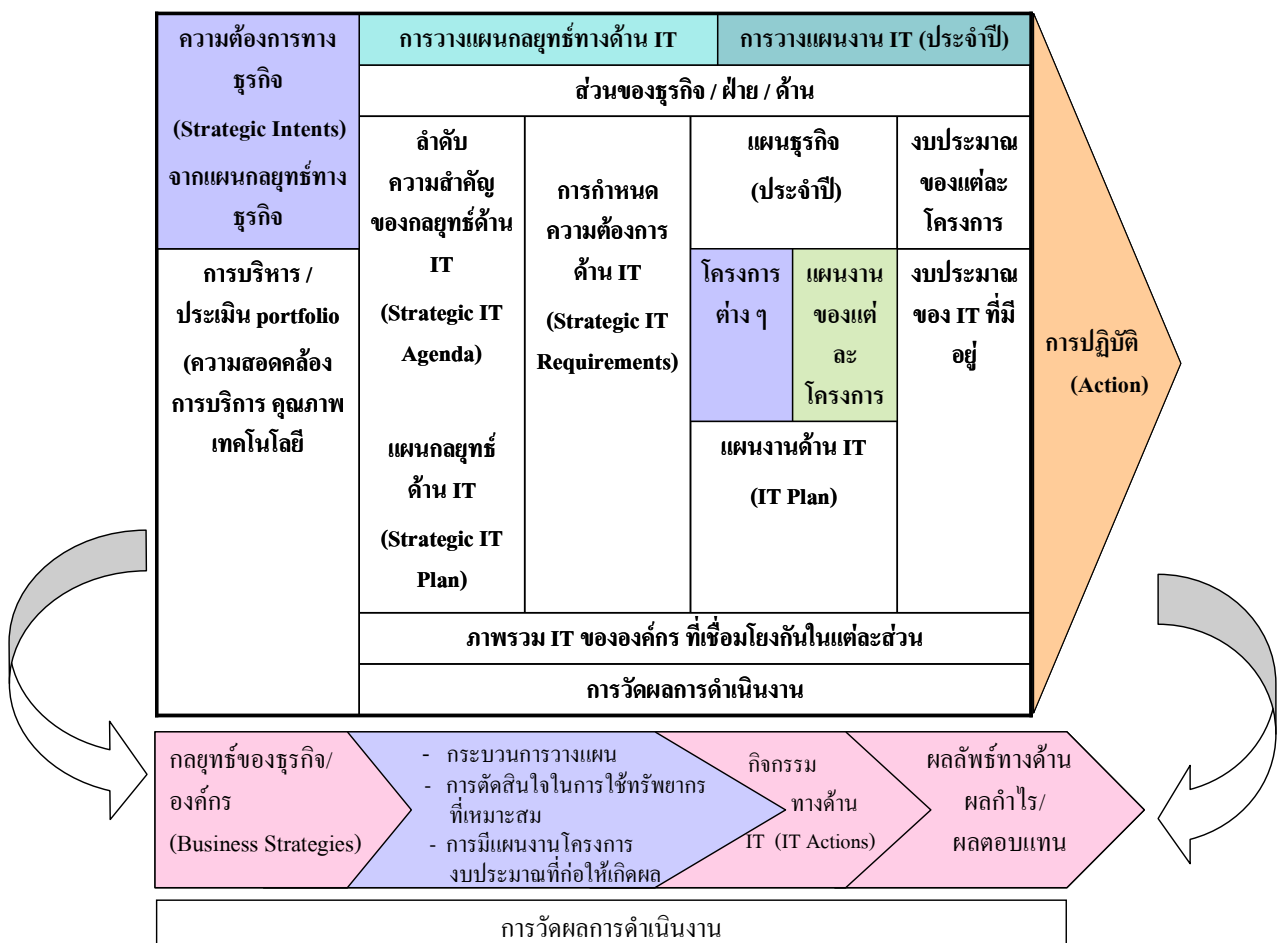
## 5. การวัดผลการดำเนินงาน

การวัดผลการดำเนินงานทางด้าน IT ที่สอดคล้องกับองค์กร การวัดผลการดำเนินงานในด้านเทคนิคและการปฏิบัติงานนั้นทำได้ไม่ยาก แต่การวัดผลที่ IT สร้างคุณค่าให้กับองค์กรนั้น กระทำได้ค่อนข้างยากที่ดีที่สุดคือ การวัดผลที่ผสมผสานทั้ง 2 ส่วนเข้าด้วยกัน ดังนั้นจึงจะต้องมีการกำหนดว่าจะวัดอะไร เข้าใจได้อย่างไร ซึ่งผลที่ต้องการคือ มีการปรับปรุงผลการดำเนินงาน เพราะมีการวัดผล และการปรับปรุงการสื่อสารที่มีต่อผู้บริหารในส่วนหนึ่งของธุรกิจให้ดียิ่งขึ้น เพื่อให้เข้าใจและปฏิบัติสอดคล้องกันทั้งในส่วนงานของ IT และส่วนงานบริหารธุรกิจ

โดยหลักการจัดการทั้ง 5 ส่วนนี้มุ่งเน้นถึงวิธีการจัดการ การประเมินคุณค่าของ IT (IT Impact) การบริหาร Portfolio และการบริหารจัดการทางด้านวัฒนธรรมขององค์กร โดยการประเมินคุณค่าของ IT จะช่วยให้ทราบว่าอะไรที่มีความสำคัญขององค์กร การบริหาร Portfolio ช่วยให้ผู้บริหารตัดสินใจในการลงทุนและจัดลำดับความสำคัญได้ รู้ว่าจะใช้จ่ายไปกับ IT เท่าไร อย่างไร และในด้านวัฒนธรรมขององค์กรเองจะช่วยให้ผู้บริหารสามารถก้าวข้ามสิ่งกีดขวางต่าง ๆ ที่ทำให้กระบวนการทำงานสามารถเชื่อมโยงและสอดคล้องประสานกันได้ดียิ่งขึ้น

หลักการทั้ง 5 จะช่วยให้องค์กรเชื่อมโยงการลงทุนทางด้าน IT เข้ากับกลยุทธ์ขององค์กรได้ แต่ยังคงจำเป็นต้องอาศัยกระบวนการทำงานที่เชื่อมโยงกัน เพื่อให้เกิดการปฏิบัติที่ถูกต้องเหมาะสม อันจะส่งผลให้เกิดผลลัพธ์ที่ถูกต้องด้วยเช่นกัน ดังแสดงในแผนภาพดังต่อไปนี้

### การเชื่อมโยง Value Chain ของกลยุทธ์สู่การปฏิบัติ



ความสำเร็จสุดท้ายอยู่ที่การนำไปปฏิบัติ (Action) ที่เหมาะสมถูกต้อง หมายถึง IT จะต้องรู้ว่าสิ่งที่ปฏิบัติอยู่นั้นสอดคล้องกับกลยุทธ์ของธุรกิจหรือไม่ ถ้าไม่สอดคล้องก็ไม่ควรปฏิบัติ เพื่อให้การควบคุมต้นทุนเกิดประสิทธิผลและช่วยให้ IT สามารถสร้างคุณค่าเพิ่มและให้ผลตอบแทนที่สูงขึ้นแก่ธุรกิจได้

### การจัดการทางด้าน IT Portfolio และ IT Investment

การจัดทำ IT Portfolio จะช่วยให้ IT Steering Committee สามารถทราบถึงสถานะของ IT Investment และสามารถติดตามการใช้ประโยชน์ และวัดผลถึงประสิทธิภาพและประสิทธิผล เพื่อพิจารณาถึงผลตอบแทนที่ได้รับ ทั้งในรูปตัวเงินและไม่ใช่ตัวเงิน และการบรรลุถึงความต้องการและเป้าหมายทางธุรกิจได้ โดยจะช่วยให้การจัดลำดับความสำคัญของ IT Investment แต่ละส่วนทำได้อย่างชัดเจน และช่วยในการจัดสรรทรัพยากรให้กับ IT Investment ที่มีความสำคัญ ในขณะที่ IT ในบางส่วนที่หมดความสำคัญหรือล้าสมัยแล้วจะสามารถวางแผนในการเปลี่ยน/ทดแทนด้วยรุ่นใหม่ที่สามารถสร้างประสิทธิผลและประสิทธิภาพได้ดีกว่า เนื่องจากต้นทุนทางด้าน IT ทั้ง Hardware และ Software มีแนวโน้มที่มีราคาถูกลง

IT Portfolio คือ กลุ่มของการลงทุนทางด้าน IT (IT Investment) และทรัพยากรที่ใช้ รวมทั้งข้อมูลที่เกี่ยวข้องกับการลงทุนในแต่ละส่วน โดยประกอบด้วยแต่ละรายการที่แบ่งอยู่ในกลุ่มของ

1. **Application** ประกอบด้วยกลุ่มของ User Applications ที่มีการใช้งานและบำรุงรักษาที่เป็นความรับผิดชอบของ IT ต้นทุนที่เกี่ยวข้องและบันทึกใน Portfolio จะรวมถึงผู้บริหารและพนักงานที่เกี่ยวข้องกับ Application นั้น ๆ
2. **Infrastructure** ประกอบด้วย Hardware และ Software ที่ให้บริการกับ User ซึ่งจะรวมถึง Processors, Peripherals, Communications, Operating Software และสถานที่/ อุปกรณ์อำนวยความสะดวกต่าง ๆ ต้นทุนที่เกี่ยวข้องและบันทึกใน Portfolio จะรวมถึงผู้บริหารและพนักงานที่เกี่ยวข้องกับ Infrastructure ทั้งหมด
3. **Service** ประกอบด้วยการให้บริการ และสนับสนุนการใช้งานของ User เช่น Help Desk และบริการซ่อม PC โดยจะไม่รวมการบริการที่ให้แก่ภายในหน่วยงานด้าน IT แต่จะเป็นบริการที่มีการเรียกใช้ตามตารางการบริการที่มีให้แก่ User หรือตามที่ User ร้องขอ ต้นทุนที่เกี่ยวข้องและบันทึกใน Portfolio จะรวมถึงผู้บริหารและพนักงานที่เกี่ยวข้องกับการให้บริการแก่ User ทั้งหมด
4. **Management** ประกอบด้วยกิจกรรมที่เกี่ยวข้องกับการบริหาร และการให้บริการที่สนับสนุนการทำในของหน่วยงานทางด้าน IT ที่เกี่ยวข้องกับ Application, Infrastructure และ Service กับ User

## ตัวอย่างรูปแบบเบื้องต้นของ IT Portfolio

	Alignment	Service Level	Quality	Current Budget(฿M)	Future Budget(฿M)
Applications					
Payroll					
Financial Analysis					
Sales Information					
Infrastructure					
E-mail					
Network facilities					
Data Warehouse					
Management tools, information					
Service					
Data administration					
Help Desk					
Network Monitoring					
Training					
Management					
Enterprise Architecture					
Budgeting					
Planning					
Procurement					
Employee Development					

การจัดการทางด้าน IT Portfolio ถือได้ว่าเป็นเครื่องมือที่สำคัญที่จะช่วยผู้บริหารในการทำความเข้าใจถึงการลงทุนทางด้าน IT ในมุมมองของต้นทุน และทรัพยากรต่าง ๆ ที่เกี่ยวข้อง เพื่อช่วยในการวางแผน และเป็นเครื่องมือที่ช่วยในการตัดสินใจ

แนวความคิดในด้าน IT Management ในการจัดการทรัพยากรต่าง ๆ ทางด้าน IT ในรูปแบบของ Portfolio ได้เกิดมาประมาณ 30 ปีที่ผ่านมาตั้งแต่ปี 1970 โดย Warren McFarlan และอื่น ๆ โดยเริ่มต้นจากการพัฒนาของ Application Development Portfolio ล่าสุดทางรัฐบาลกลางของสหรัฐฯ ได้ใช้ Portfolio Management นี้ให้เป็นเครื่องมือสำหรับผู้บริหารในการจัดลำดับความสำคัญ และใช้ในการจัดการ Application Development Project ต่าง ๆ

การที่นำทรัพยากรต่าง ๆ ทางด้าน IT มาอยู่ในรูปของ Portfolio จะช่วยให้ผู้บริหารสามารถ

1. จัดลำดับการลงทุนทางด้าน IT โครงการใหม่ ๆ
2. เข้าใจถึงการจัดสรรทรัพยากรที่จะมีให้กับโครงการ IT ใหม่ ๆ และค่าใช้จ่ายที่ใช้ในการจัดการกับ IT ที่ต้องใช้อยู่ในปัจจุบัน (On-Going)
3. กำหนดเป้าหมายของการใช้จ่ายในการจัดการกับ IT ที่ต้องใช้อยู่ในปัจจุบัน ทั้งในด้านของระดับการบริการและคุณภาพที่ต้องการ และทางด้านต้นทุนที่เกิดขึ้นรวมทั้งความสามารถในการลดต้นทุนด้วย
4. ประเมินถึงความสามารถในการใช้งานของแต่ละรายการใน IT Portfolio
5. จัดรายการใน IT Portfolio ที่ให้ประสิทธิผลต่ำ ได้ผลงานคุณภาพต่ำ หรือมีต้นทุนที่สูงเกินไปออกไป
6. ตัดสินใจ และกำหนดกลยุทธ์ในการปรับเปลี่ยน/ ทดแทนรายการใน IT Portfolio ที่เป็น IT ที่ต้องใช้อยู่ในปัจจุบัน (On-Going)
7. การใช้ Portfolio นี้จะช่วยให้ผู้บริหารสามารถตัดสินใจในแต่ละรายการโดยใช้แนวทางเดียวกัน แทนที่จะตัดสินใจแบบที่เป็นแต่ละกรณีไป ซึ่งจะมีประโยชน์ต่อผู้บริหารในการพิจารณาว่า
  - 1) การจัดสรรทรัพยากรทางด้าน IT อยู่ในสัดส่วนที่เหมาะสมหรือไม่
  - 2) ควรจะมีการทดแทน หรือจัด รายการในแต่ละกลุ่ม ของ application, service หรือ infrastructure หรือไม่
  - 3) กลุ่มของ IT investment ที่มีอยู่สอดคล้องกับความต้องการของธุรกิจในปัจจุบันหรือไม่
  - 4) กลุ่มของ IT investment ที่มีอยู่สามารถรองรับความต้องการ และกลยุทธ์ของธุรกิจในอนาคตได้หรือไม่

- 5) กลุ่มของ IT investment ที่มีอยู่นั้นมีความสมดุลในด้านระดับการให้บริการ (service) และคุณภาพ (quality) หรือไม่
- 6) มีทรัพยากรทางด้าน IT ในส่วนใดที่ไม่มีประสิทธิภาพเพียงพอ

ขอบเขตของ IT Portfolio รวมถึงการพิจารณา IT Asset ที่มีอยู่ในปัจจุบัน รวมทั้งโครงการที่กำลังจะทำ หรือที่ทำอยู่ (IT Projects) และการพัฒนาเทคโนโลยีใหม่ๆ (IT Development)

IT Asset Portfolio	IT Project Portfolio	IT Development Portfolio
<ul style="list-style-type: none"> <li>• เน้นพิจารณาระบบ IT และ solutions ที่ใช้อยู่ในปัจจุบันว่าควรจะมีการเปลี่ยน หรือปรับการใช้งาน หรือจะคงไว้เดิม หรือนำมาพัฒนาใหม่</li> <li>• ประกอบด้วย               <ul style="list-style-type: none"> <li>• Infrastructure &amp; Applications</li> <li>• Human capital</li> <li>• Information &amp; Data</li> <li>• Process</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• การขยาย เปลี่ยน หรือ แก้ไข IT Solutions</li> <li>• เน้นที่เป็นรูปแบบโครงการต่างๆ ที่มีศักยภาพ และมีการสนับสนุนด้านการเงิน</li> </ul>	<ul style="list-style-type: none"> <li>• การมองถึงการลงทุนของเทคโนโลยีในอนาคต เนื่องจากการเปลี่ยนแปลงของเทคโนโลยีใหม่ๆ มีการขยายแนวธุรกิจ หรือเข้าสู่ธุรกิจใหม่ หรือการรวม/เข้าซื้อธุรกิจต่างๆ โดยเน้นนวัตกรรมและการพัฒนาเทคโนโลยีใหม่ๆ</li> <li>• เป็นลักษณะของแนวคิด ความคิดใหม่ๆ หรือโอกาสที่สังเกตเห็น</li> </ul>

รูปแบบของ IT Portfolio สามารถจะมีได้หลากหลายขึ้นกับ ตัวชี้วัดที่แต่ละองค์กรใช้ และต้องการจะประเมิน ตัวอย่างของรูปแบบ IT Portfolio ตามแนวทาง IT Management ดังแสดงในตาราง จะเน้นองค์ประกอบของ IT ที่มีใช้อยู่ในปัจจุบัน (On-Going) และเกี่ยวข้องกับการจัดการทางด้านเทคโนโลยีที่มีอยู่ ส่วนในโครงการ IT ใหม่ควรจะต้องพิจารณาในมุมมองของการตัดสินใจในเชิงธุรกิจ ที่เกี่ยวข้องกับการตัดสินใจในรูปแบบของความสอดคล้องกับกลยุทธ์ขององค์กรและผลตอบแทน ดังรูปแบบในตาราง

## ตัวอย่างรูปแบบ IT Portfolio ของการลงทุนในโครงการใหม่ตามมุมมองเชิงธุรกิจ

	Strategic Alignment	Technical Assessment	ROI	Risk & Uncertainty	Resources Consumed (฿M)
Strategic					
CRM					
e-Procurement					
Factory					
Financial Analysis					
Data Warehouse					
Training					
Future Strategic					
Content applications					
e-Commerce					
e-Logistics					
Mandatory					
e-DOC					
IT Security Room					
Business Continuity Management					
Employee Development					

แหล่งข้อมูล: *IT Changes the Way You Compete*, Harvard Business Review, Warren McFarlan, 1984

โดยมุมมองนี้ใช้พิจารณา ดังนี้

1. **Strategic** - การลงทุนที่ช่วยเพิ่มศักยภาพในการแข่งขัน ช่วยเพิ่มรายได้ หรือป้องกันการเข้าสู่ตลาดของคู่แข่ง เกณฑ์ที่ใช้วัดคุณค่าที่ได้รับนั้นจะพิจารณาถึง รายได้ ส่วนแบ่งการตลาด นวัตกรรม ความยืดหยุ่นและคล่องตัว ขององค์กรที่ได้รับจากกลุ่ม IT นี้
2. **Factory** - การลงทุนเพื่อให้บริษัทสามารถดำเนินงานได้อย่างต่อเนื่อง เช่น การลงทุนใน Back Office เกณฑ์ที่ใช้วัดคุณค่าที่ได้รับนั้นจะพิจารณาถึง การลดต้นทุน การเพิ่มขึ้นของจำนวน Through put ลดระยะเวลาของงาน/กระบวนการ เพิ่มผลิตผลต่อราย อันเนื่องมาจากการใช้งานของ IT ในกลุ่มนี้
3. **Future Strategic** - การลงทุนที่มีผลต่อการเพิ่มศักยภาพในอนาคต เป็นการลงทุนในธุรกิจใหม่หรือผลิตภัณฑ์/บริการใหม่ เกณฑ์ที่ใช้วัดคุณค่าที่ได้รับจะเหมือนกับกลุ่ม Strategic
4. **Mandated** - การลงทุนที่เป็นไปตามข้อบังคับ หรือมติของคณะกรรมการ เกณฑ์ที่ใช้วัดคุณค่าที่ได้รับในบางกรณีจะเหมือนกับกลุ่ม Factory

ข้อมูลที่ใช้ในการพิจารณาใน IT Portfolio ในการกำหนดระดับการให้คะแนนส่วนใหญ่จะประกอบด้วย

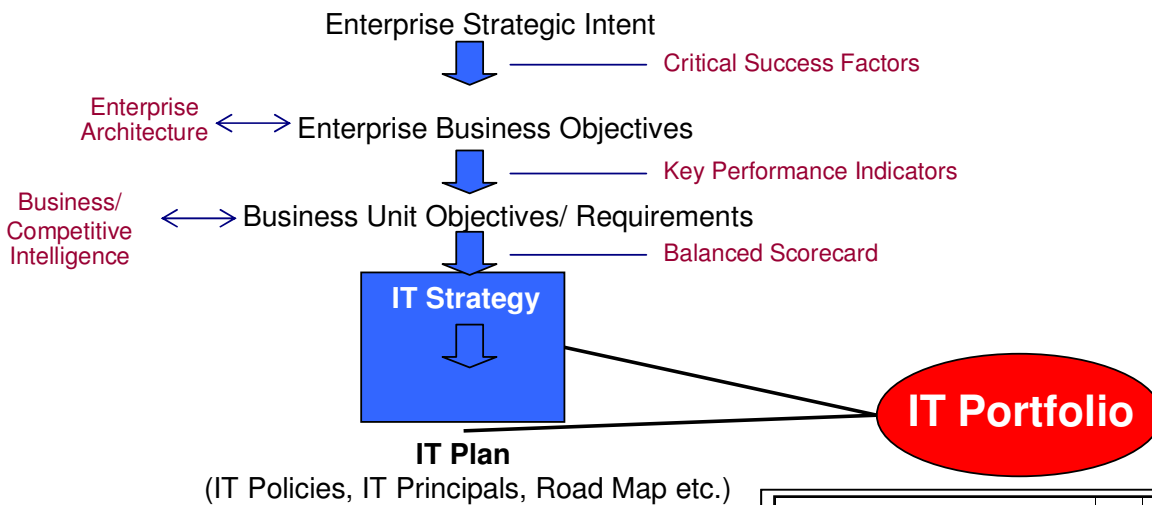
- Service and Quality
  - Functionality
  - Accuracy
  - Availability
  - Responsiveness
- Risk & Uncertainty ที่มีเกี่ยวข้องกับ
  - การดำเนินธุรกิจ
  - Technology
  - องค์กร/ วัฒนธรรมองค์กรโดยรวม
- Value คุณค่าที่เกิดขึ้น โดยพิจารณาจาก
  - ด้านเทคนิค (technical assessment)
  - ด้านความสอดคล้องกับกลยุทธ์ (strategic alignment)
  - ด้านผลตอบแทนจากการลงทุน (ROI)

การกำหนดระดับของคะแนนของ แต่ละปัจจัยจึงขึ้นอยู่กับ การให้น้ำหนักความสำคัญของปัจจัยที่เกี่ยวข้อง และอาจมีการกำหนดเป็นช่วงของข้อมูล เพื่อทำการให้น้ำหนัก เช่น ROI

% ROI-ตัวอย่าง	Score	Value (%)
% ผลตอบแทนจากการลงทุนที่คำนวณโดยฝ่ายการเงิน	0	<0%
	20	1-4%
	40	5-10%
	60	11-15%
	80	16-20%
	100	>20%

เป็นคะแนนที่อยู่ใน Portfolio

1. ความสัมพันธ์ของ IT Portfolio ที่สนับสนุนความสอดคล้องกับกลยุทธ์ทางด้าน IT



	Alignment	Service Level	Quality	Current Budget(€M)	Future Budget(€M)
<b>Applications</b>					
Payroll	25	1.6	2.1	30	
Financial Analysis	42	1.9	2.3	40	
Sales Information	37	1.2	2.5	30	
<b>Infrastructure</b>					
E-mail	36	2.8	2.3	30	
Network facilities	61	2.9	1.8	250	
Data Warehouse	45	0.2	0.3	70	
Management tools, information	34	1.3	1.5	10	
<b>Service</b>					
Data administration	46	2.0	1.8	30	
Help Desk	33	1.5	0.5	10	
Network Monitoring	27	2.8	2.4	10	
Training	16	1.3	0.9	9	
<b>Management</b>					
Enterprise Architecture	14	1.3	0.9	300	
Budgeting	25	2.4	1.0	19	
Planning	46	2.3	1.0	20	
Procurement	32	2.0	1.3	30	
Employee Development	12	0.2	0.2	25	

หัวใจหลักของการทำ IT Portfolio ก็เพื่อให้การลงทุนทางด้านการลงทุนทางธุรกิจขององค์กร สามารถวัดผลได้ถึงความคุ้มค่าที่อยู่ในรูปของผลตอบแทน และผลสำเร็จจากการ

ประเมินของตัวชี้วัดตามหลักการของ Balanced Scorecard โดย IT Portfolio จะช่วยเป็นเครื่องมือในการวางแผนทางด้าน IT และใช้ในการจัดสรรทรัพยากรที่ระบุในแผนงาน โดยแบ่งเป็น

1. IT Asset Portfolio ส่วนของ IT ที่ใช้อยู่ในปัจจุบัน ทั้ง Application, Infrastructure, Service และ Management

2. IT Project Portfolio และ/หรือ IT Development Portfolio ส่วนของโครงการที่มีการเปลี่ยนแปลง/ทดแทน หรือเป็น โครงการที่มีการพัฒนา IT ใหม่ ที่จำเป็นต้องมีการจัดทำ Business Case และนำมาจัดลำดับความสำคัญเพื่อจัดสรรทรัพยากรที่เหมาะสม และสอดคล้องกับกลยุทธ์

2. ความสัมพันธ์ของ IT Portfolio ที่เกี่ยวข้องกับการจัดลำดับความสำคัญของการลงทุน/โครงการ

Projects-example	Value	Resources Consumed(\$M)
Business Continuity Management	48	6
e-DOC	39	10
e-Logistics	38	10
Financial Analysis	35	10
Content applications	27	30
IT Security Room	25	19
CRM	24	30
e-Procurement	21	37
e-Training	19	9
Employee Development	15	2
Data Warehouse	14	10
e-Commerce	12	10

แต่ละส่วนคือ IT Investment ที่มี Profile ในรูปของ Business Case

IT Portfolio ช่วยให้องค์กรสามารถจัดลำดับความสำคัญของการลงทุนทางด้าน IT โดยพิจารณาหลักเกณฑ์และให้น้ำหนักของการลงทุนกับคุณค่าที่ได้รับ ที่สอดคล้องกับความต้องการทางธุรกิจและเพื่อจัดลำดับการลงทุนและการใช้ทรัพยากรที่เหมาะสม ตามงบประมาณ เวลา ทรัพยากรและศักยภาพที่มีอยู่

ปัจจัยที่จำเป็นต้องพิจารณา คือ มูลค่าของโครงการ ความเสี่ยง (Risk & Uncertainty) และผลตอบแทน/คุณค่าที่ได้รับ (Value) ในการจัดลำดับความสำคัญ การทำ Business Case ของแต่ละรายการ โดยเฉพาะรายการที่มีมูลค่าสูง และมีความเสี่ยงสูงจะช่วยให้การพิจารณามีความรอบคอบยิ่งขึ้น และมีความโปร่งใส สามารถกลับไปตรวจสอบ และย้อนพิจารณาใหม่ได้

### 3. ความสัมพันธ์ของ IT Portfolio ที่เกี่ยวข้องกับ IT Infrastructure Plan

IT Portfolio จะช่วยให้เกิด Alignment ระหว่างกลยุทธ์ที่ต้องการ (Strategic Intent) ให้เข้ากับความจำเป็นในการดำเนินงาน (Operational Requirements) หรือกระบวนการทำงานที่สอดคล้องกัน โดยสามารถใช้เป็นแนวทางในการกำหนดความต้องการทางด้าน IT ในส่วนของ Application, Infrastructure, Service และ Management ที่อยู่ในรูปของ IT Infrastructure Plan ที่ชัดเจนและสามารถสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบได้

IT Infrastructure Plan จะใช้ในการกำหนดรูปแบบ IT ในการจัดซื้อ/ จัดหา และพัฒนา ที่ครอบคลุมภาพรวมของ IT ทั้งหมดขององค์กร เปรียบเสมือนเป็นรากฐาน และแนวทาง (Blueprint) ในการใช้งานและพัฒนาทางด้าน IT ที่มีความสอดคล้องกับโครงสร้างพื้นฐานทางด้าน IT โดยรวม โดยจะต้องมีการพิจารณาและศึกษาถึงแนวโน้มการเปลี่ยนแปลงของเทคโนโลยีและนำมาพิจารณาเปลี่ยนแปลงใน IT Infrastructure Plan ที่มีอยู่แล้วด้วย ตัวอย่าง IT Infrastructure Plan สามารถดูได้จาก [www.its.state.ms.us](http://www.its.state.ms.us) ของ Department of Information Technology, Mississippi State, USA

### 4. ความสัมพันธ์ของ IT Portfolio ที่เกี่ยวข้องกับ IT Performance Measurement

IT Portfolio จะช่วยประสานตัวชี้วัดที่ใช้ประเมินผลเพื่อพิจารณาถึงคุณค่าที่ได้รับและความสอดคล้องของการลงทุนในด้านของกลยุทธ์ขององค์กร ความเหมาะสมทางด้านเทคนิค และผลตอบแทนที่ได้รับ เปรียบเทียบกับระดับบริการและคุณภาพที่ได้จากการลงทุนใน IT โดยตัวชี้วัดที่พิจารณาส่วนใหญ่จะเกี่ยวข้องกับข้อมูลทางด้าน Service/ Quality และ Value คุณค่าที่เกิดขึ้น ทั้งในด้านความสอดคล้องกับกลยุทธ์ (Strategic Alignment) ด้านผลตอบแทนจากการลงทุน (ROI) และด้านเทคนิค (Technical Assessment)

นอกเหนือจาก การบริหาร IT portfolio/ IT Investment แล้ว ยังจำเป็นที่จะต้องจัดมาตรฐาน IT Process ที่เกี่ยวข้องเพื่อช่วยในการจัดการ IT Portfolio ที่ครอบคลุมกระบวนการทางด้าน IT และที่เกี่ยวข้องกับ IT ได้ครบถ้วน

อย่างไรก็ตามโครงการต่างๆ ของหน่วยงาน ที่มี ยังไม่ได้มีการวิเคราะห์ IT Portfolio เพื่อจัดลำดับความสำคัญ ซึ่งถือได้ว่ามีความสำคัญในการจัดการทรัพยากรที่คุ้มค่าและสอดคล้องกับความต้องการทางธุรกิจ เนื่องจากเทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็ว การใช้ทรัพยากรไปในโครงการที่มีความสำคัญ จึงต้องมีการศึกษาความเป็นไปได้อย่างระมัดระวังโดยใช้การบริหารความเสี่ยงเข้ามาจัดการ และมีการจัดทำ Business Case ที่สามารถประเมินเบื้องต้นถึงผลที่ได้จากการทำโครงการทั้งในรูปของตัวเงิน และประโยชน์ในด้านอื่นเทียบกับการลงทุน

คุณภาพของการจัดการโครงการถือเป็นประเด็นที่มีความสำคัญกับองค์กร ที่จะต้องให้ความสนใจ เพื่อให้ปัญหาหลังการดำเนินการเมื่อมีการติดตั้งเทคโนโลยีต่าง ๆ มีน้อยที่สุด และมีระดับความเสี่ยงที่ต่ำสุด

### กำหนดบุคลากรและการแต่งตั้งคณะกรรมการที่เหมาะสม

ความสำเร็จของ IT Governance จะขึ้นอยู่กับความเกี่ยวข้องโดยตรงของผู้บริหาร โดยผู้ดำเนินการหลักนั้นควรจะเป็นบุคคลที่ทำให้ IT Governance ประสบความสำเร็จได้ และไม่ควรมีการเปลี่ยนแปลงตัวบุคคลบ่อยเพราะจะขาดความต่อเนื่อง ซึ่ง โดยคณะกรรมการใน IT Strategy Committee ควรจะมีอย่างน้อย 2 ท่าน เพื่อความต่อเนื่องเมื่อมีผู้ใดขาดไป และสามารถมีผู้เชี่ยวชาญอยู่ในคณะได้เพื่อความเข้าใจทางด้านข้อมูลในเชิงลึก ส่วนที่เป็น IT Steering Committee จะประกอบด้วยผู้บริหารระดับสูงที่เกี่ยวข้อง รวมทั้ง CIO และที่ปรึกษาที่เป็นผู้เชี่ยวชาญ ที่จะต้องตัดสินใจใน IT Investment ขนาดใหญ่ โดยประสานงานร่วมกับ Program Management Office (PMO) ที่รับผิดชอบดูแลทางด้าน Project Management และ Project Portfolio Management ในขณะที่ IT Investment ที่มีขนาดเล็กอาจแต่งตั้งคณะกรรมการ (Subcommittee) เพื่อพิจารณาแทนได้

การกำหนดคณะทำงานเฉพาะเรื่อง เช่น IT Portfolio Management Committee หรือ IT Infrastructure Planning Committee ก็สามารถรวมทีมจากผู้ที่มีคุณสมบัติที่เหมาะสมเพื่อกำหนดขั้นตอนมาตรฐาน และกรอบการทำงาน โดยจะต้องมีผู้ที่มีความรู้ความเข้าใจในด้านนั้นเป็นหลัก ควรมีการกำหนดบทบาทหน้าที่ความรับผิดชอบของคณะทำงานในแต่ละ Committee ที่ชัดเจน รวมทั้งขอบเขตของอำนาจ และแนวทางในการตัดสินใจ

### บทบาทหน้าที่ของคณะกรรมการและผู้บริหารขององค์กรเกี่ยวกับ IT Governance

1. นำกรอบงานธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT Governance) มาใช้ในองค์กร
2. กำหนดกลยุทธ์ด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับเป้าหมายการทำธุรกิจ
3. การเชื่อมโยงกลยุทธ์ และเป้าหมายลงไปในแต่ละระดับขององค์กร
4. กำหนดโครงสร้างองค์กรที่ช่วยสนับสนุนการดำเนินงานตามกลยุทธ์ที่วางไว้
5. นำกรอบงานด้านการควบคุมเทคโนโลยีสารสนเทศ และด้าน IT Governance มาใช้
6. จัดให้มีโครงสร้างพื้นฐานด้านเทคโนโลยีที่ช่วยสนับสนุนการสร้างสารสนเทศทางธุรกิจ และการใช้

สารสนเทศดังกล่าวร่วมกัน

7. การผนวกรวมความรับผิดชอบต่อด้านการบริหารความเสี่ยงไว้ในองค์กร
8. มุ่งเน้นกระบวนการเทคโนโลยีสารสนเทศที่สำคัญ และความสามารถหลักของเทคโนโลยีสารสนเทศ (Core IT competencies)
9. วัดผลการดำเนินงาน (Balanced Business Scorecard)

### การสร้างคุณค่าเพิ่มทางด้านเทคโนโลยีสารสนเทศและการจัดการ

การควบคุมต้นทุนทางด้านเทคโนโลยีสารสนเทศ และสามารถสร้างคุณค่าเพิ่มและผลกำไรให้เพิ่มขึ้นได้ ดังนั้นจำเป็นต้องมีความเข้าใจในกระบวนการบริหารงาน ในลักษณะสอดประสานและบูรณาการทั่วทั้งองค์กร ความเข้าใจดังกล่าวสามารถสร้างความแตกต่าง และยกระดับการแข่งขัน รวมทั้งการสร้างความพึงพอใจให้แก่ลูกค้า

1. การควบคุมต้นทุนทางด้านเทคโนโลยีสารสนเทศ และสามารถสร้างคุณค่าเพิ่มและผลกำไรให้เพิ่มขึ้นได้นั้นจำเป็นต้องมี
  - 1.1. กระบวนการวางแผนที่ดี
  - 1.2. การตัดสินใจในการใช้ทรัพยากรที่เหมาะสม
  - 1.3. การมีแผนงานและงบประมาณที่ก่อให้เกิดผล

ที่ผ่านมาจะพบว่าบริษัท / องค์กร ส่วนใหญ่มักจะพบกับปัญหาในด้าน การวางแผน การจัดสรร และจัดความสำคัญของทรัพยากรกับงาน การทำงานประมาณ การวัดผลการดำเนินงาน และอื่นๆ ที่มีการจัดการแบบต่างคนต่างทำเป็นส่วน ๆ และขาดการสอดประสานกันระหว่างหน่วยงานที่เกี่ยวข้อง ขาดการเชื่อมโยงซึ่งกันและกัน ตัวอย่างที่เห็นได้ คือ บริษัท / องค์กร อาจมีกลยุทธ์ในการดำเนินธุรกิจแต่การวัดผลการดำเนินงานนั้นไม่สอดคล้องกับกลยุทธ์ที่มีอยู่ การวางแผนธุรกิจ และเทคโนโลยีสารสนเทศไม่สอดคล้องกัน หรือกระบวนการดำเนินงานที่มีอยู่ไม่ได้ใช้ข้อมูลอยู่บนฐานเดียวกันและไม่เชื่อมโยงกัน

อีกประการหนึ่งคือ บริษัทส่วนใหญ่จะมีการแบ่งงานชนิดที่ต่างคนต่างทำตามสายงานเป็นหลัก จึงมักขาดการสอดประสาน และขาดการมองภาพรวมขององค์กร รวมทั้งขาดการเชื่อมโยงเพื่อข้ามกำแพงที่ขวางแผนก / ส่วน / ฝ่าย ทำให้ธุรกิจไม่เชื่อมโยงกัน แต่ในบทบาทของเทคโนโลยีสารสนเทศนั้น นอกเหนือจากการมีความควบคุมต้นทุนทางด้านเทคโนโลยีสารสนเทศและการสร้างผลตอบแทนที่ดีแล้ว เทคโนโลยีสารสนเทศยังจะต้องช่วยในการเชื่อมต่อ / เชื่อมโยงการดำเนินงานขององค์กรด้วย

โครงสร้างพื้นฐานของเทคโนโลยีสารสนเทศ (IT Infrastructure) จะต้องสร้างมาเพื่อเชื่อมโยงระบบข้อมูล เพื่อให้การทำงานของแต่ละฝ่าย เชื่อมโยงและสอดประสานกันข้ามพรมแดนของแต่ละฝ่าย และในมุมมองเดียวกัน การวางแผนงาน การจัดลำดับความสำคัญของงาน การจัดสรรงบประมาณ ฯลฯ ก็จำเป็นต้องเชื่อมโยงแต่ละฝ่ายเพื่อให้เกิดประสิทธิผลด้วย

การบริหารงบประมาณ และการจัดการในโครงการต่าง ๆ จะให้ผลลัพธ์ที่ดีได้ต่อเมื่อผู้บริหาร และบุคลากรในองค์กรปฏิบัติได้อย่างมีประสิทธิภาพ โดยไม่ใช่ต่างคนต่างทำ หรือขาดการเชื่อมโยงกัน

2. ข้อสังเกตอาจพบได้เมื่อองค์กรขาดการเชื่อมต่อกันในการปฏิบัติงานในด้านเทคโนโลยีสารสนเทศที่ใช้เป็นแนวทางการศึกษาได้บางประการ คือ
  - 2.1. แผนธุรกิจไม่ได้เป็นตัวกำหนดแผนเทคโนโลยีสารสนเทศ
  - 2.2. แผนเทคโนโลยีสารสนเทศมุ่งเน้นด้านเทคโนโลยีมากกว่า การสนองตอบ / สนับสนุนกลยุทธ์ขององค์กร
  - 2.3. ผู้บริหารไม่ได้เล็งเห็นว่าเทคโนโลยีสารสนเทศจะช่วยสนับสนุนกลยุทธ์ขององค์กรได้

2.4. โครงการทางด้านเทคโนโลยีสารสนเทศไม่ได้สนับสนุนกลยุทธ์ขององค์กร การใช้จ่ายทางด้านเทคโนโลยีสารสนเทศ ในด้านการดูแลบำรุงรักษา IT Infrastructure และ Application ไม่ได้สนับสนุนกลยุทธ์ขององค์กร

2.5. งบประมาณของบริษัท / องค์กร ไม่ได้นำส่วนของการวางแผนทางด้านเทคโนโลยีสารสนเทศมาเกี่ยวข้องด้วย

2.6. แผนงานทางด้านเทคโนโลยีสารสนเทศไม่ได้ช่วยให้ผู้บริหารสามารถใช้ในการตัดสินใจหรือใช้ในการกำหนด / บริหารโครงการและการทำงานงบประมาณ

2.7. การบริหารและกับดูแลเทคโนโลยีสารสนเทศที่ดี (IT Governance) ไม่ได้กำกับเทคโนโลยีสารสนเทศไปในทิศทางที่สอดคล้องกับธุรกิจ

สิ่งเหล่านี้ที่เกิดขึ้นก็เนื่องมาจากความล้มเหลวในการวางแผนการทำงานที่ไม่สอดคล้องกัน ความล้มเหลวในการจัดลำดับความสำคัญของงาน การขาดการสร้างนวัตกรรมใหม่ ๆ การขาดการวัดผลการดำเนินงานทางด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับกลยุทธ์ขององค์กร ซึ่งเป็นผลมาจากวัฒนธรรมในการบริหารงานที่ไม่สอดคล้องกันระหว่างการบริหารองค์กรกับเทคโนโลยีสารสนเทศ

ดังนั้นการแก้ปัญหาจุดต่าง ๆ นี้จะสามารถทำได้โดยการพิจารณาถึงกระบวนการจัดการในมุมมองของ Value Chain ในการนำกลยุทธ์ไปสู่การเพิ่มคุณค่า / ผลกำไรได้ โดยมุ่งเน้นการเชื่อมโยง การวางแผนและการกำหนดกลยุทธ์ขององค์กรเข้ากับ การวางแผนทางด้านเทคโนโลยีสารสนเทศ การกำหนดงบประมาณ การกำหนดกิจกรรมทางด้านเทคโนโลยีสารสนเทศ รวมทั้งการวัดผลการดำเนินงานเพื่อติดตามผล

เทคโนโลยีสารสนเทศถูกกำกับโดยวิธีการปฏิบัติที่ดี หรือเป็นเลิศเพื่อแน่ใจได้ว่าสารสนเทศขององค์กรและเทคโนโลยีที่นำมาใช้เป็นไปตามวัตถุประสงค์ของธุรกิจ รวมถึงการนำทรัพยากรไปใช้อย่างรับผิดชอบ และการจัดการความเสี่ยงเป็นไปอย่างเหมาะสม วิธีการปฏิบัติเหล่านี้เป็นพื้นฐานของการกำหนดทิศทางในกิจกรรมต่าง ๆ ด้านเทคโนโลยีสารสนเทศ ได้แก่ การวางแผนและจัดองค์กร การจัดหา และการนำระบบงานออกใช้งานจริง การส่งมอบและการสนับสนุน และการเฝ้าติดตาม โดยมีจุดประสงค์ทั้งสองประการคือ การจัดการความเสี่ยง เพื่อให้มีความปลอดภัย ความน่าเชื่อถือ และการปฏิบัติตามกฎระเบียบข้อบังคับ การได้รับผลประโยชน์ การเพิ่มประสิทธิภาพและประสิทธิผล และให้มีการรายงานผลการดำเนินงานของกิจกรรมด้านเทคโนโลยีสารสนเทศ ซึ่งมีการวัดผลเปรียบเทียบกับวิธีการปฏิบัติและการควบคุมอื่น ๆ

ผู้บริหารระดับสูงขององค์กรต่าง ๆ ในฐานะกรรมการขององค์กร ซึ่งถือได้ว่าเป็นตัวแทนของผู้ถือหุ้นและผู้มีผลประโยชน์รวมได้ตระหนักถึงแนวโน้มและความจำเป็นของการสร้างคุณค่าในการใช้งานเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยเฉพาะความสำคัญของข้อมูลที่ผู้บริหารใช้ในการตัดสินใจซึ่งจำเป็นจะต้องเชื่อถือได้ และมีการรักษาความปลอดภัยของข้อมูลที่เหมาะสม และจุดนี้ทำให้ข้อมูลถือได้ว่าเป็น Intangible Asset สามารถสร้างคุณค่าให้แก่ธุรกิจในการเพิ่มมูลค่าในตลาด และการมุ่งไปสู่การดำเนินงานที่มีศักยภาพอย่างเต็มที่

### กรอบการบริหารและกระบวนการดำเนินงานด้าน IT Governance ตามแนวทาง COBIT (COBIT Framework)

ความสามารถในการบริหารจัดการด้านสารสนเทศ และเทคโนโลยีสารสนเทศที่ใช้ได้อย่างมีประสิทธิภาพ โดยเฉพาะในสภาวะของโลกาภิวัตน์ที่ข่าวสารข้อมูลต่าง ๆ สื่อสารกันได้อย่างรวดเร็วในโลกของข้อมูล อิเล็กทรอนิกส์ที่ไร้ข้อจำกัดในด้านเวลา ระยะเวลา และความเร็ว ความสำคัญของปัจจัยดังกล่าวเกิดขึ้นจากความต้องพึ่งพาอาศัยข้อมูล และระบบเทคโนโลยีสารสนเทศมากขึ้นในการดำเนินงาน

การเพิ่มขึ้นของภาวะเสี่ยงด้านเทคโนโลยีสารสนเทศ และความหลากหลายซับซ้อนของภัยคุกคามขนาดของการลงทุนด้านเทคโนโลยีที่นำไปสู่การเปลี่ยนแปลงโครงสร้าง และการประกอบธุรกิจอย่างฉับพลันตลอดจนการสร้างโอกาส และลดต้นทุนของธุรกิจ

*หลายองค์กรยังไม่ได้ตระหนักถึงความสำคัญของ Risk IT และ IT Risk ที่มีผลกระทบต่อกระบวนการบริหารโดยรวม การก้าวไปสู่การบริหารตามแนว GRC จะช่วยนำทางองค์กรไปสู่ความสำเร็จได้อย่างยั่งยืน*

สำหรับองค์กรหลายแห่งสารสนเทศ และเทคโนโลยีที่นำมาใช้เป็นสินทรัพย์ที่มีค่ายิ่งต่อองค์กร ยิ่งไปกว่านั้นด้วยสภาพการแข่งขันของธุรกิจ และการเปลี่ยนแปลงอย่างรวดเร็วของสภาพแวดล้อมในปัจจุบัน ผู้บริหารจึงมีความคาดหวังอย่างสูงต่อประโยชน์ที่จะได้รับจากระบบเทคโนโลยีสารสนเทศ ทั้งในด้านการเพิ่มคุณภาพของข้อมูล หน้าที่งาน และความสะดวกในการใช้งาน ตลอดจนการลดระยะเวลาในการส่งมอบข้อมูล และเพิ่มระดับการให้บริการให้ดีขึ้นอย่างต่อเนื่อง ในขณะที่สามารถลดต้นทุนในด้านนี้ให้ต่ำลง

การเปลี่ยนแปลงที่เกิดขึ้นอย่างมากของเทคโนโลยีสารสนเทศ และสภาพแวดล้อมในการทำงานที่เกี่ยวข้องก่อให้เกิดความจำเป็นที่ต้องการจัดการกับความเสี่ยงทางด้านเทคโนโลยีสารสนเทศให้ดีขึ้น กระบวนการ

ธุรกิจที่สำคัญจำเป็นต้องอาศัยข้อมูลอิเล็กทรอนิกส์ และระบบเทคโนโลยีสารสนเทศ นอกจากนี้หน่วยงานที่กำกับดูแลได้เพิ่มความเข้มงวดในมาตรการควบคุมด้านสารสนเทศอันเป็นผลมาจากเหตุการณ์ความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และการทุจริตทางอิเล็กทรอนิกส์ที่ได้ปรากฏมากขึ้น การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในปัจจุบัน จึงถือเป็นส่วนสำคัญของธรรมาภิบาลขององค์กร (Enterprise governance)

ภายใต้ธรรมาภิบาลขององค์กร IT Governance ซึ่งเป็นส่วนหนึ่งของการบริหารแบบ GRC มีบทบาทที่สำคัญมากขึ้นอย่างเห็นได้ชัด และได้รับการกำหนดให้เป็นโครงสร้างของความสัมพันธ์ กระบวนการของการกำกับและการควบคุมเพื่อให้องค์กรบรรลุเป้าหมาย โดยการเพิ่มมูลค่าให้องค์กรไปพร้อมกับการรักษาสมดุลระหว่างความเสี่ยงกับผลตอบแทนจากเทคโนโลยีสารสนเทศและกระบวนการที่เกี่ยวข้อง

IT Governance เป็นองค์รวมของความสำเร็จของธรรมาภิบาลขององค์กร โดยทำให้มั่นใจได้ว่าจะมีการปรับปรุงประสิทธิภาพและประสิทธิผลที่สามารถวัดผลได้ของกระบวนการทางธุรกิจที่เกี่ยวข้อง IT Governance ก่อให้เกิดโครงสร้างที่เชื่อมโยงกันระหว่างกระบวนการ ทรัพยากร และข้อมูล กับกลยุทธ์และวัตถุประสงค์ขององค์กร ยิ่งไปกว่านั้น IT Governance ยังก่อให้เกิดการดำเนินงานตามแนวทางการปฏิบัติที่ดี (good / best practice) ในเรื่องการวางแผนและการจัดองค์กร การจัดหาและการนำระบบออกใช้งานจริง การส่งมอบและการสนับสนุน และการเฝ้าติดตามผลการดำเนินงานด้านเทคโนโลยีสารสนเทศ เพื่อให้แน่ใจได้ว่าสารสนเทศขององค์กรและเทคโนโลยีที่ใช้สามารถสนับสนุนวัตถุประสงค์ของธุรกิจ ดังนั้น IT Governance ทำให้องค์กรสามารถใช้สารสนเทศได้อย่างเต็มที่ ยังผลให้เกิดประโยชน์สูงสุด โดยใช้โอกาสให้เกิดประโยชน์ และเกิดความได้เปรียบเชิงแข่งขัน

1. การสร้างความเข้าใจในการกำกับดูแลกิจการที่ดีทางด้านเทคโนโลยีสารสนเทศตามกรอบ IT Governance

#### 1.1. IT Governance กับผู้บริหาร

เป็นโครงสร้างของความสัมพันธ์ และกระบวนการของการกำกับและควบคุมเพื่อให้องค์กรบรรลุเป้าหมาย โดยการเพิ่มมูลค่าให้องค์กรไปพร้อมกับการรักษาสมดุลระหว่างความเสี่ยงกับผลตอบแทนจากเทคโนโลยีสารสนเทศ และกระบวนการที่เกี่ยวข้อง

สารสนเทศขององค์กรต้องสามารถตอบสนองความต้องการด้านคุณภาพ ความน่าเชื่อถือ และการรักษาความปลอดภัยเช่นเดียวกับทรัพย์สินอื่น ๆ ผู้บริหารขององค์กรย่อมต้องใช้ทรัพยากรที่มีอยู่ ไม่ว่าจะเป็นข้อมูล ระบบงานประยุกต์ เทคโนโลยี สิ่งอำนวยความสะดวก และบุคลากร ให้เกิดประโยชน์สูงสุดในหน้าที่

ความรับผิดชอบดังกล่าว และเพื่อให้บรรลุวัตถุประสงค์ขององค์กร ผู้บริหารจะต้องเข้าใจถึงสถานภาพของระบบเทคโนโลยีสารสนเทศของตน และตัดสินใจว่าควรมีการควบคุมและการรักษาความปลอดภัยอย่างไรจึงจะเหมาะสม

ผู้บริหารต้องแน่ใจได้ว่า องค์กรมีระบบ หรือกรอบงานสำหรับการควบคุมภายในที่จะสนับสนุนกระบวนการทางธุรกิจ และมีความชัดเจนว่าแต่ละมาตรการการควบคุมจะช่วยตอบสนองความต้องการด้านข้อมูล และจะมีผลต่อทรัพยากรด้านเทคโนโลยีสารสนเทศอย่างไร ทั้งนี้กรอบงานโคบิต (COBIT Framework) ได้เน้นถึงผลของการควบคุมทรัพยากรด้านเทคโนโลยีสารสนเทศแต่ละประเภทไปพร้อมกับความต้องการของธุรกิจที่ต้องได้รับการตอบสนอง ในแง่ของประสิทธิภาพ ประสิทธิภาพ การรักษาความลับ ความครบถ้วนถูกต้อง สภาพพร้อมใช้งาน การปฏิบัติตามกฎระเบียบข้อบังคับ และความเชื่อถือได้ การควบคุมซึ่งรวมถึงนโยบาย โครงสร้างองค์กร วิธีการปฏิบัติ และระเบียบปฏิบัติเป็นความรับผิดชอบของผู้บริหาร

ทั้งนี้โดยการใช้หลักธรรมาภิบาลขององค์กร ผู้บริหารต้องแน่ใจว่า บุคลากรที่เกี่ยวข้องทั้งหมดใช้ความระมัดระวังอย่างเพียงพอในการบริหาร การใช้ การออกแบบ การพัฒนา การบำรุงรักษา และการปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์การควบคุมด้านเทคโนโลยีสารสนเทศ เป็นคำประกาศถึงผลที่ประสงค์หรือเจตนากรณีในการนำการควบคุมมาใช้ในกิจกรรมด้านเทคโนโลยีสารสนเทศ โคบิตจัดทำขึ้นโดยมีเนื้อหาเน้นไปในมุมมองด้านธุรกิจ โดยได้รับการออกแบบให้สามารถนำไปใช้ได้ไม่เพียงแต่สำหรับผู้ใช้งานและผู้ตรวจสอบเท่านั้น แต่ที่สำคัญยังรวมถึงให้แนวทางที่สมบูรณ์แก่ผู้บริหารและเจ้าของ กระบวนการทางธุรกิจ การดำเนินธุรกิจในปัจจุบันให้ความสำคัญมากขึ้นสำหรับการให้อำนาจแก่เจ้าของกระบวนการทางธุรกิจเพื่อให้สามารถรับผิดชอบต่อกระบวนการทางธุรกิจในทุกเรื่อง โดยเฉพาะในเรื่องการจัดให้มีการควบคุมที่เหมาะสมเพียงพอ

## 1.2. Cobit / โคบิตกับผู้บริหาร

กรอบงานโคบิต สามารถใช้เป็นเครื่องมือสำหรับเจ้าของกระบวนการทางธุรกิจซึ่งจะช่วยในการปฏิบัติหน้าที่ตามความรับผิดชอบดังกล่าว กรอบงานเริ่มต้นอย่างง่าย ๆ โดยสรุปใจความได้ดังนี้

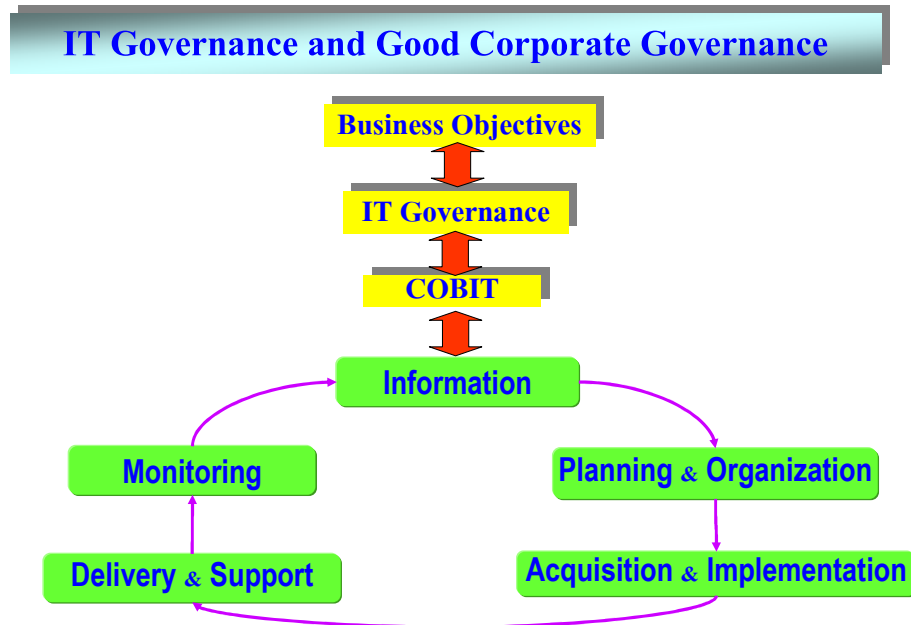
เพื่อให้เกิดสารสนเทศ ที่ช่วยให้องค์กรบรรลุวัตถุประสงค์ตามความต้องการ ทรัพยากรด้านเทคโนโลยีสารสนเทศจำเป็นต้องได้รับการจัดการด้วยชุดของกระบวนการ

กรอบงาน ดังกล่าวขยายความออกเป็นชุดของ วัตถุประสงค์การควบคุม (Control Objectives) ซึ่งมีทั้งหมด 34 หัวข้อ ตามจำนวนของกระบวนการด้านเทคโนโลยีสารสนเทศ ซึ่งได้จัดเป็น 4 โดเมน (Domain) ซึ่งเป็นการควบคุมระดับสูง ได้แก่ การวางแผนและการจัดการ การจัดหาและการนำระบบออกใช้งานจริง การส่งมอบและการสนับสนุน และการเฝ้าติดตาม ซึ่งโครงสร้างดังกล่าวนี้ครอบคลุมทุกแง่มุมของสารสนเทศและเทคโนโลยีที่ใช้ เจ้าของกระบวนการทางธุรกิจสามารถแน่ใจได้ว่า สภาพแวดล้อมของเทคโนโลยีสารสนเทศจะมีระบบการควบคุมที่เพียงพอ โดยยึดถือวัตถุประสงค์การควบคุมในระดับสูงตามหลัก COBIT ซึ่งใช้หลัก Control Objectives สำหรับการจัดการข้อมูลด้านเทคโนโลยีสารสนเทศเพื่อให้เกิด Business Process ที่ดี และนำไปสู่ Control Objectives ขององค์กรอย่างมีประสิทธิภาพ

กรอบงาน CobiT/โคบิต ยังได้ให้แนวทางของ IT Governance โดย IT Governance ได้ให้โครงสร้างการทำงานที่แสดงความเชื่อมโยงจากกระบวนการด้านเทคโนโลยีสารสนเทศ ทรัพยากรด้านเทคโนโลยีสารสนเทศ ไปยังกลยุทธ์และวัตถุประสงค์ขององค์กร IT Governance ได้รวมเอาวิธีการที่ดีที่สุดในการวางแผนและการจัดองค์กร การจัดหาและการนำออกใช้งานจริง การส่งมอบและการสนับสนุน และการเฝ้าติดตามผลการดำเนินงานด้านเทคโนโลยีสารสนเทศเข้าไว้ด้วยกัน IT Governance จะช่วยให้องค์กรใช้ประโยชน์จากสารสนเทศได้อย่างเต็มที่ ได้รับผลตอบแทนที่สูงที่สุดสามารถใช้ประโยชน์จากโอกาสทางธุรกิจ และเกิดความได้เปรียบเชิงแข่งขัน

CobiT/โคบิตยังได้กำหนดให้มีมาตรฐานของระดับการควบคุม (Maturity Model) สำหรับการควบคุมกระบวนการเทคโนโลยีสารสนเทศ เพื่อให้ผู้บริหารสามารถเปรียบเทียบระดับการควบคุมขององค์กรในปัจจุบันกับระดับที่เป็นเลิศของธุรกิจประเภทเดียวกันกับมาตรฐานสากล และกับเป้าหมายที่องค์กรต้องการ ปัจจัยสำคัญสู่ความสำเร็จ (Critical Success Factors) เป็นตัวกำหนดแนวทางด้านการบริหารงานเพื่อให้เกิดผลสำเร็จของการควบคุมในกระบวนการด้านเทคโนโลยีสารสนเทศ ดัชนีเป้าหมายหลัก (Key Goal Indicators) กำหนดตัวชี้วัดความสำเร็จของกระบวนการด้านเทคโนโลยีสารสนเทศในการตอบสนองต่อความต้องการทางธุรกิจให้ผู้บริหารทราบข้อเท็จจริงที่เกิดขึ้นแล้ว ดัชนีวัดผลการดำเนินงานหลัก (Key Performance Indicators) เป็นตัวชี้หลักที่กำหนดแนวทางการวัดผลการดำเนินงานของกระบวนการด้านเทคโนโลยีสารสนเทศว่าเป็นไปได้ดีเพียงใด ในอันที่จะทำให้สามารถบรรลุเป้าหมาย

การบริหารเทคโนโลยีสารสนเทศที่ดีของทุกองค์กรควรจัดให้มีวิธีการที่ดีสำหรับกระบวนการดำเนินงาน 4 ด้าน (IT Process) หลักๆ ซึ่งเน้นการควบคุมระดับสูง คือ



- การวางแผนและการจัดองค์กร (Planning & Organization-PO)
- การจัดหาและการนำระบบงานออกใช้งานจริง (Acquisition & Implementation-AI)
- การส่งมอบและการสนับสนุน (Delivery & Support-DS)
- การติดตามและการสอบทาน (Monitoring-M) ด้านเทคโนโลยีสารสนเทศจากผู้เข้าใจ

จริงทางด้านการ บริหารแบบ บูรณาการระหว่าง IT Governance กับ Good Corporate Governance

IT Governance ได้รับการพิจารณาเป็นส่วนหนึ่งที่ยากกันไม่ได้ กับการกำกับดูแลกิจการที่ดีขององค์กร (Corporate Governance) เพราะเป็นความสำเร็จในด้านการกำกับดูแลกิจการที่ดีขององค์กรที่สามารถสร้างความโปร่งใส ประสิทธิภาพในการดำเนินงาน การแข่งขัน และการให้บริการที่ดีกับลูกค้า

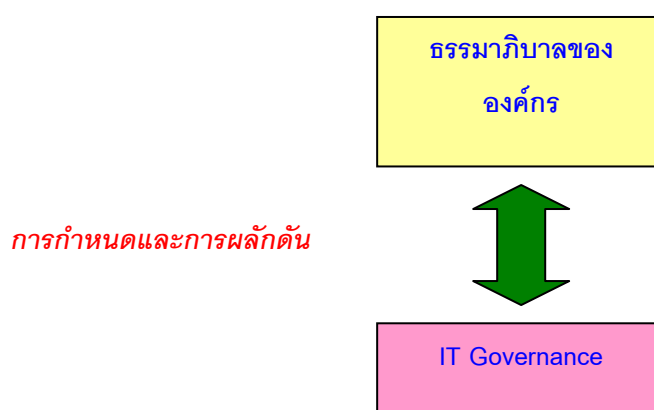
การปฏิบัติที่เท่าเทียมกัน การลดขั้นตอนที่ไม่จำเป็นในการปฏิบัติงาน การประสานงาน การบูรณาการ การสร้างมูลค่าเพิ่มจากวิสัยทัศน์จากความเข้าใจ ทางด้านเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดี ที่สามารถวัดผลได้ทางด้านประสิทธิภาพ และประสิทธิผล ที่สามารถสร้างความได้เปรียบ เพิ่มโอกาสในการแข่งขัน ในการสร้างมูลค่าเพิ่ม ให้กับผู้มีผลประโยชน์ร่วมได้เป็นอย่างมาก

## แนวทางในการกำหนดกิจกรรมหลักของ IT Governance

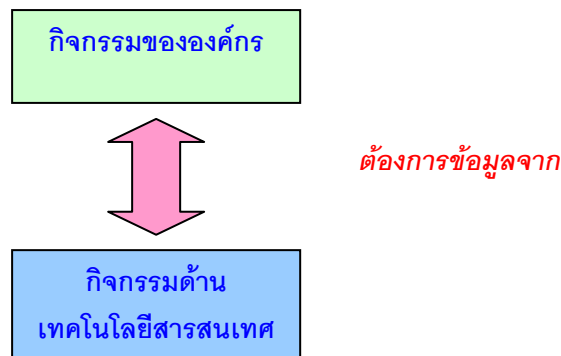
การที่จะประสบความสำเร็จในยุคเทคโนโลยีสารสนเทศ ธรรมชาติขององค์กร และ IT Governance ไม่สามารถแยกกันหรือใช้กฎเกณฑ์ที่แตกต่างกันได้อีกต่อไป ธรรมชาติขององค์กรที่มีประสิทธิภาพ มุ่งเน้นความชำนาญและประสบการณ์ทั้งปัจเจกบุคคลและของหมู่คณะ ซึ่งก่อให้เกิดผลสูงสุด ใฝ่ติดตามและวัดผลการดำเนินงาน และรับประกันการแก้ปัญหาวิกฤต เทคโนโลยีสารสนเทศ ซึ่งเดิมได้รับการพิจารณาว่าเป็นเพียงปัจจัยหนุนกลยุทธ์ของธุรกิจมาเป็นเวลานาน ปัจจุบันได้รับการพิจารณาให้รวมอยู่เป็นหนึ่งในกลยุทธ์ของธุรกิจ

IT Governance มีโครงสร้างที่เชื่อมโยง กระบวนการทางด้านเทคโนโลยีสารสนเทศ (IT process) ทรัพยากรด้านเทคโนโลยีสารสนเทศ (IT resource) และสารสนเทศ (information) ควบคู่ไปกับกลยุทธ์และวัตถุประสงค์ของธุรกิจ IT Governance ได้รวบรวมและจัดให้มีวิธีที่ดีที่สุดสำหรับการวางแผนและการจัดองค์กร การจัดหาและการนำระบบออกใช้งานจริง การส่งมอบและการสนับสนุน และการเฝ้าติดตามการดำเนินงานด้านเทคโนโลยีสารสนเทศ IT Governance ถูกรวมเป็นส่วนหนึ่งของความสำเร็จในธรรมชาติขององค์กร โดยรับประกันในเรื่องการปรับปรุงที่สามารถวัดผลได้ทางด้านประสิทธิภาพและประสิทธิผลของกระบวนการทางธุรกิจ IT Governance ช่วยให้องค์กรใช้ข้อได้เปรียบจากสารสนเทศได้อย่างเต็มที่ เพื่อให้ได้รับผลประโยชน์สูงสุด ใช้โอกาสทางธุรกิจ และเกิดความได้เปรียบเชิงแข่งขัน

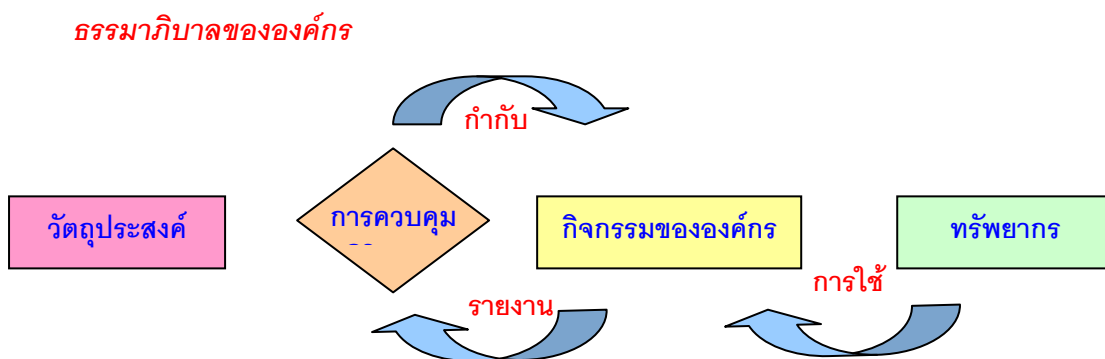
เมื่อมองถึงบทบาทความสัมพันธ์ระหว่างกระบวนการของธรรมชาติขององค์กร และ IT Governance ในรายละเอียด จะเห็นว่าธรรมชาติขององค์กรนั้นเป็นระบบซึ่งทำหน้าที่กำกับ ควบคุม ผลักดัน และกำหนด IT Governance ในขณะเดียวกันเทคโนโลยีสารสนเทศควรให้ข้อมูลที่สำคัญในการจัดทำแผนกลยุทธ์ และควรเป็นส่วนหนึ่งที่สำคัญของแผนฯ อันที่จริงแล้วเทคโนโลยีสารสนเทศอาจมีอิทธิพลต่อโอกาสเชิงกลยุทธ์ที่องค์กรได้จัดสร้างขึ้น



กิจกรรมขององค์กรต้องการข้อมูลที่ได้มาจากการทำงานของระบบเทคโนโลยีสารสนเทศในอันที่จะบรรลุถึงวัตถุประสงค์ขององค์กร องค์กรที่ประสบความสำเร็จต้องแน่ใจได้ว่ากิจกรรมด้านเทคโนโลยีสารสนเทศและการวางแผนกลยุทธ์นั้นมีความสัมพันธ์กัน เทคโนโลยีสารสนเทศจะต้องสอดคล้องกับองค์กรและช่วยให้องค์กรใช้ข้อได้เปรียบจากสารสนเทศได้อย่างเต็มที่ เพื่อให้ได้รับผลประโยชน์สูงสุด ใช้โอกาสทางธุรกิจ และเกิดความได้เปรียบเชิงแข่งขัน



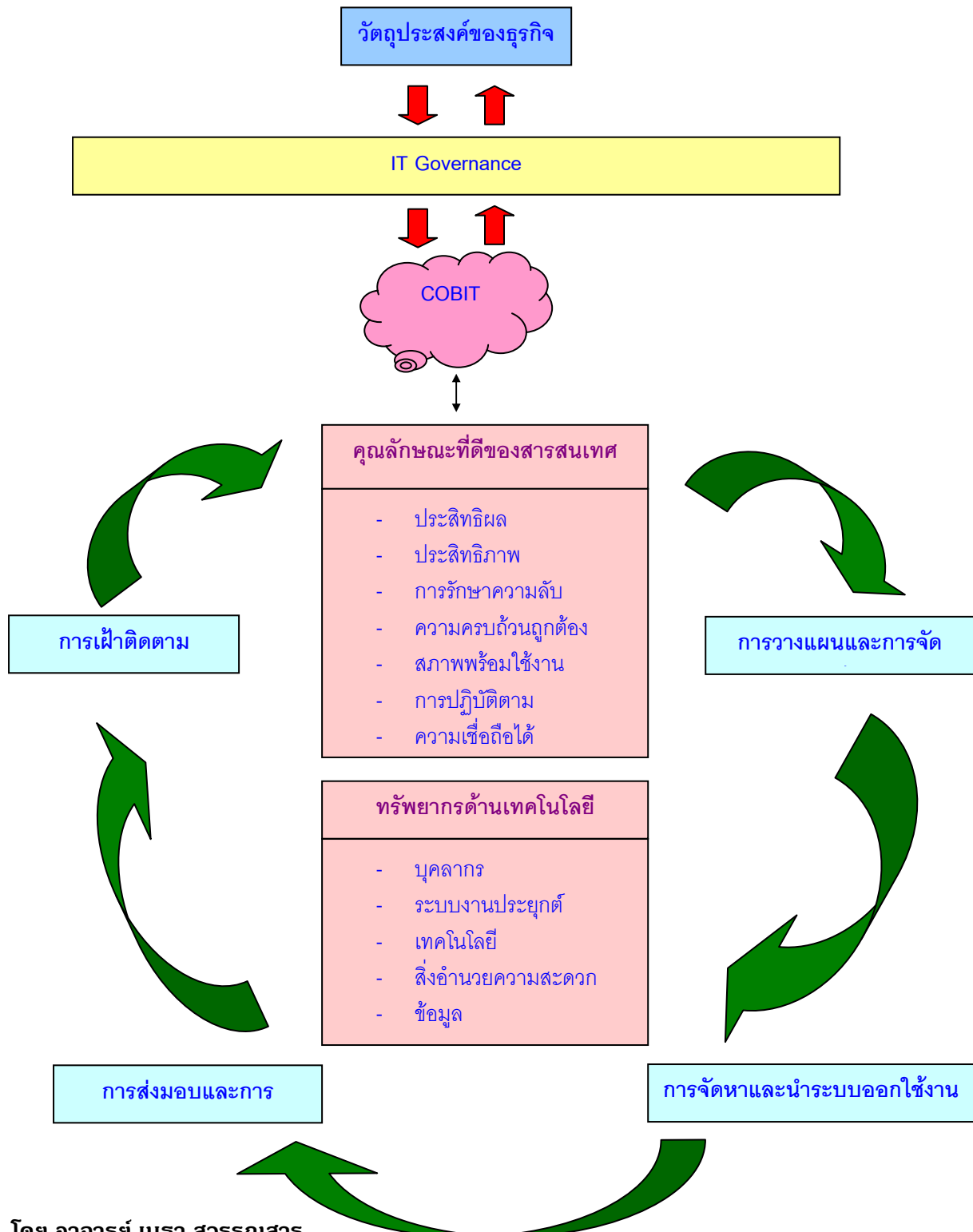
องค์กรมักได้รับการกำกับดูแลด้วยแนวทางการปฏิบัติที่ดี (หรือที่เป็นเลิศ) ซึ่งเป็นที่ยอมรับโดยทั่วไป เพื่อให้แน่ใจได้ว่าองค์กรจะสามารถบรรลุถึงเป้าหมาย โดยมีการควบคุมบางประการเพื่อรับประกันในเรื่องดังกล่าว วัตถุประสงค์เหล่านี้ช่วยให้เกิดการดำเนินงานไปตามทิศทางขององค์กร ซึ่งกำหนดกิจกรรมต่าง ๆ ที่ใช้ทรัพยากรขององค์กร ผลของการดำเนินกิจกรรมจะต้องได้รับการวัดผลและการรายงาน เพื่อเป็นข้อมูลในการปรับปรุงและบำรุงรักษามาตรการการควบคุมอย่างสม่ำเสมอ



เทคโนโลยีสารสนเทศถูกกำกับโดยวิธีการปฏิบัติที่ดี (หรือเป็นเลิศ) เพื่อแน่ใจได้ว่าสารสนเทศขององค์กรและเทคโนโลยีที่นำมาใช้เป็นไปตามวัตถุประสงค์ของธุรกิจ รวมถึงการนำทรัพยากรไปใช้อย่างรับผิดชอบ และการจัดการความเสี่ยงเป็นไปอย่างเหมาะสม วิธีการปฏิบัติเหล่านี้เป็นพื้นฐานของการกำหนดทิศทางในกิจกรรมต่าง ๆ ด้านเทคโนโลยีสารสนเทศ ได้แก่ การวางแผนและจัดองค์กร การจัดหาและการนำระบบงานออกใช้งานจริง การส่ง

มอบและการสนับสนุน และการเฝ้าติดตาม โดยมีจุดประสงค์ทั้งสองประการคือ การจัดการความเสี่ยง (เพื่อให้มีความปลอดภัย ความน่าเชื่อถือ และการปฏิบัติตามกฎระเบียบข้อบังคับ) การได้รับผลประโยชน์ (การเพิ่มประสิทธิภาพและประสิทธิผล) และให้มีการรายงานผลการดำเนินงานของกิจกรรมด้านเทคโนโลยีสารสนเทศ ซึ่งมีการวัดผลเปรียบเทียบกับวิธีการปฏิบัติและการควบคุมอื่น ๆ

### กระบวนการด้านเทคโนโลยีสารสนเทศของโคบิต ที่กำหนดภายใต้ 4 โดเมน



โดย อาจารย์ เมธา สุวรรณสาร

ที่มา : IT Governance Institute และ Information systems Audit and Control Association

## ความเข้าใจในคุณลักษณะที่ดีของสารสนเทศ ของผู้ที่เกี่ยวข้องทุกฝ่าย

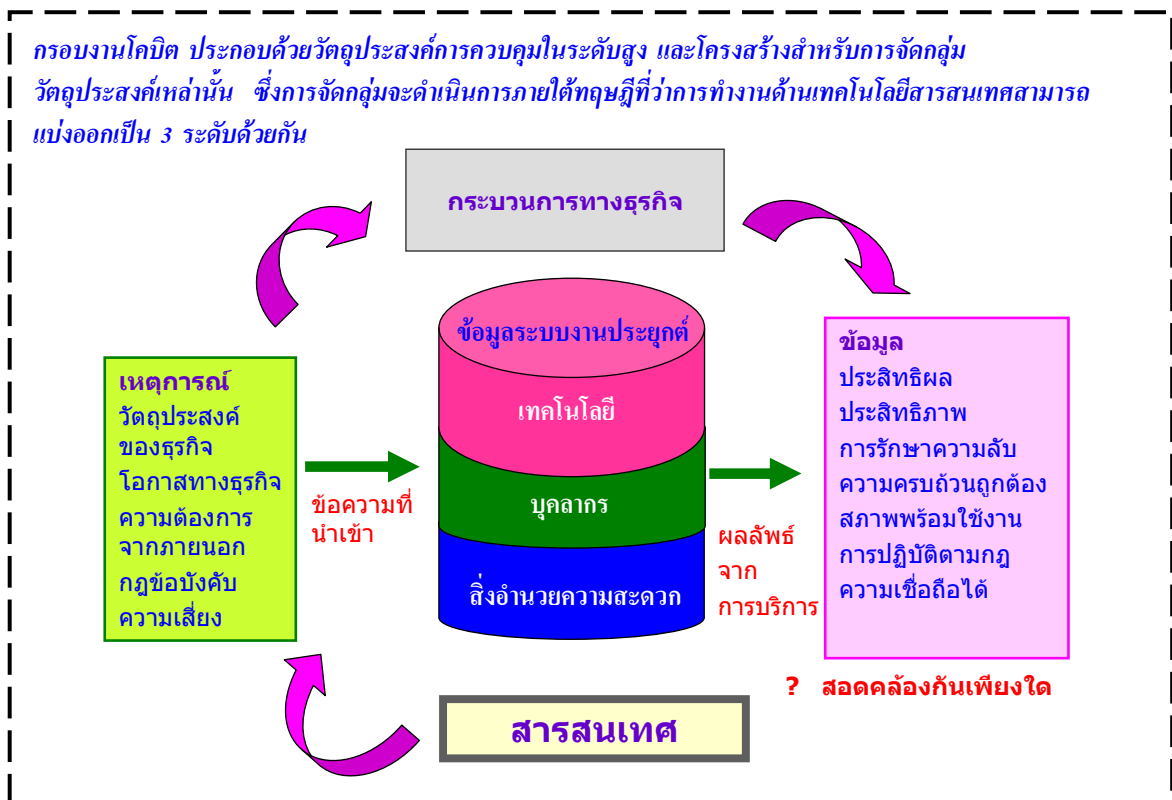
ประสิทธิผล	หมายถึง สารสนเทศที่ตรงประเด็นและสัมพันธ์กับกระบวนการทางธุรกิจ อีกทั้งเป็นสารสนเทศที่ทันต่อเวลา ถูกต้อง สม่าเสมอ และนำไปใช้ประโยชน์ได้
ประสิทธิภาพ	หมายถึง การได้มาซึ่งสารสนเทศโดยการใช้ประโยชน์จากทรัพยากรต่าง ๆ อย่างเต็มที่ (ได้ผลผลิตสูงสุดและประหยัดที่สุด)
การรักษาความลับ	หมายถึง การป้องกันการเปิดเผยข้อมูลที่สำคัญโดยไม่ได้รับอนุญาต
ความครบถ้วนถูกต้อง	หมายถึง ความครบถ้วนและถูกต้องของสารสนเทศ รวมทั้งเป็นสารสนเทศที่ใช้ได้อย่างสอดคล้องกับค่านิยมและความคาดหวังของธุรกิจ
สภาพพร้อมใช้งาน	หมายถึง การใช้สารสนเทศเมื่อมีความต้องการใช้งานในกระบวนการทางธุรกิจทั้งในปัจจุบันและอนาคต รวมถึงการรักษาความปลอดภัยและความสามารถในการใช้งานของทรัพยากรต่าง ๆ ที่เกี่ยวข้อง
การปฏิบัติตามกฎ	หมายถึง การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ และข้อสัญญาที่เกี่ยวข้องกับกระบวนการทางธุรกิจ อาทิเช่น กฎเกณฑ์ข้อบังคับทางธุรกิจที่กำหนดขึ้นจากภายนอก
ความเชื่อถือได้	หมายถึง การให้สารสนเทศที่เหมาะสมแก่ผู้บริหารเพื่อใช้ในการดำเนินกิจการและเพื่อให้ผู้บริหารสามารถปฏิบัติความรับผิดชอบในเรื่องการรายงานข้อมูลทางการเงินและรายงานการปฏิบัติตามกฎ

## ค่านิยมของทรัพยากรด้านเทคโนโลยีสารสนเทศที่กล่าวถึงในโคบิตนั้น มีดังนี้

ข้อมูล	หมายถึง วัตถุประสงค์ต่าง ๆ ในความหมายที่กว้างที่สุด (นั่นคือ ทั้งภายในและภายนอก)
ระบบงานประยุกต์	หมายถึง การทำงานร่วมกันของโปรแกรมคอมพิวเตอร์และการปฏิบัติโดยคน
เทคโนโลยี	หมายรวมถึง ฮาร์ดแวร์ ระบบปฏิบัติการ ระบบการจัดการฐานข้อมูล ระบบเครือข่าย มัลติมีเดีย เป็นต้น
สิ่งอำนวยความสะดวก	หมายถึง ทรัพยากรต่าง ๆ ที่ใช้เพื่อเป็นที่ตั้งและสนับสนุนการทำงานของระบบสารสนเทศ
บุคลากร	หมายถึง ทักษะของพนักงาน ความตื่นตัว และความมีประสิทธิภาพในการวางแผน การจัดการองค์กร การจัดหา การส่งมอบ การสนับสนุน การเฝ้าติดตามระบบสารสนเทศ และการให้บริการสารสนเทศ

เพื่อให้แน่ใจว่าความต้องการสารสนเทศขององค์กรได้รับการตอบสนอง จำเป็นต้องกำหนดมาตรการควบคุมที่เหมาะสม รวมถึงการนำไปใช้ และเฝ้าติดตามทรัพยากรเหล่านั้น อย่างไรก็ตาม องค์กรจะรู้ได้อย่างไรว่าสารสนเทศที่ได้รับมีคุณลักษณะที่ต้องการ จึงเป็นที่มาของความต้องการกรอบงานที่ดีของวัตถุประสงค์ของการบริหารความเสี่ยงและการควบคุมด้านเทคโนโลยีสารสนเทศ แนวคิดดังกล่าวแสดงได้ดังภาพด้านล่างนี้

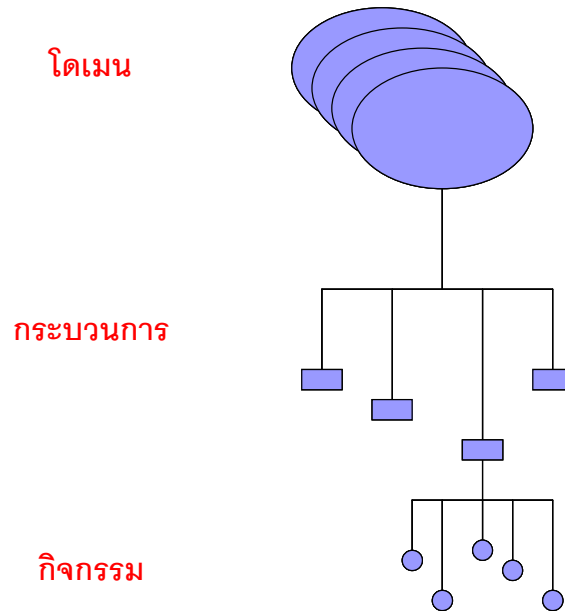
### ความสัมพันธ์ ระหว่างทรัพยากรด้านเทคโนโลยีสารสนเทศกับการส่งมอบบริการต่าง ๆ สามารถแสดงในอีกแง่มุมหนึ่งดังในภาพด้านล่างนี้



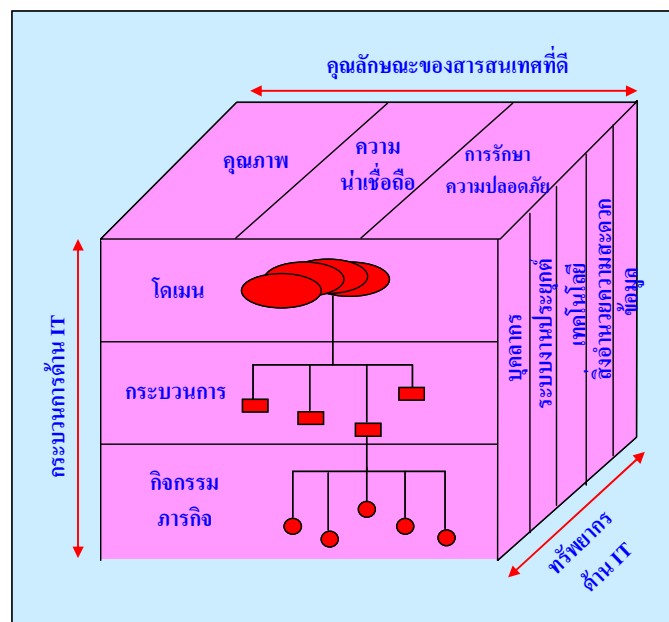
กรอบงานโคบิต ประกอบด้วยวัตถุประสงค์การควบคุมในระดับสูง และโครงสร้างสำหรับการจัดกลุ่มวัตถุประสงค์เหล่านั้น ซึ่งการจัดกลุ่มจะดำเนินการภายใต้ทฤษฎีที่ว่าการทำงานด้านเทคโนโลยีสารสนเทศสามารถแบ่งออกเป็น 3 ระดับด้วยกัน

โดยพิจารณาถึงการจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ เริ่มจากระดับล่างสุด มีกิจกรรมและภารกิจที่จะต้องทำให้สำเร็จและสามารถวัดผลได้ โดยที่กิจกรรมมีลักษณะที่เป็นวงจร ในขณะที่ภารกิจมีลักษณะที่ทำเป็นครั้ง ๆ แยกจากกันในส่วนของกิจกรรมที่มีลักษณะของวงจร จะต้องการมาตรการควบคุมที่แตกต่างไปจากลักษณะของภารกิจที่แยกจากกัน ขึ้นมาในระดับที่สอง ได้แก่ กระบวนการ ซึ่งก็คือ กิจกรรมและ

ภารกิจต่าง ๆ ที่นำมาทำต่อเนื่องกันไปโดยมีการควบคุมในแต่ละจุด ในระดับที่สามที่เป็นระดับสูงสุด คือ กระบวนการต่างๆ ได้รับการจัดกลุ่มโดยแยกเป็นโดเมน ซึ่งการจัดกลุ่มเป็นโดเมนมักจะสอดคล้องกับหน้าที่ความรับผิดชอบในโครงสร้างขององค์กรนั้น ๆ และสอดคล้องกับวงจรของการบริหารงานหรือวงจรการทำงานด้านเทคโนโลยีสารสนเทศ



ดังนั้น สามารถมองกรอบงานในเชิงแนวคิดได้เป็น 3 มิติ คือ คุณลักษณะของสารสนเทศที่ดี (Information Criteria) ทฤษฎีการด้านสารสนเทศ กระบวนการสารสนเทศ มิติทั้งสามนี้สามารถแสดงเป็นภาพของลูกบาศก์ (COBIT Cube) ได้ดังนี้



จากกรอบงานข้างต้นนี้ จะเห็นได้ว่าชื่อของแต่ละโดเมนที่ตั้งขึ้นเป็นคำที่ผู้บริหารมักจะใช้สำหรับกิจกรรมประจำวันของการดำเนินธุรกิจขององค์กรไม่ใช่คำที่ใช้ในภาษาผู้ตรวจสอบ ดังนั้นโดเมนกว้าง ๆ ทั้ง 4 จึงเรียกว่า การวางแผนและการจัดองค์กร การจัดหาและการนำระบบออกใช้งานจริง การส่งมอบและการสนับสนุน และการเฝ้าติดตาม ซึ่งเป็นการควบคุมระดับสูงที่สุด

### คำจำกัดความของโดเมนทั้ง 4 ในการแบ่งกลุ่มหลัก ๆ มีดังนี้

การวางแผนและการจัดองค์กร	โดเมนนี้รวมถึงการวางแผนกลยุทธ์ และยุทธวิธี ตลอดจนการหาทางที่จะทำให้เทคโนโลยีสารสนเทศมีบทบาทสำคัญที่จะทำให้ธุรกิจบรรลุวัตถุประสงค์ ยิ่งไปกว่านั้นการดำเนินงานให้เป็นที่ไปตามวิสัยทัศน์เชิงกลยุทธ์จำเป็นต้องมีการวางแผน สื่อสาร และจัดการในหลาย ๆ ด้าน และท้ายที่สุดองค์กรจำเป็นต้องมีการจัดองค์กรและโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่เหมาะสม
การจัดหาและการนำระบบออกใช้งานจริง	ในการดำเนินงานตามกลยุทธ์ที่วางไว้ จะต้องมีกระบวนการถึงเทคโนโลยีสารสนเทศต่าง ๆ ที่จะต้องใช้ในการดำเนินงาน และจะต้องมีการพัฒนาและจัดซื้อจัดหา การนำระบบออกใช้งานจริง ตลอดจนการผนวกรวมเทคโนโลยีสารสนเทศเข้าเป็นส่วนหนึ่งของกระบวนการทางธุรกิจ ในโดเมนนี้ยังรวมถึงการเปลี่ยนแปลงและการปรับปรุงระบบงานที่มีอยู่แล้วเพื่อให้วงจรของระบบเหล่านี้ดำเนินต่อไป
การส่งมอบและการสนับสนุน	ในโดเมนนี้เกี่ยวข้องกับบริการส่งมอบบริการด้านข้อมูลตามความต้องการ ซึ่งรวมถึงตั้งแต่การดำเนินงานด้านการรักษาความปลอดภัย ความต่อเนื่องของการให้บริการ ไปจนถึงการฝึกอบรม รวมทั้งการจัดให้มีกระบวนการสนับสนุนสำหรับการส่งมอบบริการ ในโดเมนนี้รวมถึงการประมวลผลของข้อมูลจริงโดยระบบงานประยุกต์ ซึ่งมักจัดอยู่ในส่วนของการควบคุมโปรแกรมประยุกต์
การเฝ้าติดตาม	กระบวนการด้านเทคโนโลยีสารสนเทศทั้งหมด จะต้องได้รับการประเมินเป็นประจำเมื่อเวลาผ่านไป เพื่อรับประกันได้ถึงคุณภาพและการปฏิบัติตามข้อบังคับด้านการควบคุม โดเมนนี้จึงเป็นการระบุถึงการกำกับดูแลการดำเนินงานโดยผู้บริหารในด้านกระบวนการควบคุมขององค์กร และประเมินโดยหน่วยงานอิสระทั้งจากผู้ตรวจสอบภายในและภายนอก หรือจากแหล่งทางเลือกอื่น

ควรสังเกตว่า กระบวนการด้านเทคโนโลยีสารสนเทศนี้สามารถนำไปใช้ได้ในทุกระดับขององค์กร เช่น บางกระบวนการจะใช้ในระดัของค์กร บางกระบวนการจะใช้ในระดับหน่วยงานด้านเทคโนโลยีสารสนเทศ บางกระบวนการใช้ในระดับเจ้าของกระบวนการทางธุรกิจ เป็นต้น

ควรสังเกตต่อไปอีกด้วยว่า คุณลักษณะที่ชี้แสดงถึงประสิทธิผลของกระบวนการวางแผนหรือส่งมอบงาน เพื่อตอบสนองความต้องการของธุรกิจนั้น ในบางครั้งอาจรวมถึงคุณลักษณะที่ชี้แสดงถึงความพร้อมใช้งาน ความครบถ้วนถูกต้อง และการรักษาความลับด้วยเช่นกัน ซึ่งในทางปฏิบัติสิ่งเหล่านี้ก็คือ ความต้องการของธุรกิจ เช่น กระบวนการด้าน “การเลือกเทคโนโลยีมาใช้ในการปฏิบัติงาน” จะต้องตอบสนองความต้องการทั้งเรื่องสภาพพร้อมใช้งาน ความครบถ้วนถูกต้อง และการรักษาความลับได้อย่างมีประสิทธิภาพ

อย่างไรก็ดี เห็นได้ชัดเจนว่ามาตรการการควบคุมภายในแต่ละมาตรการนั้นไม่จำเป็นต้องตอบสนองความต้องการทางธุรกิจในเรื่องของสารสนเทศได้เท่าเทียมกันทุกกรณี

- หลัก (Primary – P)

เป็นระดับที่วัตถุประสงค์ของการควบคุมให้ผลโดยตรงต่อคุณลักษณะของสารสนเทศข้อนั้น

- รอง (Secondary – S)

เป็นระดับที่วัตถุประสงค์ของการควบคุมให้ผลในทางอ้อมต่อคุณลักษณะของสารสนเทศข้อนั้น หรือในระดับที่น้อยกว่า

- ว่าง

อาจมีผลต่อคุณลักษณะของสารสนเทศข้อนั้นได้ แต่มีข้ออื่นที่มีผลชัดเจนกว่า และ / หรือ ให้ผลในกระบวนการอื่นได้ชัดเจนกว่า

ดังนั้น การกำหนดกรอบการบริหาร IT Governance ระดับบนจึงไม่ควรพิจารณาการบริหารที่ละกระบวนการ (Process) แต่ควรจะเน้นการบริหารเพื่อมุ่งผลสัมฤทธิ์ในระดับบนหรือผลสัมฤทธิ์ขององค์กรเป็นสำคัญ โดยมีดัชนีเป้าหมายหลัก (Key Goal Indicator) กำหนดตัวชี้วัดความสำเร็จของกระบวนการด้านเทคโนโลยีสารสนเทศในการตอบสนองต่อความต้องการทางธุรกิจของบริษัทฯ ให้ผู้บริหารทราบภายใต้หลักการของกรอบงาน ดังนี้

- ความต้องการด้านคุณภาพของสารสนเทศ (Quality Requirement) ซึ่งจะวัด
  - 1) คุณภาพจากความไม่ผิดพลาด ความน่าเชื่อถือ ความครบถ้วนถูกต้องเป็นไปตามความคาดหวังของผู้ใช้งาน และการสร้างประสิทธิผล ประโยชน์การใช้งานของสารสนเทศ
  - 2) ต้นทุน
  - 3) การส่งมอบ
  
- ความต้องการด้านความไว้วางใจของสารสนเทศ (Fiduciary Requirement) ซึ่งจะวัด
  - 1) ความมีประสิทธิภาพและประสิทธิผลในการดำเนินงาน
  - 2) ความเชื่อถือได้ของข้อมูล
  - 3) การปฏิบัติตามกฎหมายและข้อบังคับต่างๆ
  
- ความต้องการด้านการรักษาความปลอดภัยของสารสนเทศ (Security Requirement) ซึ่งจะวัด
  - 1) การรักษาความลับของข้อมูล
  - 2) ความครบถ้วนถูกต้อง และวัสดุภาพพร้อมใช้งาน

**องค์รวมหลัก (Domains) ของกระบวนการควบคุมกระบวนการทางเทคโนโลยีระดับบนที่นำไปสู่กระบวนการบริหารทางธุรกิจแบบผสมผสานในการบรรลุวัตถุประสงค์ขององค์กรกับความเข้าใจของผู้บริหาร**

1. การวางแผนและจัดการองค์กร (Planning & Organization)

1.1. การวางแผนกลยุทธ์ และยุทธวิธี ตลอดจนการหาหนทางที่จะทำให้เทคโนโลยีสารสนเทศมีบทบาทสำคัญที่จะทำให้ธุรกิจบรรลุวัตถุประสงค์

การดำเนินงานให้เป็นไปตามวิสัยทัศน์เชิงกลยุทธ์ และจำเป็นต้องมีการวางแผนงาน สื่อสาร และจัดการในหลาย ๆ ด้าน

องค์กรจำเป็นต้องมีการจัดการองค์กรที่สัมพันธ์กับโครงสร้างพื้นฐานด้านเทคโนโลยีตาม Business Processes และ IT Processes อย่างเหมาะสม

2. การจัดหาและการนำระบบออกใช้งานจริง (Acquisition & Implementation Plan)
  - 2.1. การดำเนินงานตามกลยุทธ์ที่วางไว้ องค์กรจะต้องมีการระบุถึงเทคโนโลยีสารสนเทศต่าง ๆ ที่ต้องใช้ในการดำเนินงาน และจะต้องมีการพัฒนา หรือจัดซื้อ จัดหา เพื่อการนำระบบออกใช้งานจริง โดยมีแผนงานรองรับอย่างเหมาะสม
  - 2.2. จัดให้มีการผนวกรวมเทคโนโลยีสารสนเทศเข้าเป็นส่วนหนึ่งของกระบวนการทางธุรกิจ
  - 2.3. ปรับปรุงเปลี่ยนแปลงระบบงานที่มีอยู่แล้วเพื่อให้วงจรของระบบงานเหล่านี้ดำเนินต่อไป
3. การส่งมอบและการบำรุงรักษา (Delivery & Support)
  - 3.1. เกี่ยวข้องกับการส่งมอบบริการด้านข้อมูลและสารสนเทศรวมทั้งการดำเนินงานด้านการรักษาความปลอดภัย ความต่อเนื่องของการให้บริการไปจนถึงการฝึกอบรมฯ
  - 3.2. จัดให้มีกระบวนการสนับสนุนสำหรับการส่งมอบการให้บริการทางด้านเทคโนโลยีสารสนเทศและอื่น ๆ
  - 3.3. การประมวลผลข้อมูลจริงโดยระบบงานประยุกต์ (Application System) ซึ่งมักจัดอยู่ในส่วนของการควบคุมเฉพาะระบบงาน
4. การติดตาม (Monitoring)
  - 4.1. กระบวนการด้านเทคโนโลยีสารสนเทศทั้งหมด จะต้องได้รับการประเมินเป็นประจำเมื่อเวลาผ่านไป เพื่อรับประกันได้ถึงคุณภาพ และการปฏิบัติตามกฎเกณฑ์และข้อบังคับด้านการควบคุม ทั้งจากภายนอกและภายในองค์กร
  - 4.2. ระบุการกำกับดูแลการดำเนินงานโดยผู้บริหารในด้านกระบวนการควบคุมขององค์กร และประเมินโดยหน่วยงานอิสระทั้งจากผู้ตรวจสอบภายในและภายนอก หรือจากแหล่งทางเลือกอื่น

#### IT Governance กับความเสี่ยงขององค์กรในมุมมอง Corporate Governance บางมุมมอง

5 องค์กรประกอบของการบริหารของทุกองค์กร และ 5-M Model ที่เกี่ยวข้องกับการระบุปัจจัยเสี่ยงประกอบไปด้วยการบริหารทรัพยากรหลักตามที่จะกล่าวต่อไปนี้

1. Man : ความเสี่ยงด้านปัจจัย ความรู้ความสามารถ ความมุ่งมั่น ความร่วมมือร่วมใจ ของบุคลากรในองค์กร

2. **Machine** : ความเสี่ยงด้านระบบงาน อุปกรณ์ เงิน และเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการพนักงานและการจัดการ
3. **Management** : ความเสี่ยงด้านการบริหารและการจัดการ ในการใช้ทรัพยากรต่าง ๆ อย่างเหมาะสมโดยไม่ยึดติดกับโครงสร้างกายภาพด้าน IT
4. **Mission** : ความเสี่ยงด้านปฏิสัมพันธ์ ความสามารถ ระหว่างบุคลากรระดับต่าง ๆ โดยเฉพาะอย่างยิ่งการประสานงานกับระบบงาน/อุปกรณ์และโครงสร้างในการปฏิบัติงานจริง
5. **Media** : ความเสี่ยงด้านสภาพแวดล้อม การปรับเปลี่ยนความคิด การปฏิบัติ วัฒนธรรมการทำงาน จริยธรรม ระเบียบ ประกาศ คำสั่ง เงื่อนไขต่าง ๆ โครงสร้างองค์กร ระบบงาน ความร่วมมือ การประสานงาน และอื่น ๆ

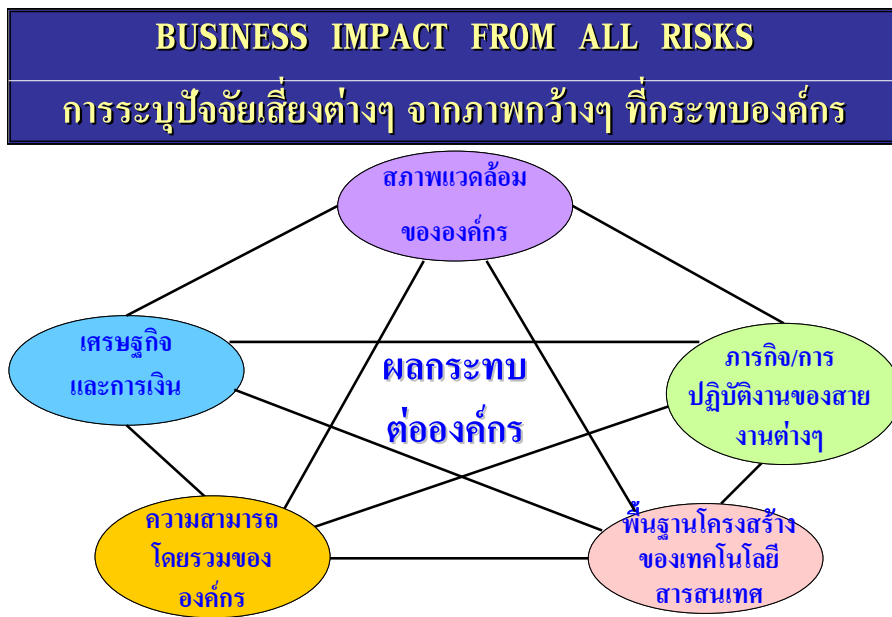
การประเมินความเสี่ยงของหลายองค์กรไม่ได้กล่าวถึง IT และ IT Governance รวมทั้ง IT Risk เท่าที่ควร ทำให้การบริหารความเสี่ยงของหลายองค์กรที่เป็นส่วนหนึ่งของการกำกับดูแลกิจการที่ดีไม่ได้ผลตามที่ต้องการ โดยเฉพาะอย่างยิ่ง ในหลายองค์กรที่ยังให้ความสนใจที่จะระบุปัจจัยเสี่ยงต่าง ๆ ที่เกิดจาก IT Governance / IT Risk จาก 5 องค์ประกอบการบริหาร และ 5M-Model ข้างต้น น้อยมากหรือไม่มีเลยการประเมินประสิทธิภาพการบริหารองค์กร และการกำกับดูแลกิจการที่ดี (Corporate Governance) จึงควรพิจารณาคุณภาพการบริหาร IT และ IT Governance (ITG) รวมทั้งการตรวจสอบด้าน ITG ด้วยเสมอ

**การระบุปัจจัยเสี่ยงต่าง ๆ จากภาพกว้าง ๆ ที่กระทบองค์กร และ Information Technology (IT) และ ITG**

ความเสี่ยง หมายถึง โอกาสที่จะเกิดปัญหา ความผิดพลาด ความสูญเปล่าการรั่วไหล ความล้มเหลว ความเสียหาย หรือเหตุการณ์ซึ่งไม่พึงประสงค์ต่าง ๆ ที่ทำให้งานทั้งระดับประเทศหรือองค์กรไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้ หรือ

ความเสี่ยง หมายถึง สถานการณ์ที่อาจเกิดขึ้น และเป็นอุปสรรคต่อการบรรลุถึงเป้าหมายอย่างมีคุณภาพ

ผลกระทบขององค์กรจากความเสี่ยงโดยภาพกว้าง ๆ ขออธิบายเป็นรูปภาพแทนคำบรรยาย ซึ่งจะมีปัจจัยต่าง ๆ อีกมาก โดยเฉพาะผลกระทบต่อเรื่อง ที่จะมีผลกระทบหรือเป็นภัยคุกคามต่อความสำเร็จ และศักยภาพการแข่งขันทุกระดับโดยย่อ ดังนี้



### บทสรุปของการกำกับดูแลกิจการที่ดีของทุกองค์กร

1. องค์กรและการสร้างการกำกับดูแลกิจการที่ดีประกอบด้วย
  - 1.1. ความรู้ความสามารถ ความมุ่งมั่นที่แท้จริง ความเที่ยงธรรมของบุคลากรภายในองค์กร เพื่อสร้างพื้นฐานหลักที่ดีในการทำงาน
  - 1.2. การสร้างรูปธรรม แก่นสาร และจิตวิญญาณ ในการนำองค์กรไปสู่การกำกับดูแลกิจการที่ดี ภายในเวลาที่กำหนดโดยมีวิธีการสื่อความที่เหมาะสมและทั่วถึงเพื่อความเข้าใจที่ตรงกัน เพื่อ
  - 1.3. ให้องค์กรบรรลุเป้าหมายวัตถุประสงค์หลักอย่างมีประสิทธิภาพและมีประสิทธิผล
2. สร้างสภาพแวดล้อม วัฒนธรรม เพื่อให้เกิดการดำเนินงานที่มีคุณภาพ ศักยภาพในทุกระดับขององค์กร โดยมีลักษณะพิเศษที่เหมาะสมกับองค์กรของตน
3. โครงสร้างและรูปแบบของการกำกับดูแลกิจการที่ดี ก็คือ การสร้างความสัมพันธ์และความสอดคล้องต่อกันระหว่าง ระบบการบริหารความเสี่ยง ระบบการควบคุมภายใน และระบบการตรวจสอบตามฐานความเสี่ยง โดยให้โครงสร้างหลักที่ประกอบเป็นการกำกับดูแลกิจการที่ดี (Good Corporate Governance) ทั้ง 3 ประเภท และโยงใยซึ่งกันและกันนั้นสัมพันธ์กับระบบงานต่าง ๆ และความสามารถในการใช้ IT ได้อย่างคุ้มค่าสอดคล้องกับระบบงานหลัก ๆ ขององค์กร

4. เสริมสร้างบทบาทของผู้ตรวจสอบภายใน และระบบการตรวจสอบภายในขององค์กรอย่างลงตัวระหว่างผู้ตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ ซึ่งมีชื่อเรียกต่าง ๆ กันว่า IT / IS Auditors หรือ BIS / BIT Auditor หรือ Examiner กับผู้ตรวจสอบด้านการเงินทั่วไปที่เรียกว่า Financial Examiners / Auditors หรือชื่ออื่น ๆ เช่น Compliance Auditors ซึ่งขึ้นอยู่กับหน้าที่หลักที่แตกต่างกันของการตรวจสอบ โดยลดช่องว่างให้เกิด Audit Risk ประเภทต่าง ๆ ให้น้อยที่สุดเท่าที่จะทำได้ ซึ่งต้องการความเข้าใจในภาพโดยรวมที่แท้จริงของผู้บริหาร และผู้ที่เกี่ยวข้อง ทั้งนี้ เพราะ IT Governance และความเสถียรด้าน IT เป็นส่วนสำคัญยิ่งของ Good Corporate Governance

5. จัดให้มีการประเมินตนเองของคณะกรรมการต่าง ๆ อย่างเหมาะสมทุก ๆ ปี

6. หลักสำคัญในการจัดทำกรกำกับดูแลกิจการที่ดี

6.1. มีความรับผิดชอบต่อการปฏิบัติหน้าที่

6.2. มีความสำนึกในหน้าที่โดยมีความรู้ ความสามารถที่เหมาะสมในงานที่ทำ

6.3. ปฏิบัติต่อผู้มีส่วนได้เสียอย่างเท่าเทียมกัน

6.4. มีความโปร่งใสในการดำเนินงานและการเปิดเผยข้อมูล

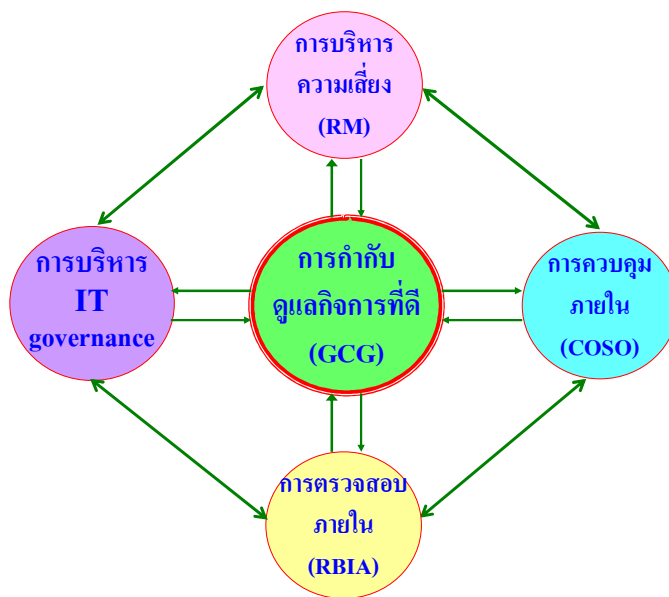
6.5. มีวิสัยทัศน์ที่จะสร้างมูลค่าเพิ่มในระยะยาวให้แก่องค์กร

6.6. มีคุณธรรมและส่งเสริมการกำกับดูแลกิจการที่ดีให้กับองค์กร

ความเข้าใจในวิธีการวิเคราะห์ความเสี่ยงขององค์กร ซึ่งรวมถึงการบริหารความเสี่ยง การควบคุม ความเสี่ยง และการตรวจสอบ โดยใช้ฐานความเสี่ยงอย่างเป็นรูปธรรมจริง ๆ ในแต่ละองค์กรมีความแตกต่างกัน ในการนำความสำเร็จในลักษณะการกำกับดูแลกิจการที่ดีที่มีประสิทธิผลและประสิทธิภาพอย่างแท้จริง

ดังนั้นภาพประกอบต่อไปนี้ จะช่วยให้ผู้ที่เกี่ยวข้องทุกฝ่ายได้เข้าใจตรงกันระหว่างความสัมพันธ์ของการกำกับดูแลกิจการที่ดีขององค์กร (Good Corporate Governance) กับการบริหารความเสี่ยง (Risk Management) การควบคุมภายใน (Internal Control) และการตรวจสอบภายใน (Internal Audit) โดยย่อ ๆ เป็นกรอบใหญ่ก่อนที่จะพัฒนาลงในรายละเอียดไปสู่กระบวนการของการกำกับดูแลกิจการที่ดีขององค์กรอย่างเป็นระบบและมีขั้นตอนแต่ละเรื่องต่อไป

## การกำกับดูแลกิจการที่ดี กับ การบริหารความเสี่ยง





## การประเมินตนเองเพื่อการบริหารจัดการเทคโนโลยีสารสนเทศ/สารสนเทศที่ดี

IT Governance กับคณะผู้บริหารและคณะกรรมการต่าง ๆ

IT Governance คือหน้าที่ความรับผิดชอบเกี่ยวกับการจัดการที่ดีทางด้านเทคโนโลยีสารสนเทศควบคู่กันไปกับความสามารถด้านอื่น ๆ ของคณะผู้บริหารระดับสูงและคณะกรรมการที่ใช้เป็นกรอบและองค์ประกอบของกระบวนการบริหารงานในการปฏิบัติตามนโยบาย กลยุทธ์เพื่อสร้างศักยภาพและคุณค่าเพิ่ม และการเติบโตอย่างยั่งยืนอย่างรู้คุณค่าให้กับองค์กร ควบคู่ไปกับการกำกับดูแลกิจการที่ดีที่แยกกันไม่ได้ในกระบวนการบริหารตั้งแต่การวางแผน การจัดองค์กร การพนักงาน การดำเนินงาน การควบคุม

ทั้งนี้ เพื่อให้เกิดการบูรณาการ การบริหารงานที่เป็นระบบ เป็นระเบียบ เป็นขั้นตอน ลดความซ้ำซ้อน ลดความเสี่ยงโดยทำงานข้ามสายงานและประสานงานระหว่างองค์กรได้อย่างรวดเร็วทันเวลา มีประสิทธิภาพสอดคล้องประสานกับการดำเนินงานระดับต่าง ๆ จากการใช้ความสามารถและศักยภาพของเทคโนโลยีสารสนเทศ และทรัพยากรต่าง ๆ เพื่อการผลักดันความสำเร็จของการจัดการอย่างเป็นกระบวนการ และบูรณาการที่เป็นรูปแบบ

เทคโนโลยีสารสนเทศสร้างความเสี่ยงใหม่ ๆ ที่คาดไม่ถึงในการบริหารงานระดับต่าง ๆ ขององค์กรควบคู่ไปด้วย ดังนั้น การผสมผสานความสามารถด้านต่าง ๆ ขององค์กรกับศักยภาพของระบบงานเทคโนโลยีสารสนเทศ จึงเป็นความรับผิดชอบที่ไม่อาจหลีกเลี่ยงได้ของคณะผู้บริหารขององค์กรในปัจจุบัน

### คณะกรรมการ

1. คณะกรรมการสนใจถามคำถามเกี่ยวกับ IT เป็นครั้งคราว
2. คณะกรรมการได้รับรายงานเกี่ยวกับการริเริ่ม สถานะ และประเด็นที่เกี่ยวข้องกับ IT อยู่เสมอ
3. กลยุทธ์ IT สอดคล้องและเป็นไปในแนวเดียวกับกลยุทธ์ขององค์กร
4. คณะกรรมการเป็นผู้พิจารณาอนุมัติกลยุทธ์ของ IT
5. ในกรณีที่มีคณะกรรมการกำหนดกลยุทธ์ทางด้าน IT (IT Strategy Committee) มีผู้แทนทางด้านธุรกิจเข้าร่วมเป็นกรรมการด้วย
6. คณะกรรมการทบทวนกลยุทธ์ IT อย่างสม่ำเสมอ
7. มีการสื่อสารและสร้างความเข้าใจในเรื่องกลยุทธ์ IT และดำเนินการให้มีการประสานร่วมกันตลอดทั่วทั้งองค์กร
8. คณะกรรมการทบทวนสรุปประเด็นความเสี่ยงด้าน IT อย่างสม่ำเสมอ

9. ในการประชุมคณะกรรมการ มีวาระที่เกี่ยวกับ IT อยู่เสมอ
10. คณะกรรมการมีความเข้าใจชัดเจนในเรื่องการลงทุนด้าน IT ที่สำคัญจากมุมมองทางด้านความเสี่ยงและผลตอบแทนที่จะได้รับ
11. คณะกรรมการได้รับรายงานความคืบหน้าของโครงการ IT ขนาดใหญ่เป็นประจำ
12. คณะกรรมการตระหนักถึงความขัดแย้งที่มีนัยสำคัญระหว่างส่วนงานต่าง ๆ ภายในองค์กรกับการปฏิบัติทางด้าน IT
13. คณะกรรมการได้รับทราบและเห็นภาพว่าองค์กรลงทุนทางด้าน IT เป็นอย่างไร มากน้อยแค่ไหน เมื่อเปรียบเทียบกับองค์กรอื่น ๆ ในลักษณะเดียวกัน
14. คณะกรรมการทำการประเมินผลการดำเนินงานของฝ่ายบริหารในการปฏิบัติตามกลยุทธ์ IT

### การบริหารงาน

1. ความสัมพันธ์ของกระบวนการการดำเนินธุรกิจ (Business Process) กับกระบวนการของ IT (IT Process) ระดับต่าง ๆ และความสอดคล้องกับกระบวนการบริหาร (Management Process)
2. ทรัพยากร โครงสร้างพื้นฐาน และศักยภาพทาง IT ได้รับการจัดสรรเพื่อสนับสนุนให้สามารถบรรลุกลยุทธ์และวัตถุประสงค์ขององค์กร
3. การกำหนดเป้าหมาย การดำเนินงานด้าน IT สมเหตุสมผล
4. นำนโยบายและมาตรฐานด้าน IT ออกใช้ใช้งาน
5. ติดตามดูแลความเสี่ยง และระบุความเสี่ยง IT ที่ยอมรับได้
6. ดำเนินการให้การประเมินผลกระทบทางธุรกิจเป็นส่วนหนึ่งของกระบวนการบริหารความเสี่ยงขององค์กร
7. ประเมินและบรรเทาความเสี่ยงและเปิดเผยความเสี่ยงให้ผู้มีส่วนได้ส่วนเสียในกิจการทราบ
8. โครงสร้างองค์กร (ขนาด ลำดับชั้นของการบังคับบัญชา) สอดคล้องกับเป้าหมายขององค์กร
9. หน่วยงานทางธุรกิจและหน่วยงาน IT รับผิดชอบร่วมกันในการดำเนินงานขององค์กร
10. ผู้บังคับบัญชาอธิบายกลยุทธ์ นโยบาย และเป้าหมายให้ผู้บังคับบัญชาเข้าใจโดยทั่วถึง และถือปฏิบัติในทุกระดับขององค์กร
11. ผู้บริหารมุ่งเน้นกระบวนการ IT ซึ่งมีส่วนในการเพิ่มมูลค่าทางธุรกิจ
12. การใช้เวลาในการตัดสินใจที่สำคัญเกี่ยวกับ IT
13. การลงทุนและการใช้ทรัพยากรด้าน IT มีความโปร่งใส

14. ควบคุมดูแลและจัดทำงบประมาณและแผนการลงทุนด้าน IT
15. งบประมาณ IT ได้ถูกเชื่อมโยงกับเป้าหมายและวัตถุประสงค์ทางกลยุทธ์
16. ผู้บริหารให้ความสำคัญกับต้นทุนและค่าใช้จ่ายทางด้าน IT
17. ผู้บริหารควบคุมงานโครงการ IT ให้อยู่ภายในงบประมาณ
18. กำหนดกลยุทธ์และนโยบายที่ชัดเจนในการให้บริการ IT จากบุคคลภายนอก
19. ระดับชั้นของการรายงานได้สอดคล้องกับความสำคัญทางด้าน IT
20. ผู้บริหารให้ความสำคัญกับศักยภาพทางธุรกิจที่ IT ต้องให้การสนับสนุน
21. ผู้บริหารทางด้านธุรกิจกำหนดและสรรหาบริการทาง IT ใหม่ ๆ

#### **การควบคุมการดำเนินงาน**

1. ผู้บังคับบัญชาทุกระดับชั้นตระหนักถึงความเสี่ยง เข้าใจในลักษณะของความเสี่ยงว่าปัจจัยเสี่ยงด้านต่างๆมีผลต่องานเพียงใด
2. ผู้บังคับบัญชากำหนดวิธีการควบคุมเพื่อป้องกันหรือลดความเสี่ยงและแก้ไขปัญหา
3. การกำหนดขั้นตอนและวิธีการปฏิบัติงานมีความชัดเจน เข้าใจง่าย และสามารถปฏิบัติได้
4. มีการควบคุมที่ดี เพื่อให้ได้ข้อมูลที่ต้องการ เชื่อถือได้ และทันเวลา เพื่อให้สามารถนำไปใช้งานได้  
อย่างมีประสิทธิภาพ
5. มีขั้นตอนและกระบวนการปฏิบัติงานที่ใช้ต้นทุนอย่างมีประสิทธิภาพ
6. การติดตามการปฏิบัติงานอย่างมีประสิทธิภาพ
7. ความเหมาะสมในการแบ่งแยกหน้าที่
8. การควบคุมการใช้งาน IT
9. การควบคุมและเผยแพร่ข้อมูล IT ต่อบุคคลภายนอก
10. ความเหมาะสมและความเพียงพอของกระบวนการรักษาความปลอดภัย และผู้ปฏิบัติงานรับทราบ  
และถือปฏิบัติ

#### **การประเมินผลการดำเนินงาน**

1. ผู้ใช้ (End Users) พึงพอใจกับคุณภาพของการบริหาร/ การดำเนินงานด้าน IT
2. การวัดผลการดำเนินงานด้าน IT มีการวัดมูลค่าเพิ่มทางธุรกิจ และเพิ่มความได้เปรียบในการแข่งขันให้แก่องค์กร

3. โครงการหรือแผนงาน IT ประสบความสำเร็จ สามารถส่งมอบงานได้ตามที่วางแผนไว้
4. ใช้เวลาและค่าใช้จ่ายขององค์กรในการลดความเสี่ยงอย่างเหมาะสมเมื่อเทียบกับผลที่จะได้รับ
5. ระบบการประเมินผลการปฏิบัติงานชัดเจน โปร่งใส อธิบายได้
6. การแก้ไขปัญหาและอุปสรรคจากการทำงาน
7. การสอบทานงานตามลำดับการบังคับบัญชาอย่างต่อเนื่องและสม่ำเสมอ
8. รายงานความคืบหน้าในการปฏิบัติงานอย่างเหมาะสม
9. มีการประเมินการควบคุมภายในสายงานอย่างสม่ำเสมอ และปรับปรุงให้ทันสมัยเป็นประจำ
10. ความเหมาะสมในการประเมินการควบคุมโดยหน่วยงานอิสระ (ตรวจสอบภายใน)

#### บุคลากร

1. บุคลากรทุกระดับมีจำนวนเหมาะสมกับปริมาณและลักษณะของงาน
2. มีความรู้ ความสามารถ และประสบการณ์เหมาะสมกับหน้าที่ ความรับผิดชอบ
3. ผู้ตรวจสอบภายในมีความเป็นอิสระและเป็นกลางในการปฏิบัติหน้าที่ ความรับผิดชอบ
4. อุทิศเวลาอย่างเพียงพอในการปฏิบัติงาน
5. ได้รับการพิจารณาเพียงพอที่จะส่งเสริมการปฏิบัติงานอย่างมีประสิทธิภาพ
6. การทำตัวเป็นแบบอย่างและสนับสนุนวัฒนธรรม ค่านิยมร่วมขององค์กร

#### กิจกรรมโดยรวมที่เกี่ยวข้องกับ IT Governance และบทบาทที่เกี่ยวข้องกับคณะกรรมการ คณะกรรมการตรวจสอบ และผู้บริหารขององค์กร

1. โดยทั่วไป ปัจจัยที่ใช้วัดความสำเร็จทางด้าน IT และ ITG ที่สำคัญ<sup>4</sup> ซึ่งจะเชื่อมโยง นำไปสู่ความสำเร็จขององค์กรโดยรวม จะพิจารณาทางด้านกฎหมาย ด้านเทคนิค ด้านการจัดองค์กรและกระบวนการปฏิบัติงานทั่วทั้งองค์กร ไม่ว่าจะใช้โปรแกรมประยุกต์เพื่อการบริหารทรัพยากรทั่วทั้งองค์กร ซึ่งอาจเป็นระบบ Enterprise Resource Planning (ERP) หรือไม่ก็ตาม การวางแผน การปฏิบัติ การสอบทาน และการแก้ไข เพื่อนำไปสู่ความคิดในการพัฒนางานด้าน ITG ให้เป็นส่วนหนึ่งของการกำกับดูแลกิจการที่ดี (GCG) นั้น เป็นทั้งหน้าที่และความรับผิดชอบของผู้บริหารระดับสูงและคณะกรรมการของทุกองค์กร

<sup>4</sup> การวัดความสำเร็จนี้จะพบกับคุณภาพการปฏิบัติงาน การบริหารงานด้าน IT และ ITG ตั้งแต่ระดับ 1 ถึง ระดับ 5 หน่วยงานของรัฐในประเทศไทยส่วนใหญ่จะอยู่ใน ระดับ 2 จากระดับ 5 ที่ดีที่สุด ทั้งนี้ควรดูข้อ 7-11 ประกอบเป็นเบื้องต้นได้ระดับหนึ่ง

## 2. กิจกรรมด้าน IT Governance โดยย่อ จะประกอบด้วย

กำหนด IT Master Plan วิธีการปฏิบัติงานใหม่ที่ใช้ IT และผลกระทบทางด้าน IT ที่มีต่อองค์กรและวิธีการทำงานใหม่

กำหนดความคาดหวังและผลตอบแทนจากการใช้ IT อย่างคุ้มค่า

การพิจารณา Physical Security และ Information Security Governance ที่เป็นรูปธรรม

กำหนดหน้าที่ ความรับผิดชอบ การประสานงาน การใช้ IT ของแต่ละสายงานทั่วทั้งองค์กร

การพิจารณาใช้ IT สนับสนุนกระบวนการปฏิบัติงาน ทั้งภายในและภายนอกอย่างสอดคล้องและต่อเนื่องทั่วถึงกันทุกระบบ ที่สำคัญขององค์กร

กำหนดจุดควบคุมกระบวนการสอบทาน ติดตาม ในกระบวนการปฏิบัติงาน

รวบรวมและบริหารทรัพยากรอย่างผสมผสานของ 5 องค์กรประกอบในการบริหาร ตั้งแต่การวางแผนการจัดองค์กร การพนักงาน การกำกับไปจนถึงการติดตาม

การบริหารและจัดการกับความเสี่ยงที่เกี่ยวข้องทั่วทั้งองค์กร

จัดให้มีการวัดผลการปฏิบัติงานทุกสายงาน และภาพโดยรวมขององค์กร

สอบทาน และรับรองคุณภาพของผลการปฏิบัติงานโดยรวมจากการมี การใช้ IT และ IT Governance (ITG)

การพิจารณาความดีความชอบจากการบริหาร และการปฏิบัติงานด้าน ITGและด้านทั่วไปอย่างผสมผสาน ทั่วทั้งองค์กรในส่วนที่เกี่ยวข้อง

## บทบาทของ CIO และ CEO ที่เปลี่ยนไป เพื่อการสร้างมูลค่าเพิ่มในการบริหารยุคใหม่

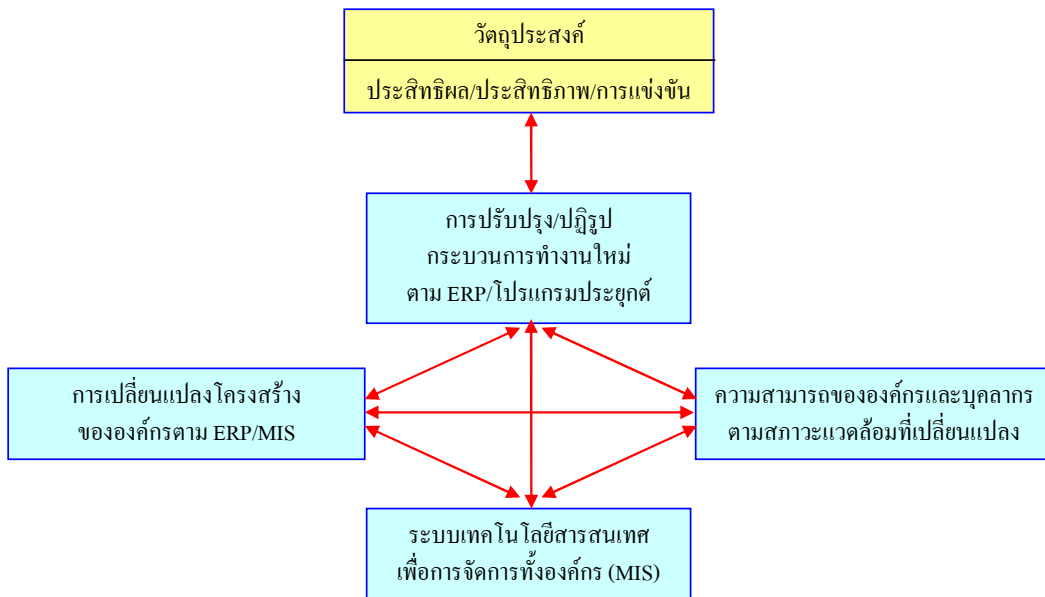
บทบาทหน้าที่ของ CIO โดยปกติจะเน้นถึงการให้บริการในส่วนของ Utility ต่าง ๆ ในการรักษาระบบที่ใช้ อยู่ให้การปฏิบัติงาน / การให้บริการสามารถดำเนินไปได้ ซึ่งรวมถึงการบริหารจัดการ IT Architecture และให้ความรู้ความเข้าใจและผลักดันในการคิดค้นพัฒนาผลิตภัณฑ์ และ Solutions ใหม่ ๆ อย่างไรก็ตามบทบาทที่มีความสำคัญมากขึ้นและถือได้ว่าเป็นปัจจัยสู่ความสำเร็จในการจัดการด้านเทคโนโลยีสารสนเทศในยุคปัจจุบัน คือ

1. สื่อความรู้ และความเป็นผู้นำในการสื่อให้เห็นความสำคัญและคุณค่าของเทคโนโลยีสารสนเทศ ที่มีต่อองค์กร รวมทั้งการบริหาร IT Investment ของระบบเทคโนโลยีสารสนเทศที่มีอยู่และที่จะเกิดใหม่
2. บริหารและจัดการบุคลากรทางด้าน เทคโนโลยีสารสนเทศ เพื่อให้ได้มาและรักษาไว้ซึ่งบุคลากรที่ดีที่สุด
3. บริหารการสื่อสารที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ให้ทั่วทั้งองค์กร รวมทั้งก้าวข้ามการต่อต้านในองค์กร
4. เป็นผู้วางกลยุทธ์ นำเสนอแนวคิดในการวางกลยุทธ์ขององค์กรและบริหารความสมดุลของการลงทุนในกลุ่มผลิตภัณฑ์และบริการต่าง ๆ ในแต่ละ Business Unit และฝ่าย
5. ใช้วิธีการการวิเคราะห์การลงทุนและผลตอบแทนในการวิเคราะห์ความเสี่ยงของ IT Solutions ที่จะนำมาใช้ ในการเพิ่ม Productivity สร้างการเติบโตของรายได้ให้เกิดขึ้น และลดต้นทุน
6. รักษาระดับความเสี่ยงที่มองเห็นและยอมรับได้ใน IT Portfolio และมั่นใจถึงผลตอบแทนทางการเงินที่อยู่ในระดับที่คาดหวัง
7. บริหารและวัดผลการดำเนินงานและความสอดคล้องของ IT Portfolio Management

### คุณค่าความเข้าใจในการบริหารทรัพยากรด้าน ITG บางมุมมอง

การปรับปรุง/ปฏิรูปกระบวนการทำงานใหม่ตามโปรแกรมประยุกต์ หรือโปรแกรม ERP (Enterprise Resource Planning) กับการเปลี่ยนแปลงโครงสร้าง และวิธีการทำงานใหม่ขององค์กร

ขอแสดงปัจจัยที่เกี่ยวข้องเนื่อง ผลกระทบจากความคิดที่เป็นระบบตามรูปภาพ ดังนี้



ข้อสังเกตจากรูปภาพข้างต้น จะเกิดอะไรขึ้นถ้าการปฏิรูปโครงสร้างขององค์กรใหม่และการเปลี่ยนแปลงกระบวนการทำงานใหม่ที่ไม่สอดคล้องกัน โดยเฉพาะในกระบวนการว่าจ้างที่ปรึกษาภายนอกแยกเป็น 2 ทีม และกำหนดขอบเขตของงาน (Term of Reference – TOR) ไม่สัมพันธ์กันเท่าที่ควรจะเป็น หรือไม่สัมพันธ์กันเลย คณะกรรมการว่าจ้าง คณะกรรมการตรวจรับ มีความเข้าใจในกระบวนการทำงานทั่วทั้งองค์กรแตกต่างกัน โดยเฉพาะอย่างยิ่ง ทางด้านกระบวนการ IT Governance ที่เกี่ยวข้อง

นอกจากนี้กระบวนการของ IT Governance ก็ยังสัมพันธ์กับวิธีการทำงานใหม่ และการทำงานข้ามสายงาน และการประสานงานทั่วทั้งองค์กร การวัดประสิทธิภาพการดำเนินงานขององค์กรควรใช้แนวทางวัด หรือเครื่องมือใดจึงจะเหมาะสม

เรื่องนี้เพียงเรื่องเดียว ก็สร้างความเสี่ยงจากโอกาส และภัยคุกคามที่จะเกิดปัญหา ความผิดพลาด ความสูญเปล่า ความล้มเหลว ความเสียหาย และเรื่องที่ไม่พึงประสงค์ต่าง ๆ อย่างคาดไม่ถึง รวมทั้งการสูญเสียเงินจำนวนมากมายหลายร้อยล้าน หรือสูงกว่าพันล้านบาท รวมทั้งค่าใช้จ่ายต่อเนื่องจากการบำรุงรักษา

และค่าเสื่อมจำนวนมากเป็นเวลานาน รวมทั้งความเสียหายทรัพยากรด้านอื่น ๆ ที่ยากต่อการแก้ไข และมีผลกระทบต่อประสิทธิภาพของงานเป็นอย่างยิ่งของหลายองค์กรที่เกิดขึ้นแล้ว และกำลังจะเกิดขึ้นในอีกหลายองค์กรต่อไปด้วย

หากจะพิจารณามุมมองอื่น ๆ ที่เกี่ยวข้องทั้งในภาพ Macro และ Micro และความเกี่ยวเนื่องก็จะพบกับความเสี่ยงที่จะเกิดความเสียหายที่จะตามมาอีกมาก และจะมีต้นทุนในการตัดสินใจใหม่ในการปรับปรุง บริหาร ทรัพยากรใหม่ตามมาอีกมากแน่นอน โดยเฉพาะการปฏิบัติงานของพนักงาน การประสานงานทั่วทั้งองค์กร และการสูญเสียของการใช้ทรัพยากรต่าง ๆ จากการบริหารงานที่ไม่ได้คุณภาพและขาดความสัมพันธ์ระหว่างกัน

### IT Governance กับการควบคุมและการตรวจสอบตามฐานความเสี่ยง<sup>5</sup>

วัตถุประสงค์ในการกำกับควบคุม และการตรวจสอบทางด้าน IT Governance มีความแตกต่างจากการกำกับ การควบคุม และการตรวจสอบตามฐานความเสี่ยงของงานโดยทั่วไปเป็นอย่างมากทั้งในลักษณะของงาน เทคนิค และเครื่องมือที่ใช้ แต่เนื่องจากงานด้าน IT Governance กับ Corporate Governance เป็นกระบวนการบริหารที่แยกกันไม่ได้ ดังนั้น การผสมผสานองค์ประกอบต่าง ๆ ของการบริหารเข้าด้วยกันอย่างกลมกลืนและลดช่องว่างทุกชั้นตอนให้มากที่สุด จนเสมือนหนึ่งเป็นกลไกเดียวกัน โดยมีความเกี่ยวพันสัมพันธ์กัน และลดความซ้ำซ้อนให้มากที่สุดเท่าที่จะทำได้แล้ว จะเป็นทั้งเป้าหมายและวัตถุประสงค์ในการสร้างประสิทธิผล และประสิทธิภาพขององค์กรแน่นอน

คณะกรรมการและผู้ตรวจสอบภายในทุกประเภทจึงต้องมีบทบาทและปฏิบัติหน้าที่ให้ครอบคลุมถึงเรื่อง IT Governance อย่างหลีกเลี่ยงไม่ได้ เพราะในที่สุดแล้ว IT Governance จะมีผลต่อการดำเนินงานและฐานะทางการเงินในที่สุดด้วย

ดังนั้น ความเข้าใจพื้นฐานของ IT Governance ที่เกี่ยวกับ Corporate Governance และผลกระทบต่อการบริหารความเสี่ยง เพื่อการเติบโตอย่างยั่งยืนเป็นเรื่องที่น่าสนใจยิ่ง

<sup>5</sup> ระบบ IT ควรเชื่อมโยงกันได้อย่างสมบูรณ์ ทั่วองค์กร ทั้ง Front-Middle-Back Office เพื่อลดความซ้ำซ้อนในการปฏิบัติงาน โดยการใช้ IT และเพิ่มประสิทธิภาพ การบริหารงานตรวจสอบ ควบเน้นการบริหารทรัพยากร การประสานงาน การบริหารความเสี่ยงและการยอมรับสภาพความเสี่ยงด้าน IT และ ITG เมื่อเปรียบเทียบกับมาตรฐาน

## สรุป การประเมินตนเองเพื่อการควบคุมภายในและเพื่อการบริหารความเสี่ยง

เพื่อให้ IT Governance กับการบริหารความเสี่ยงมีประโยชน์ใช้ได้ในทางปฏิบัติเบื้องต้นระดับหนึ่งและอาจใช้เป็นส่วนสำคัญในการสร้างมูลค่าเพิ่มในทุกระดับขององค์กรประกอบในการบริหาร และการจัดการในโอกาสต่อไปนั้น ขึ้นอยู่กับความมุ่งมั่น จากความพยายามที่จะทำความเข้าใจกับองค์ประกอบของการกำกับดูแลกิจการที่ดี (Corporate Governance) ที่สัมพันธ์กับการนำ Information Technology (IT) หรือการนำเทคโนโลยีสารสนเทศมาผสมผสานกับความสามารถขององค์กรทางด้านต่าง ๆ เพื่อบรรลุวัตถุประสงค์และเป้าหมายทั้งในระดับประเทศรวมทั้งระดับองค์กรเป็นหลัก

เมื่อมีความคิดว่า IT Governance เป็นส่วนหนึ่งของและที่แยกไม่ได้จาก Corporate Governance และมีความเข้าใจถ่องแท้แล้ว การสื่อสารเพื่อให้เกิดความเข้าใจถึงคุณค่าของ IT Governance กับการบริหารความเสี่ยง การควบคุมภายใน และการตรวจสอบภายในตามฐานความเสี่ยง ซึ่งเป็นองค์ประกอบที่เกี่ยวข้องของการกำกับดูแลกิจการที่ดี กระบวนการเรียนรู้และการบริหารในเชิงรุก(Pro-Active) ควรกระทำต่อเนื่องสำหรับพื้นฐานเบื้องต้นก็คือ

### การประเมินตนเองเพื่อการบริหารความเสี่ยง (Control Self Assessment – CSA)

การดำเนินการด้าน IT และ IT Governance จะดำเนินการอย่างเป็นระบบ โดยใช้วิธีการหลากหลายตามความเหมาะสม และความเข้าใจขององค์กร คือใช้ Risk – Based, Objective – Based, Control – Based, Process – Based, Departmental – Based และการผสมผสานอย่างเหมาะสม องค์กรก็จะได้ภาพที่น่าสนใจงานทางด้าน IT และ ITG มากที่คาดไม่ถึง หากกระบวนการจัดทำ CSA ซึ่งมีหลายรูปแบบ รวมทั้งบุคลากรที่เกี่ยวข้อง มีความเข้าใจและมีความสมดุลระหว่างผู้อำนวยความสะดวก (Facilitator) ซึ่งทำหน้าที่กำกับการทำ CSA กับทีมงานที่เกี่ยวข้องเข้าใจเทคนิคและกระบวนการทำ CSA ดีพอ และต้องไม่ลืมว่า IT Governance เป็นองค์ประกอบส่วนหนึ่งที่สำคัญของการกำกับดูแลกิจการที่ดี การพิจารณาจัดทำ CSA ต้องคิดและเข้าใจองค์รวมของการบริหารงานทั้งระบบขององค์กร โดยเฉพาะอย่างยิ่งความเข้าใจของ Organizational Governance Process ก่อนการวางแผน การจัดโครงสร้างองค์กร การพนักงาน การกำกับและการติดตามงาน ข้อสำคัญก็คือต้องไม่ลืมเรื่อง Risk IT และ IT Risk และผลกระทบที่เกี่ยวข้อง

วิธีที่ง่ายที่สุดในการทำ CSA โดยใช้เวลาน้อยที่สุด คือ การประเมินตนเองแบบกว้าง ๆ เป็นเพียงเบื้องต้น โดยเฉพาะหัวข้อสั้น ๆ ที่ได้กล่าวแล้วโดยสังเขปข้างต้น เช่น การสร้าง Organizational Governance Process และ Information Security Governance ด้านต่าง ๆ ที่คำนึงถึงความสามารถในการดำเนินงานอย่าง

ต่อเนื่อง โดยคำนึงถึงไม่เพียงแต่ IT Governance แต่ต้องรวมถึง Corporate Governance หรือกำกับดูแลกิจการที่ดี และองค์ประกอบที่เกี่ยวข้องเพื่อการเติบโตอย่างยั่งยืนขององค์กรเป็นสำคัญ

การปรับปรุง การบริหารความเสี่ยงจากการทำ CSA<sup>6</sup> จะนำไปสู่การบริหารที่มีประสิทธิภาพเพิ่มขึ้น นี้ก็คือส่วนหนึ่งของการกำกับดูแลกิจการที่ดี อันเกิดจากภายในองค์กรเอง ซึ่งมีความสำคัญมากเพราะเกิดจากการริเริ่มของผู้บริหารขององค์กรและสอดคล้องกับคำกล่าวในลักษณะของคำที่มีความสัมพันธ์กัน และมีความหมายสำหรับคณะกรรมการผู้บริหารทุกระดับ และผู้ปฏิบัติงานทุกคน ทั้งนี้ ต้องไม่ลืมว่า IT Governance เป็นส่วนหนึ่งของ Corporate Governance

### ความเชื่อและหลักการของ IT Governance สำคัญยิ่งกว่าวิสัยทัศน์

IT Governance ทำให้เกิดการบูรณาการการบริหารที่เป็นระบบ เป็นระเบียบ เป็นขั้นตอน ลดความซ้ำซ้อน สร้างประสิทธิภาพและประสิทธิผลในการดำเนินงาน การปฏิบัติตามกฎหมาย กฎเกณฑ์ ระเบียบฯ ซึ่งจะมีผลทำให้เกิดประสิทธิภาพทางการเงินอย่างเป็นรูปธรรม และมีความโปร่งใส ซึ่งเป็นไปตามเป้าหมายในการดำเนินงานตามหลักการกำกับดูแลกิจการที่ดีอย่างสำคัญยิ่ง

วิสัยทัศน์ซึ่งตามด้วยพันธกิจของประเทศและขององค์กรอาจเปลี่ยนแปลงได้ขึ้นอยู่กับสภาวะแวดล้อมและทิศทางของประเทศและขององค์กร ที่จะกำหนดความต้องการของตนเองในอนาคตซึ่งเปลี่ยนแปลงได้ง่ายกว่าความเชื่อและหลักการของ IT Governance ตามที่กล่าวในเบื้องต้น! แต่ถ้าความเข้าใจในเรื่อง IT Governance ได้รับการพิจารณาว่าเป็นเพียงความรับผิดชอบในระดับปฏิบัติการของฝ่ายเทคโนโลยีสารสนเทศแล้วจะส่งผลกระทบต่ออย่างสำคัญยิ่งต่อกระบวนการบริหาร การจัดการ และความสำเร็จต่อการบรรลุวัตถุประสงค์ เป้าหมาย กลยุทธ์ พันธกิจ และวิสัยทัศน์ของประเทศและขององค์กรโดยรวม

### IT Governance มีความแตกต่างจาก IT ในระดับของวิสัยทัศน์ และกระบวนการบริหารความเสี่ยง

กระบวนการจัดการของทุกองค์กรโดยทั่วไป ประกอบด้วย 5 องค์ประกอบที่สำคัญคือ การวางแผน การจัดองค์กร การพนักงาน การกำกับดูแล และการควบคุม จะขอยกตัวอย่างของ IT Governance ทางด้านการวางแผนโดยสรุปดังนี้

<sup>6</sup> ควรคิดให้ลึกเชิงวิเคราะห์และคิดให้กว้างอย่างสร้างสรรค์ในการพิจารณาและตัดสินใจอย่างเป็นระบบ เพื่อสร้างมูลค่าเพิ่มในงาน ทรัพยากรต่าง ๆ ขององค์กร สำหรับผู้ตรวจสอบภายใน การประเมิน IT และ IT Governance ควรพิจารณาผลกระทบและการประสานงานต่อไปยังเป้าหมาย การตรวจสอบทางด้าน Operational - Financial - Compliance เพื่อลดความเสี่ยงทางด้าน Audit Risk ที่เกี่ยวข้องอย่างเป็นระบบ

### การวางแผนกลยุทธ์ – การระบุวัตถุประสงค์ ปัจจัยเสี่ยง

1. ถ้าไม่มีการกำหนดแผนระยะยาวและระยะสั้นทางด้านกลยุทธ์ ทำให้การทำงานที่ใช้ระบบ IT ของส่วนงานต่าง ๆ ไม่สอดคล้องและเป็นไปในทิศทางเดียวกันมีผลทำให้ไม่สามารถบรรลุวัตถุประสงค์ระดับองค์กรและระดับส่วนงานต่าง ๆ ได้
2. หากแผนระยะยาวไม่มีการปรับปรุงและพัฒนาจะทำให้ระบบงานโดยรวมไม่ทันสมัย และไม่สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยี ทำให้เกิดความเสียหายทางด้านประสิทธิภาพ การแข่งขัน
3. หากไม่มีการสื่อสารแผนงานทางด้าน IT หรือผู้ที่เกี่ยวข้องกับแผนงานดังกล่าวไม่ทราบหรือไม่เข้าใจในแผนงานนั้นจะส่งผลกระทบต่อความสำเร็จต่อแผนงานโดยรวม
4. หากไม่มีการติดตามประเมินผลแผนงานทางด้าน IT และระบบงานที่ใช้อยู่ในปัจจุบันจะทำให้ไม่สามารถประเมินประสิทธิภาพและประสิทธิผลของแผนรวมทั้ง ระบบงานที่ใช้อยู่ในปัจจุบันว่าได้ถูกใช้งานอย่างเหมาะสม สอดคล้องกับความต้องการขององค์กรหรือไม่ และจะปรับปรุงให้เหมาะสมอย่างไร

ผู้บริหารระดับสูงควรมั่นใจว่า IT Issues ได้รับการประเมินและสะท้อนถึงแผนระยะสั้นและระยะยาว และควรมีการพัฒนาให้มั่นใจได้ว่าจะมีการนำ IT มาปรับใช้ให้สอดคล้องกับภารกิจและกลยุทธ์ขององค์กร การวางแผนควรรวมถึงกรรมวิในการชักชวนผู้ที่เกี่ยวข้องทั้งภายในและภายนอกองค์กรที่ได้รับผลกระทบจากแผนกลยุทธ์ทางด้าน IT โดยกำหนดโครงสร้างและการวางแผนที่เป็นมาตรฐาน และต้องรับผิดชอบต่อผลที่ได้จากการประเมินความเสี่ยงทางด้านเทคโนโลยี บุคลากร ด้านธุรกิจ และด้านสิ่งแวดล้อม ควรมีดัชนีที่วัดเป้าหมายและคุณภาพของแผน และตัวแผนทางด้าน IT เองก็ควรจะสอดคล้องและสัมพันธ์กับแผนอื่น ๆ ภายนอกองค์กรด้วย

**IT Governance เป็นการสร้างคุณค่าเพิ่มจากศักยภาพของเทคโนโลยีสารสนเทศ (IT) ในทุกรูปแบบของกระบวนการจัดการ**

จากตัวอย่างข้างต้นของการวางแผนกลยุทธ์ทางด้าน IT โดยย่อ นั้น องค์กรสามารถขยายผลของการวางแผนที่จะจัดการความเสี่ยงทางด้านกลยุทธ์ (Strategic Risk) ต่อไปได้อีกในประเด็นและมิติต่าง ๆ โดยย่อ ดังนี้

1. การประเมินผลกระทบจากการเปลี่ยนแปลงโครงสร้างองค์กรหรือตำแหน่งที่มีความสำคัญต่อองค์กร

2. การวางแผนกลยุทธ์ และการตัดสินใจต่าง ๆ ที่มีผลกระทบต่อทรัพยากร ระบบการจัดการ การบริหารความเสี่ยง และการกำหนดแผนดำเนินงานที่ดีมารองรับความเสี่ยงที่เกิดจากการวางแผนกลยุทธ์ด้าน IT โดยรวม
3. ผลกระทบจากการตัดสินใจทางด้านกลยุทธ์หรือการเปลี่ยนแปลงจากเหตุการณ์ภายนอกที่มีผลต่อองค์กรโดยรวม
4. การบริหารและการจัดการตามหลักการกำกับดูแลกิจการที่ดีและตาม พรก.ว่าด้วยหลักเกณฑ์และการบริหารกิจการบ้านเมืองที่ดี พ.ศ.2546
5. การสร้างระบบสารสนเทศเพื่อการบริหารและการสร้างระบบ e-Doc (Electronic Department Operation Center) ตามนโยบายของรัฐบาลเพื่อสร้างระบบการบริหารและการจัดการที่ดีจากการจัดการเทคโนโลยีสารสนเทศที่ดี (IT Governance) อย่างเป็นระบบ เป็นรูปธรรม เพราะระบบ e-Doc นี้ต้องส่งต่อไปยังระดับกระทรวง (Mdoc) ซึ่งจะต้องส่งต่อไปยังนายกรัฐมนตรี (Pre-Doc) เพื่อการจัดการในระดับประเทศจากระบบอิเล็กทรอนิกส์ของหน่วยงานต่าง ๆ ซึ่งพิจารณาได้ว่าเป็น e-Government ระดับหนึ่ง

กระบวนการสร้าง IT Governance ซึ่งเป็นระบบการจัดการที่ต้องพึ่งพิงความรู้ทางด้านการจัดการ IT ที่ดี จะทำให้การประสานงานภายในองค์กร การบูรณาการการจัดการในระดับองค์กรและระดับประเทศเป็นไปอย่าง เป็นรูปธรรมโดยมีเป้าหมายที่จะลดต้นทุนและเพิ่มประสิทธิภาพในการดำเนินการ สนองตอบต่อความต้องการของ องค์กรและของรัฐ สร้างแนวทางในการให้บริการ และสร้างรายได้ใหม่ ๆ สร้างรูปแบบใหม่ในการดำเนินธุรกิจของ องค์กร สร้างความสามารถในการแข่งขันและสร้างมูลค่าเพิ่มให้กับองค์กร

### สรุปแง่มุม ของ IT Governance ที่ควบคู่กับ Good Corporate Governance โดยย่อบางประการ

เพื่อสร้างความเข้าใจในการสร้างคุณค่าเพิ่มของ IT Governance จาก IT เพื่อแสดงถึงการสร้างคุณค่า เพิ่มเพื่อบรรลุวัตถุประสงค์จากพันธกิจที่ดีตามหลักของการกำกับดูแลกิจการที่ดี จึงขอเสนอตัวอย่างเพื่อเป็น แนวทางให้เห็นดังต่อไปนี้

1. เป้าหมายขององค์กรตามหลักการกำกับดูแลกิจการที่ดีจะคู่กับกิจกรรมและกระบวนการจัดการ เทคโนโลยีสารสนเทศที่ดี

2. สารสนเทศเพื่อการจัดการและการบริหารเทคโนโลยีสารสนเทศที่ดีซึ่งเป็นสิ่งสำคัญยิ่งในกระบวนการจัดการทางด้านการกำกับดูแลกิจการที่ดีนั้นจะควบคู่ไปกับกระบวนการจัดการทรัพยากรและบุคลากรทางด้าน IT Governance

3. ความสัมพันธ์และการบริการให้กับลูกค้าและสร้างความพึงพอใจให้กับลูกค้าและผู้มีผลประโยชน์ร่วมตามหลักการกำกับดูแลกิจการที่ดีจะควบคู่ไปกับการสื่อสารที่ดีทั้งภายในและภายนอกองค์กรที่สามารถจัดการได้โดยใช้เทคโนโลยีสารสนเทศที่ดี นั่นคือ จะไม่มีช่องว่างในเรื่องเวลา สถานที่ เชื้อชาติ ศาสนา ความมั่งมีหรือความยากจน ลูกค้ารายใหญ่หรือรายย่อย ฯลฯ

### แนวปฏิบัติที่สำคัญของ ITG

การจัดตั้งคณะกรรมการกลยุทธ์ IT (IT Strategy Committee) ถือเป็นแนวปฏิบัติที่ดี

หน้าที่ความรับผิดชอบของคณะกรรมการกลยุทธ์ IT คือ

1. ขยายขอบเขตให้ครอบคลุมถึงการให้คำแนะนำในเรื่องกลยุทธ์เพื่อช่วยเหลือคณะกรรมการในภาวะความรับผิดชอบเรื่อง IT Governance (ITG)
2. มุ่งเน้นในเรื่องมูลค่า/คุณค่าของ IT ความเสี่ยงและผลการดำเนินงาน ทั้งนี้เป็นกลไกในการรวม IT Governance เข้ากับ Enterprise Governance

ในฐานะที่ IT Strategy Committee เป็นคณะกรรมการของคณะกรรมการองค์กร ก็จะทำหน้าที่ช่วยคณะกรรมการในการตรวจตราดูแลงานที่เกี่ยวข้องกับ IT ขององค์กร โดยมีความมั่นใจได้ว่าคณะกรรมการมีข้อมูลทั้งภายนอกและภายใน องค์กรที่จำเป็นสำหรับการตัดสินใจเรื่อง IT Governance อย่างมีประสิทธิภาพ นี่คือการบูรณาการการบริหารเพื่อบรรลุถึงวิสัยทัศน์ นโยบาย และเป้าหมายของประเทศ

### การกำกับดูแลกิจการที่ดีด้าน IT ต้องการแนวทางการตัดสินใจที่ชัดเจน

ITG เป็นการมอบอำนาจการตัดสินใจและความรับผิดชอบที่จะมั่นใจได้ว่ามีพฤติกรรมการใช้ IT เป็นไปตามที่พึงประสงค์ ดังนั้นจำเป็นต้องมีแนวทางที่ชัดเจนในการคัดเลือกผู้ที่จะทำหน้าที่ตัดสินใจ

ITG ที่มีประสิทธิภาพเป็นตัวกำหนดความสำเร็จขององค์กรด้าน Information System เป็นเบื้องต้น การกำกับดูแลประกอบด้วยการมอบหมายสิทธิในการตัดสินใจและความรับผิดชอบ โดยคำนึงถึงพฤติกรรมการใช้ IT เป็นไปตามที่พึงประสงค์จะมอบหมาย “สิทธิในการตัดสินใจ” ภายในองค์กรได้อย่างไร มีแนวทางดังนี้

### 1. กำหนดอำนาจในการตัดสินใจให้สอดคล้องไปในแนวเดียวกับวัฒนธรรมองค์กร

ทุก ๆ องค์กรย่อมมีวัฒนธรรมองค์กรของตน ซึ่งเป็นกฎเกณฑ์ที่ไม่เป็นทางการใช้กำหนดวิธีการดำเนินงานในองค์กรและประเภทของพฤติกรรมที่ยอมรับได้ เพื่อที่จะก่อให้เกิดประสิทธิผลสูงสุดต่อ ITG กลไกที่นำมาใช้จะต้องสะท้อนและสนับสนุนวัฒนธรรมที่เหนือกว่าในองค์กรที่มีสายการบังคับบัญชาตามลำดับที่เน้นการสั่งการและการควบคุมกลไกในการกำกับดูแลควรจะสะท้อนโครงสร้างขององค์กรผ่านการตัดสินใจ องค์กรที่ชื่นชอบความสอดคล้องกันควรจัดตั้งคณะกรรมการเฉพาะกิจ (Steering Committee) ต่าง ๆ สภาและคณะบุคคล โครงสร้างที่มีความร่วมมือกันเหล่านี้จะส่งเสริมสนับสนุนลักษณะทางที่มีความร่วมมือกันอยู่ทางวัฒนธรรมองค์กร

### 2. ทำให้มั่นใจได้ว่าอำนาจในการตัดสินใจมีพร้อมแล้ว ซึ่งความรู้ความเข้าใจที่จำเป็นสำหรับกระบวนการตัดสินใจ

ขอบเขตของการตัดสินใจเรื่อง ITG มีกว้างมาก ตั้งแต่สถาปัตยกรรมทางเทคนิคไปจนถึงการจัดลำดับความสำคัญของโครงการและการจัดหาเงินทุน การตัดสินใจต้องเกิดขึ้นโดยเป็นส่วนหนึ่งของการบวนการที่ระบุบทบาทและความรับผิดชอบอย่างชัดเจน การละเว้นความรับผิดชอบในกระบวนการตัดสินใจจะนำไปสู่การตัดสินใจที่ไว้วินัยของบุคคลใดก็ตามที่มีอิทธิพลทางการเมืองพอ ซึ่งแน่นอนไม่ใช่ทางออกที่ดีที่สุดเพื่อมีการมอบหมายอำนาจการตัดสินใจ ให้เริ่มต้นที่

#### 2.1. แจ้งอย่างชัดเจนว่าดำเนินงานต้องให้การตัดสินใจ

กำหนดขั้นตอนที่ต้องดำเนินการให้ไปสู่การตัดสินใจ ใครควรเป็นผู้ให้ข้อมูล และจะต้องมีกิจกรรมอะไรบ้างที่จะทำให้ได้มาซึ่งข้อมูลหนึ่ง

กำหนดตัวบุคคลที่จะทำการตัดสินใจ โดยต้องมั่นใจว่าผู้ที่ตัดสินใจได้รับข้อมูลที่ถูกต้องเป็นจริงต่อการตัดสินใจ

### 3. ให้มั่นใจว่าผู้ที่ทำการตัดสินใจมีข้อมูลที่จำเป็นอย่างเพียงพอ

ITG ไม่ใช่เป็นขององค์กรทาง Information System แต่เพียงผู้เดียว ความรับผิดชอบในการตัดสินใจได้ถูกแบ่งกระจายไปในกลุ่มของผู้ที่มีส่วนได้เสีย เช่น ผู้บริหารอาวุโสของกิจการ ผู้นำหน่วยงานและ

หน้าทำงานทางธุรกิจ คณะผู้บริหารระบบสารสนเทศและลูกค้าภายในที่จ่ายค่าบริการให้ฝ่ายระบบสารสนเทศในกิจการส่วนมากกลุ่มผู้มีส่วนได้เสีย แต่ละกลุ่มมักจะมีความเห็นเกี่ยวกับบทบาทขององค์กรทาง Information System อย่างไรก็ดีมันเป็นอันตรายที่จะกำหนดเค้าโครงและสื่อสารอย่างชัดเจนให้เห็นถึงบทบาทของแต่ละกลุ่มในกระบวนการตัดสินใจในหลาย ๆ กรณี ผู้มีส่วนได้เสียบางคนอาจถูกร้องขอให้จัดหาข้อมูลสำหรับการตัดสินใจ แต่อำนาจหน้าที่และความรับผิดชอบในการตัดสินใจมีกระจายอยู่ทั่วไป ดังตัวอย่างทั้งสองดังนี้

#### ตัวอย่างที่ 1

องค์กรที่เป็นเลิศบางแห่ง (กระตือรือร้น และนำเทคโนโลยีมาปรับใช้งานอย่างรวดเร็ว) มีคณะเทคโนโลยีที่ขยันขันแข็ง พร้อมทั้งจะแสดงและหารือเรื่องเกี่ยวกับเทคโนโลยีสมัยใหม่ที่สามารถนำมาปรับใช้แก้ปัญหาปัจจุบันของธุรกิจได้ คณะบุคคลเหล่านี้มักประกอบด้วยสถาปนิกทางเทคนิคระดับอาวุโส และผู้แทนจากกลุ่มลูกค้าคณะเทคโนโลยีจะให้ข้อมูลแก่หัวหน้าคณะเจ้าหน้าที่ทางเทคนิคหรือผู้ที่รับผิดชอบทำหน้าที่ตัดสินใจทางสถาปัตยกรรม แต่สมาชิกในคณะไม่ได้สั่งการหรือตัดสินใจกำหนดทิศทางด้านเทคนิคขององค์กร

#### ตัวอย่างที่ 2

คณะบุคคลทางธุรกิจถูกจัดตั้งขึ้นมาเพื่อแบ่งปันแนวปฏิบัติที่ดีสำหรับกระบวนการทางธุรกิจ โดยเฉพาะ ตัวอย่างเช่น Supply Chain และความสามารถในการนำเทคโนโลยีมาปรับใช้งาน คณะบุคคลทางธุรกิจ Supply Chain เหล่านี้มีหน้าที่รับผิดชอบในการวางแผนภูมิ เพื่อกำหนดทิศทางการนำ ERP มาใช้งานในองค์กร เมื่อจำเป็นต้องยกระดับและอนุญาตให้มีการปรับเปลี่ยนให้เหมาะสมกับลูกค้าและองค์กรทาง Information System ก็จะให้ข้อมูลแก่คณะบุคคล เช่น ต้นทุนและความเสี่ยงของทางเลือกต่าง ๆ แต่สภา-คณะบุคคลก็ยังคงไว้ซึ่งสิทธิในการทำการตัดสินใจ

เมื่อมีการมอบหมายสิทธิในการตัดสินใจจะต้องมั่นใจว่ามีความรับผิดชอบและสำนึกในความรับผิดชอบต่อการตัดสินใจนั้นมีความชัดเจน และผู้ที่ต้องการข้อมูลได้ตระหนักถึงบทบาทของตนเอง หากผู้มีส่วนได้เสียกลุ่มใดกลุ่มหนึ่งต้องการเพียงได้รับแจ้งสิ่งที่เกี่ยวข้องกับการตัดสินใจนั้นคือ หากไม่ต้องการข้อมูลนำเข้า ก็จะต้องมีการสื่อสารให้ทราบอย่างชัดเจน

#### 4. กำหนดอำนาจในการตัดสินใจให้สอดคล้องไปในแนวเดียวกับการปรับตัวทางธุรกิจ

ธุรกิจนำกลยุทธ์ต่าง ๆ มาใช้งานหลาย ๆ ทาง เริ่มตั้งแต่องค์กรที่มุ่งเน้นอย่างจริงจังในปรัชญา “บริษัทหนึ่งเดียว” ซึ่งให้คุณค่าแก่หน่วยธุรกิจต่าง ๆ ไปจนถึงความเป็นอิสระของหน่วยงานทางธุรกิจ และกำไร-ขาดทุนของหน่วยงานทางธุรกิจถูกตีราคาสำหรับ ITG จะมีประสิทธิผลเมื่ออำนาจในการตัดสินใจจะต้องสอดคล้องกับการปรับตัวทางธุรกิจขององค์กรที่มีหน่วยงานทางธุรกิจต่าง ๆ เป็นอิสระจากกันสูง ผู้นำของหน่วยงานทางธุรกิจควรมี ITG ฝังอยู่ในอำนาจการตัดสินใจที่มีอยู่ในมือ ไม่ใช่ไปกำหนดให้อยู่กับ Steering Committee ขององค์กรที่มีแนวคิดแบบ “บริษัทหนึ่งเดียว” หรือแบบรวมศูนย์จะพบว่าการตัดสินใจแบบรวมศูนย์เป็นเครื่องมือที่มีค่าในการคานอำนาจ

บทสรุป การมอบหมายสิทธิการตัดสินใจใน ITG เป็นงานที่ซับซ้อนที่ได้รับอิทธิพลจากวัฒนธรรมขององค์กร การปรับตัวทางธุรกิจ ความคิดเห็นของผู้มีส่วนได้เสียและความรู้ที่จำเป็นสำหรับผู้ทำหน้าที่ตัดสินใจ แนวทางนี้สามารถนำไปใช้เพื่อให้องค์กรมีโอกาสประสบความสำเร็จทางด้าน ITG ได้สูงที่สุด

จากบทความ : *IT Governance Requires Decision-Making Guidelines* โดย S.Dallas บริษัท Gartner

## การพัฒนาความคิดเพื่อการกำกับและดูแลกิจการที่ดี

การกำกับดูแลกิจการที่ดี หรือ Good Corporate Governance เป็นนามธรรมที่จำเป็นอย่างยิ่งที่ผู้เกี่ยวข้องทุกฝ่ายในองค์กร โดยเฉพาะผู้บริหารระดับสูงต้องพัฒนานำไปสู่การปฏิบัติอย่างเป็นรูปธรรม ซึ่งต้องอาศัยความคิด ความรู้ ความเข้าใจ ความมุ่งมั่น ความเสียสละ และการมีคุณธรรมที่ถูกต้อง เพื่อความสำเร็จขององค์กรให้เป็นที่ยอมรับจากผู้มีผลประโยชน์ร่วม (Stakeholders) ของทุกองค์กรทุกระดับ โดยการทำความเข้าใจกับกิจกรรมหลัก ๆ ที่มีผลต่อวัตถุประสงค์และเป้าหมาย ทั้งในระดับองค์กรและในระดับของสายงานต่าง ๆ เพื่อกำหนดจุดควบคุม การบริหารความเสี่ยง การตรวจสอบภายในโดยใช้ฐานความเสี่ยง โดยมีเกณฑ์ มาตรฐาน อันเป็นที่ยอมรับทั่วไป

ในสถานการณ์ที่นวัตกรรมทางการเงิน การบริหาร การปฏิบัติงาน การตรวจสอบเทคโนโลยีสารสนเทศ และความรู้ต่าง ๆ ได้พัฒนาไปอย่างรวดเร็วในปัจจุบัน การปรับตัวขององค์กรและพนักงานระดับต่าง ๆ เป็นความจำเป็น โดยไม่ยึดติดกับกรอบความคิดหรือวิธีการทำงานแบบเดิม ๆ องค์กรโดยเฉพาะฝ่ายบริหารต้องพร้อมที่จะก้าวไปในมิติใหม่ที่มีการค้นคว้าและยอมรับว่าเป็นผลดีอย่างยิ่งในการดำเนินงานให้สำเร็จตามเป้าหมายอย่างยั่งยืน โดยไม่จำเป็นต้องลองผิดลองถูกอย่างไม่มั่นใจ เพราะ Good Corporate Governance มีการค้นคว้าและนำไปปฏิบัติอย่างได้ผลดีในองค์กรต่างๆ ของหลายประเทศแล้ว

**จุดที่มีความสำคัญอย่างยิ่งในการพัฒนาองค์กรและบุคลากรขององค์กร เพื่อก้าวไปสู่การกำกับดูแลกิจการที่ดีบางประการ ก็คือ**

1. การเปิดใจกว้างเพื่อยอมรับการเปลี่ยนแปลง
2. ปรับตัวให้เข้ากับการเปลี่ยนแปลง และก้าวไปข้างหน้าอย่างรวดเร็วอย่างมั่นใจ
3. การรับมือกับการเปลี่ยนแปลงที่เกิดขึ้นแล้วและที่จะเกิดขึ้นในอนาคตนั้น หากยังไม่แน่ใจเรื่อง การวิเคราะห์ความเสี่ยงกับการเปลี่ยนแปลงดีพอ สิ่งที่ต้องพิจารณาก็คือ
  - 3.1. ต้องเข้าใจที่จะทำให้องค์กรมีความเรียบง่ายในทางราบและมีความยืดหยุ่นในการปรับตัวสูงตามกลยุทธ์ที่เหมาะสม
  - 3.2. ไม่ยึดติดกับความคุ้นเคยที่ปฏิบัติกันมานานจนไม่กล้าที่จะมีการเปลี่ยนแปลง ทั้ง ๆ ที่สิ่งแวดล้อมรอบข้างได้เปลี่ยนไปมากมายแล้ว
  - 3.3. ฝึกการเป็นผู้ช่างสังเกตหรือรับรู้ถึงการเปลี่ยนแปลงที่จะมีผลกระทบต่อการบริหาร และการพัฒนาความรู้ของพนักงาน เพื่อช่วยให้เราบริหารและจัดการกับความเสี่ยงระดับต่าง ๆ ได้โดยไม่อาศัยบุญเก่า

3.4. การพัฒนาความคิดและมีความมุ่งมั่นอย่างถูกต้องในการก้าวไปสู่การปฏิบัติ การปรับปรุงองค์กรและปรับปรุงวิธีการทำงานใหม่ ๆ ต้องกระทำการอย่างรวดเร็วและทันการณ์จึงจะมีประโยชน์ โดยหมั่นสอบถามและประเมินตนเองอย่างเสมอว่า

- 1) เหตุการณ์หรือการกระทำใด ๆ ทั้งโดยระบบงานหรือบุคคล อาจเกิดปัญหาหรือข้อผิดพลาดใดขึ้นได้บ้าง?
- 2) กระบวนการบริหารงาน การปฏิบัติงานที่ถูกต้องในปัจจุบันและอนาคต ควรเป็นเช่นใด?

3.5. องค์กรและ/หรือตัวเราเท่านั้นที่จะเป็นผู้ผลักดันให้เกิดการเปลี่ยนแปลงในทางสร้างสรรค์ของการทำงานอย่างมีประสิทธิภาพและมีประสิทธิผล

3.6. มีรางวัลรออยู่เสมอ เพียงแต่เราตัดสินใจอย่างมุ่งมั่นที่จะแสวงหาโดยการบริหารความคิดและการปฏิบัติงานอย่างเป็นระบบ และใช้ “ระบบงาน” คุณคน มากกว่าให้ “คน” คุณระบบงาน

ในประเด็นของเรื่อง “ระบบงาน” กับ “บุคลากร” นั้น มีผู้กล่าวไว้น่าสนใจว่า...

ระบบดี	คนดี	นั่นดีแน่
ระบบดี	คนแย่	พอแก้ไข
ระบบแย่	คนดี	มีทางไป
ระบบแย่	คนไม่เอาไหน	บรรลยเอย

อย่างไรก็ดี ระบบงานที่ดีและคนที่ดีมีความสามารถ โดยไม่มีการพัฒนาให้เหมาะสมตามการเปลี่ยนแปลงของเทคโนโลยี และการบริหารการเปลี่ยนแปลงในเวลาที่เหมาะสมนั้น ยังไม่ปรากฏในโลกของการบริหารและการกำกับดูแลกิจการที่ดีในปัจจุบัน

3.7. การยอมรับการเปลี่ยนแปลง แทนการต่อต้านการเปลี่ยนแปลงใด ๆ จะนำองค์กรและตัวเราไปสู่วิธีคิดและวิธีการทำงานแบบใหม่ที่จะนำสิ่งดี ๆ มาสู่องค์กรและผู้ปฏิบัติงานอย่างมั่นใจ

3.8. ความยั่งยืนขององค์กร ชีวิตการทำงาน และความเป็นอยู่ในการดำรงชีพภายใต้โลกของการเปลี่ยนแปลงจะดำเนินไปไม่ได้ถ้าทุกองค์กรไม่เร่งปรับตัวเพื่อความอยู่รอดและพัฒนาตนเองเพื่อเพิ่มขีดความสามารถในการแข่งขัน ทุกหน่วยงานจึงต้องการองค์กรและพนักงานที่มีความยืดหยุ่น ถึงจะปรับตัวให้เข้ากับการกำกับดูแลกิจการที่ดีกับการเปลี่ยนแปลงได้เสมอ

**ความตั้งใจจริงนำไปสู่ความคิดเชิงกลยุทธ์ และนำไปสู่การปฏิบัติอย่างเป็นรูปธรรมของกระบวนการจัดการ และการแก้ไขปัญหาที่ดี มีข้อสังเกตบางประการที่ควรพิจารณา ก็คือ**

1. แนวความคิดที่นำไปสู่การเปลี่ยนแปลงการบริหารงาน การปฏิบัติงาน ไม่ว่าจะเป็กรณิปกติหรือกรณิที่ประเทศหรือองค์กรมีปัญหา จากปัจจัยทั้งภายนอกและ/หรือปัจจัยภายใน ทั้งในระดับประเทศและระดับองค์กร มีมุมมองได้หลายด้าน และปัจจัยต่าง ๆ มีผลกระทบทั้งทางด้านบวกและด้านลบเพื่อมองต่างมุมเสมอ
2. อันตรายที่ร้ายแรงที่สุดในการปฏิบัติงาน การบริหาร ก็คือการปฏิบัติงานตาม ๆ กันไปด้วยความเคยชิน โดยไม่คำนึงถึงผลกระทบในทางลบต่าง ๆ ในทุกระดับของการจัดการจากการเปลี่ยนแปลงหรือความเสี่ยงที่เกิดขึ้น เช่น บางหน่วยงานของรัฐมีระเบียบ กฎเกณฑ์ คำสั่งต่าง ๆ ที่ไม่เคยเปลี่ยนแปลงมากกว่า 30 ปี เป็นต้น
3. ดังนั้นกลยุทธ์ของการบริหารโดยเริ่มต้นที่แนวความคิดในเชิงป้องกันหรือเชิงรุกอย่างมีระบบ จะเป็นการบริหารและการปฏิบัติงานแบบยั่งยืนที่แท้จริง ทั้งนี้ ไม่จำกัดความคิดอยู่ที่ผู้บริหารระดับสูงเท่านั้น แต่จะมีประโยชน์อย่างยิ่งต่อประเทศ ต่อองค์กร หากบุคลากรที่เกี่ยวข้องจะมีส่วนร่วมด้วยช่วยกันคิดและมีการสื่อสารและช่วยกันสร้างมูลค่าเพิ่มจากความคิดทุกระดับอย่างสร้างสรรค์ มุ่งมั่น ทุ่มเท ติดตามผลอย่างจริงจังจากระดับบนสู่ระดับล่าง จากระดับล่างสู่ระดับบน และระดับราบระหว่างหน่วยงาน เพื่อนำไปสู่การปฏิบัติงานที่วัดได้ และตรวจสอบได้
4. ผู้บริหารระดับสูงหลายหน่วยงาน โดยเฉพาะหน่วยงานของรัฐ และรัฐวิสาหกิจบางหน่วยงาน มีผู้บริหารที่มีความสามารถมาก แต่ในทางปฏิบัติหลายท่านมีความคิดดี ๆ แต่ไม่อาจสานต่อไปสู่การปฏิบัติที่เป็นรูปธรรมได้ เพราะใช้เวลาส่วนใหญ่ไปในการประชุมต่าง ๆ ประจำวันภายในองค์กร และภายนอกองค์กรตามที่กำหนดไว้ในระเบียบข้อบังคับต่าง ๆ ที่ปฏิบัติ ทำให้มีปัญหาอื่น ๆ ตามมา นั่นคือก้าวไม่ทันกับการเปลี่ยนแปลงซึ่งน่าจะเป็นปัญหาสำคัญพื้นฐานของการนำองค์กรหรือหน่วยงานในสังกัดก้าวไปสู่การกำกับดูแลกิจการที่ดีได้

#### การพัฒนาความคิดเพื่อการบริหารและการจัดการที่ดีและนำไปสู่การสร้างมูลค่าเพิ่ม 10 ประการ

1. การปรับปรุงและการพัฒนาการบริหารงานจากการเปลี่ยนแปลงทุกรูปแบบ หรือการบริหารความเสี่ยงนั้น ต้องกระทำตลอดเวลา เพราะไม่มีจุดสิ้นสุดของโลกแห่งการเปลี่ยนแปลง
2. ควรศึกษา แสวงหาความรู้ทุกรูปแบบที่จำเป็นจากแหล่งต่าง ๆ เพื่อประเมินถึงผลกระทบ และเพื่อการปรับปรุงการบริหารงานไปสู่วัตถุประสงค์และเป้าหมายของประเทศหรือองค์กรอย่างยั่งยืน

3. อย่ายึดติดกับความคิดและการปฏิบัติเดิม ๆ โดยไม่คำนึงถึงความพึงพอใจของผู้มีผลประโยชน์ร่วมที่เกี่ยวข้องของโลกแห่งการเปลี่ยนแปลง
4. ควรคิดและตระหนักเสมอว่ายังมีวิธีการที่นำไปสู่เป้าหมายและวัตถุประสงค์เสมอ
5. ไม่มีคำตอบสำหรับความผิดพลาดที่เกิดขึ้นหรืออาจจะเกิดขึ้น
6. หากมีปัญหเกิดขึ้นและต้องการคำตอบและการดำเนินการที่ถูกต้องแล้ว ให้หาวิธีการที่ง่ายและสะดวกที่พบบรรเทาปัญหานั้น ๆ โดยไม่ต้องมุ่งมั่นถือการแก้ไขปัญหาที่สมบูรณ์แบบที่สุด เพราะอาจไม่มีวิธีการที่ว่่านั้น
7. หากประเทศหรือองค์กรหรือแม้แต่ตัวของเราเอง ได้รับประสบการณ์จากความล้มเหลวในการดำเนินการหรือปฏิบัติการใด ๆ ในอดีต ก็ควรวิเคราะห์สาเหตุของปัญหาและข้อผิดพลาดที่เกิดขึ้น และต้องหาวิธีการไม่ให้ความผิดพลาดนั้น หรือทำนองคล้าย ๆ กันเกิดขึ้นอีกเป็นอันตราย และควรหาวิธีการเพื่อข้อผิดพลาดและทำเป็นกรณีศึกษาที่เป็นลายลักษณ์อักษร ให้เป็นบทเรียนของประเทศหรือผู้ที่เกี่ยวข้องทุกฝ่าย
8. ใช้ความคิดเชิงกลยุทธ์ในการบริหารเชิงรุก ในแง่มุมต่างๆ ของการจัดการกับความเสียหายอย่างฉลาด จะได้ผลว่าการใช้เงินอย่างเดียวในการพัฒนาหรือแก้ไข้ปัญหา เพราะอาจเป็นความสูญเปล่า การวิเคราะห์ที่จุดอ่อน จุดแข็ง ซึ่งเป็นสถานภาพภายในประเทศหรือขององค์กรเองที่แก้ไขได้ ปรับปรุงได้ พัฒนาได้ กับการวิเคราะห์โอกาสและอุปสรรค ซึ่งเป็นปัจจัยภายนอกองค์กรที่ไม่อาจควบคุมได้ จะมีประโยชน์ต่อการบริหารความเสี่ยงต่าง ๆ ที่จะเกิดความเสียหายได้
9. วิฤติหรือปัญหาต่าง ๆ อาจสร้างโอกาสและรางวัลต่อเราได้ แต่แนวความคิดของการบริหารที่ไม่ถูกต้องกับสถานการณ์อาจสร้างวังวนของปัญหาในระดับต่าง ๆ ได้
10. หากประเทศหรือองค์กรหรือตัวเราเองเผชิญอุปสรรค ให้หมั่นตั้งคำถามบ่อย ๆ ว่า ทำไมปัญหาจึงเกิดขึ้น และควรระดมความคิดที่ว่าเราจะแก้ไข้รวมทั้งป้องกันและบริหารเชิงรุกได้อย่างไร เพื่อการฟื้นฟูและทำให้เกิดการพัฒนาที่ยั่งยืน โดยมีบทเรียนต่าง ๆ ในอดีตเป็นเรื่องเตือนความจำไม่ให้เกิดความผิดพลาดซ้ำได้อีก และมีอนาคตของการบรรลุเป้าหมายอย่างยั่งยืนเป็นธงชัย ด้วยวิธีการกำกับดูแลกิจการที่ดีซึ่งประกอบไปด้วย การ

บริหารความเสี่ยง การควบคุมภายใน การตรวจสอบภายในที่มีมาตรฐาน จากผู้บริหารและผู้เกี่ยวข้องที่มีคุณธรรมทุกระดับของการดำเนินงาน

## สรุป

ถึงแม้ความคิดจะควบคุมเป็นรูปธรรมไม่ได้ แต่การตรวจสอบความคิดเชิงกลยุทธ์เพื่อการบริหารและการจัดการที่ดีสามารถดำเนินการได้ด้วยการใช้ความคิดเชิงกลยุทธ์เช่นกัน

- เราช่วยกันคิด ช่วยกันทำ โดยการบริหารความคิดเพื่อนำไปสู่การปฏิบัติอย่างมีกลยุทธ์และเป็นรูปธรรมในวันนี้ เพื่ออนาคตที่รุ่งเรืองของประเทศและขององค์กรแล้วหรือยัง
- เรามีการประเมินความคิดที่จะนำไปสู่รูปธรรมที่เหมาะสมอย่างได้ผลที่วัดได้เมื่อถึงเวลาที่กำหนดแล้วหรือยัง? ทั้งนี้ อาจมีการทดสอบความคิดง่าย ๆ โดยตั้งคำถามพื้นฐานของผู้บริหารระดับสูงขององค์กรว่า
- องค์กรของเรามีการปรับโครงสร้าง วิธีการทำงานให้เหมาะสมกับการเปลี่ยนแปลงทางกลยุทธ์ (Strategic) ที่สอดคล้อง Strategic Thinking ที่เหมาะสมเมื่อใด
- เราได้ตระหนักแล้วหรือยังว่า การทำธุรกิจ การผลิต การค้า การบริการ การเงิน การบริหาร ฯลฯ ความสามารถนั้นวัดกันที่ความคิดในการบริหารความเสี่ยง และการมีคุณธรรมที่จะนำไปสู่การปฏิบัติอย่างได้ผลต่อวัตถุประสงค์และเป้าหมายอย่างยั่งยืนเป็นสำคัญ
- การพัฒนาความคิดที่ถูกต้องอย่างมีขั้นตอนและเป็นระบบซึ่งประกอบไปด้วยคน เทคโนโลยี และกระบวนการควบคุมภายในและการปฏิบัติงาน จะนำไปสู่ขนาดของความสำเร็จและความก้าวหน้าขององค์กรและประเทศชาติที่วัดได้
- การฝึกใจเป็นนิสัยเพื่อคิดอย่างมีระบบ และปฏิบัติได้จริงให้ทันการเปลี่ยนแปลง เพื่อความก้าวหน้าของประเทศและองค์กร จะช่วยเพิ่มศักยภาพในการทำงานได้ทุกระดับ
- ความเชื่อมั่น ความทุ่มเท ความมุ่งมั่น ความกล้าหาญ ความดีงาม ความเสียสละ ความมีคุณธรรม คู่กันไปกับการพัฒนาความคิดเป็นสิ่งจำเป็นในการกำกับดูแลกิจการที่ดี ซึ่งเป็นแม่บทของการบริหารความเสี่ยง กระบวนการควบคุมภายใน และการตรวจสอบภายในอย่างมีคุณภาพ

## ความเสี่ยงของการจัดการงานตรวจสอบภายใน กับ IT GOVERNANCE

The Internal Auditing Standards Board ได้ทำการทบทวนมาตรฐานสำหรับเป็นแนวทางปฏิบัติในการประกอบวิชาชีพการตรวจสอบภายใน (Standards for the Professional Practice of Internal Auditing) โดยจะเริ่มใช้เป็นทางการในวันที่ 1 มกราคม 2545 ซึ่งมีการเปลี่ยนแปลงมาตรฐานและปรับเปลี่ยนมาตรฐานการปฏิบัติงานตรวจสอบภายในที่ใช้กันอยู่ในปัจจุบัน (Red Book) เสียใหม่ เพื่อให้สอดคล้องกับกรอบการปฏิบัติงาน (Professional Practices Framework) และสอดคล้องกับนิยามใหม่ของการตรวจสอบภายใน เพื่อให้เกิดความกระจ่างชัดเจนในหลาย ๆ หัวข้อที่เกี่ยวข้อง

มาตรฐานการปฏิบัติงานดังกล่าว ได้ช่วยขยายความหมายตามมาตรฐาน (Standards) ให้เป็นที่เข้าใจมากขึ้น ทั้งในลักษณะงานการตรวจสอบภายในทั่วไป และบางส่วนอาจนำมาประยุกต์ใช้กับธุรกิจเฉพาะทางได้ ทั้งนี้บทความนี้จะให้ข้อสังเกตเฉพาะมาตรฐานเกี่ยวกับการประสานงานการตรวจสอบเท่านั้น

### มาตรฐานการจัดการงานตรวจสอบภายในใหม่<sup>7</sup>

ได้กล่าวถึงเรื่องประสิทธิภาพในการจัดการงานตรวจสอบภายในเพื่อให้เกิดประโยชน์สูงสุดต่อองค์กร ในเรื่อง

1. การวางแผนการตรวจสอบตามลำดับความสำคัญและความเสียหายจากความเสียหาย
2. การสื่อสารและการอนุมัติ
3. การจัดทรัพยากรการตรวจสอบ
4. นโยบายและขั้นตอนการปฏิบัติงานตรวจสอบ
5. การร่วมมือ การประสานงาน โดยการแลกเปลี่ยนข้อมูลและการร่วมมือกับผู้ตรวจสอบภายในและภายนอกอื่น ๆ ผู้เชี่ยวชาญจากภายในและภายนอกองค์กรที่ให้คำปรึกษาในงานการตรวจสอบที่เกี่ยวข้อง เพื่อให้เกิดความมั่นใจว่า ขอบเขตของงานที่ปฏิบัติครอบคลุมทุกจุดอย่างเหมาะสม และเพื่อป้องกันการดำเนินงานที่ซ้ำซ้อน
6. การรายงานคณะกรรมการบริหารและผู้บริหารระดับสูง ทั้งนี้ให้รวมถึงความเสี่ยงที่จะทำให้องค์กรเกิดความเสียหายในการปฏิบัติงานตามหลักการกำกับดูแลกิจการที่ดีที่จะมีผลเสียหายต่อเป้าหมายและวัตถุประสงค์ขององค์กรในระดับต่าง ๆ

<sup>7</sup> ไม่ได้เป็นการแปลโดยตรงจากมาตรฐานใหม่... แต่เป็นการยกประเด็นที่น่าสนใจและขยายความเพื่อเป็นข้อคิด และพิจารณาความเสี่ยงที่อาจเกิดขึ้นในการปฏิบัติงานตามมาตรฐานข้อนี้ ซึ่งจะส่งผลกระทบต่อประสิทธิภาพและประสิทธิผลของการตรวจสอบ รวมทั้ง Performance Standards โดยทั่วไปด้วย

## การตรวจสอบองค์กรที่ใช้คอมพิวเตอร์กับมาตรฐานการจัดการงานตรวจสอบภายใน

ในการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์ ซึ่งหมายถึงทุกองค์กรที่มีการใช้เทคโนโลยีสารสนเทศ (Information Technology - IT) เข้าช่วยในการประมวลผลข้อมูลในทุกๆระดับ โดยเฉพาะอย่างยิ่งองค์กรที่ใช้เทคโนโลยีและมีระบบงานที่ซับซ้อนนั้น มักจะมีการแบ่งแยกงานตามทักษะ ประสบการณ์และความรู้ของผู้ตรวจสอบภายใน และหลาย ๆ กรณีก็มีการใช้บริการผู้เชี่ยวชาญจากภายนอกมาปฏิบัติงานตรวจสอบด้าน Information Technology (IT/IS) และด้านอื่น ๆ ในการปฏิบัติงานเพื่อให้บรรลุเป้าหมายด้วย ไม่ว่าจะใช้บริการผู้เชี่ยวชาญจากภายในองค์กร หรือผู้เชี่ยวชาญจากภายนอกองค์กร ผมก็มีข้อสังเกตจากประสบการณ์ที่ผ่านมา โดยจะกล่าวถึงผลกระทบของ Technology ต่อการบรรลุเป้าหมายตามมาตรฐานการจัดการงานตรวจสอบภายใน เฉพาะข้อ 5. ที่เกี่ยวกับงาน IT Audit บางประการดังนี้

1. ผู้เชี่ยวชาญเฉพาะทาง เช่น IT Auditors มีความรู้ด้านการตรวจสอบ IT/IS แต่บางท่านอาจไม่มีความรู้ทางด้านผลกระทบที่เกี่ยวข้องอย่างสำคัญต่อการบรรลุเป้าหมายการตรวจสอบภายในภาพใหญ่ที่เข้าถึงวัตถุประสงค์หลักของการตรวจสอบภายใน องค์กรบางแห่งจะได้รับข้อสังเกต หรือข้อแนะนำว่า Logical Security, Operational Security, Physical Security และอาจรวมทั้งความเสี่ยงทางด้าน General Control และ Application Control หรือ IT Governance มีปัญหา หรือจุดอ่อน รวมทั้งความเสี่ยงที่อาจเกิดความเสียหายที่ควรแก้ไขปรับปรุงอย่างไร ซึ่งจะขึ้นกับขอบเขตของการตรวจสอบ IT

2. ผู้เชี่ยวชาญเฉพาะทางบางรายอาจไม่สามารถดึงประเด็นของปัญหาทาง Technology ให้มีผลต่อเนืองกับวัตถุประสงค์เป้าหมายของการกำกับดูแลกิจการที่ดีในภาพรวมขององค์กรได้ ถึงแม้โดยหลักการจะมีมาตรฐานทางด้าน IT Governance ที่มีการวิเคราะห์ความเสี่ยงนานาประการของ IT ก็ตาม แต่การดึงประเด็นของ IT Governance มาสู่หลักการบริหารความเสี่ยง การควบคุม และการตรวจสอบ ตามมาตรฐานสากลภายใต้กรอบใหม่ของการกำกับดูแลกิจการที่ดีนั้น ยังน่าจะมีปัญหาอยู่ในหลายองค์กรทั้งนี้เพราะเป้าหมายของผู้เชี่ยวชาญที่องค์กรว่าจ้างอาจไม่สัมพันธ์กับเป้าหมายของผู้รับผิดชอบในการปฏิบัติงานตรวจสอบภายใน หรือขององค์กรในภาพรวมอย่างแท้จริง

3. ผู้รับผิดชอบในการปฏิบัติงานตามมาตรฐานการปฏิบัติงานตรวจสอบภายในเองก็อาจเกิดปัญหาความเข้าใจที่แตกต่างกับผลกระทบของ Information Technology Governance (ITG) ต่อระบบการบริหาร

การควบคุมภายในและการปฏิบัติงาน เพราะความเข้าใจของ Business Enabler กับ IT Enabler นั้นมีความสัมพันธ์อย่างใกล้ชิด และแยกกันแทบไม่ได้กับการกำกับดูแลกิจการที่ดี ในภาพรวมขององค์กร และระหว่างองค์กรทั้งระดับภายในและระหว่างประเทศ

4. ความเสี่ยงจากการประสานงานระหว่างผู้เชี่ยวชาญต่าง ๆ ทั้งภายในองค์กรและภายนอกองค์กร ในการปฏิบัติงานร่วมกันโดยสรุปก็คือ Audit Risk และ Co-ordination Risk รวมทั้ง Managing the Internal Audit Risk ซึ่งมีผลกระทบโดยรวมและโดยตรงต่อ Performance Standards อย่างสำคัญได้

ทั้งนี้ เพราะเป้าหมายของผู้เกี่ยวข้องในการปฏิบัติงานจะต้องมีการนำมาสรุป และรวบรวมเป็น องค์กรรวม (Holistic) หนึ่งเดียวให้เป็นที่ไปตามวัตถุประสงค์หลัก ซึ่งเป็นหน้าที่และความรับผิดชอบของผู้บริหารงานตรวจสอบภายในและเกี่ยวข้องกับผู้บริหารระดับสูงรวมทั้งคณะกรรมการขององค์กรอยู่ดี

### ความเข้าใจทางด้านผลกระทบของ IT มีความสำคัญต่อผู้ตรวจสอบและผู้บริหารองค์กร

ขออธิบายด้วยรูปภาพประกอบการอธิบายผลกระทบของ IT ต่อวัตถุประสงค์การตรวจสอบภายในทั้ง 3 ประการ และเกี่ยวเนื่องอีกทั้งโยงใยกับองค์ประกอบของการควบคุมภายในสากล 5 ประการ ทั้งนี้มูลค่าเพิ่มของการดูภาพประกอบต้องใช้จินตทัศน์ถึงความเกี่ยวเนื่องกับมาตรฐานการปฏิบัติงานตรวจสอบภายในหลายประการที่ไม่อาจใช้ตัวอักษรอธิบายได้ทั้งหมด ซึ่งอาจเปรียบเทียบได้กับการอ่านงบการเงิน และรายงานอื่น ๆ ที่ผู้อ่านควรเข้าใจเบื้องหลังและความหมายของตัวอักษรที่ปรากฏจากรายงานมากกว่า

### IT Governance เป็นเพียงส่วนหนึ่งที่สำคัญของ Good Corporate Governance

1. ขอบเขตการปฏิบัติงานของผู้เชี่ยวชาญ เช่นด้าน IT audit และ Technology อาจเป็นเพียงมุมมองเล็ก ๆ ของกรอบใหญ่ของการปฏิบัติงานตามมาตรฐานวิชาชีพการตรวจสอบภายใน และการเข้ากำกับดูแลกิจการที่ดี

2. Technology กับผู้เชี่ยวชาญอาจเป็นกรอบใหญ่ของการปฏิบัติงานตรวจสอบภายในบางด้าน ซึ่งจะขึ้นกับวัตถุประสงค์หลักของการปฏิบัติงาน ตามแผนการตรวจสอบ

3. คณะกรรมการ คณะกรรมการตรวจสอบ ผู้บริหารระดับสูง และผู้บริหารงานตรวจสอบภายในยังต้องรับผิดชอบในการตัดสินใจ การใช้ผลงานของผู้เชี่ยวชาญทุกประเภท โดยจะอ้างเป็นความรับผิดชอบของผู้เชี่ยวชาญไม่ได้

4. การตรวจสอบ Management Information System (MIS) เป็นสิ่งจำเป็น เพราะจะเกี่ยวข้องกับการประเมินการปฏิบัติงาน หรือการตรวจสอบคุณภาพของการดำเนินงานของฝ่ายงานต่าง ๆ การใช้ผู้เชี่ยวชาญจึง

อาจมีความจำเป็น แต่การประสานงานและสร้างมูลค่าเพิ่มจากการตรวจสอบ MIS และ IT Governance จากผู้เชี่ยวชาญมีความสำคัญยิ่งต่อการบรรลุ เป้าหมายในการปฏิบัติงานในภาพโดยรวมของ Good Corporate Governance

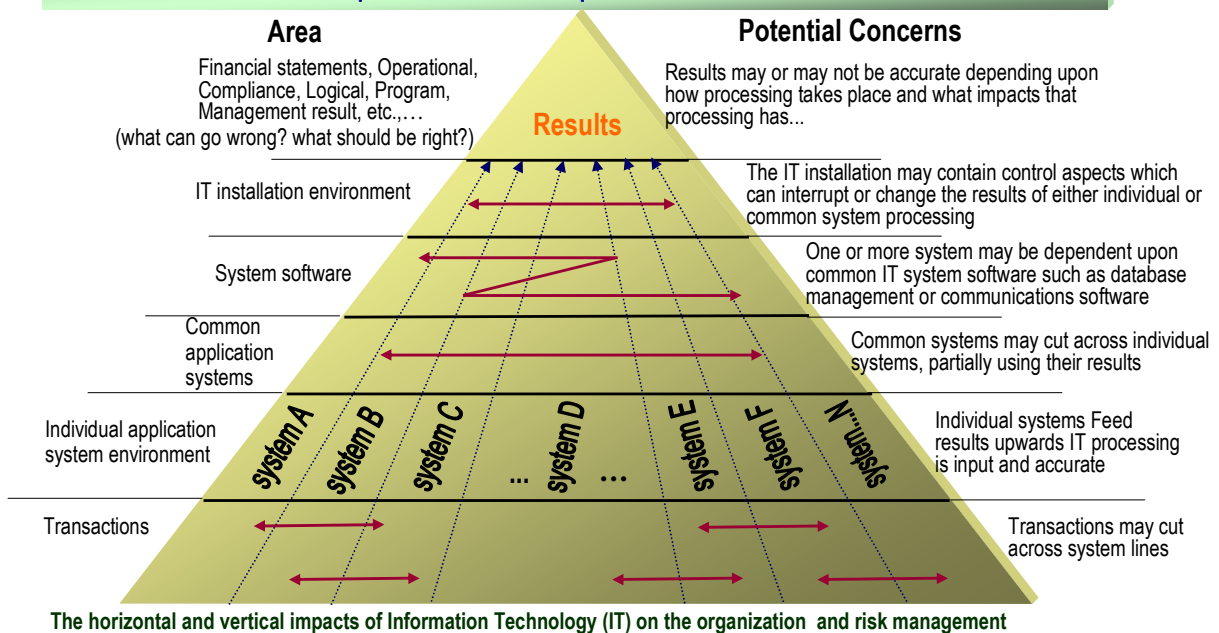
5. การยึดหลัก Value for money หรือ VFM ซึ่งเป็น concept ของการบริหารงาน และการจัดการที่ประหยัด โดยยังคงไว้ซึ่งประสิทธิผลและประสิทธิภาพที่ยอมรับได้นั้น เป็นเรื่องที่ต้องการตัดสินใจ และการประสานงานที่ถูกต้องเหมาะสม และรู้จริงจากผู้บริหาร

6. ความเสียหายจากความเสี่ยง เพราะมีความเข้าใจการมองภาพรวมของโลกแห่งการเปลี่ยนแปลง และวิธีในการประสานงาน เพื่อประสิทธิผล และประสิทธิภาพในการบริหารงานและการตรวจสอบนั้น มีนานาประการตั้งแต่ทำให้องค์กรขนาดใหญ่ และขนาดกลางหลายแห่งทั้งในและต่างประเทศล้มละลายไปแล้ว รวมทั้งบางองค์กรที่ยังดำรงเพื่อความอยู่รอดนั้นมีผลต่อเนื่องกระทบต่อเศรษฐกิจ การเงิน สังคม รวมทั้งการเมืองของไทยอย่างสำคัญชนิดคาดไม่ถึง ทั้งนี้จะได้ยกตัวอย่างจริงที่น่าสนใจหลายประการที่เกิดขึ้นแล้ว และอาจเกิดขึ้นอีกให้เป็นกรณีศึกษาไม่รู้จักโดยสังเขปเพื่อใช้ในการบริหาร และป้องกันความเสี่ยงที่อาจเกิดความเสียหายต่อประเทศและองค์กรต่าง ๆ เกินขนาดที่จะยอมรับได้ในโอกาสต่อไป

### IT Governance เป็นส่วนหนึ่งที่สำคัญยิ่งของ Good Corporate Governance ขององค์กร

ความเข้าใจในเรื่องการบริหารความเสี่ยงและการตรวจสอบ ที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ ในบางมุมมอง

#### องค์ประกอบการควบคุมภายในทั้ง 8 และวัตถุประสงค์การตรวจสอบภายในทั้ง 4 ประการ



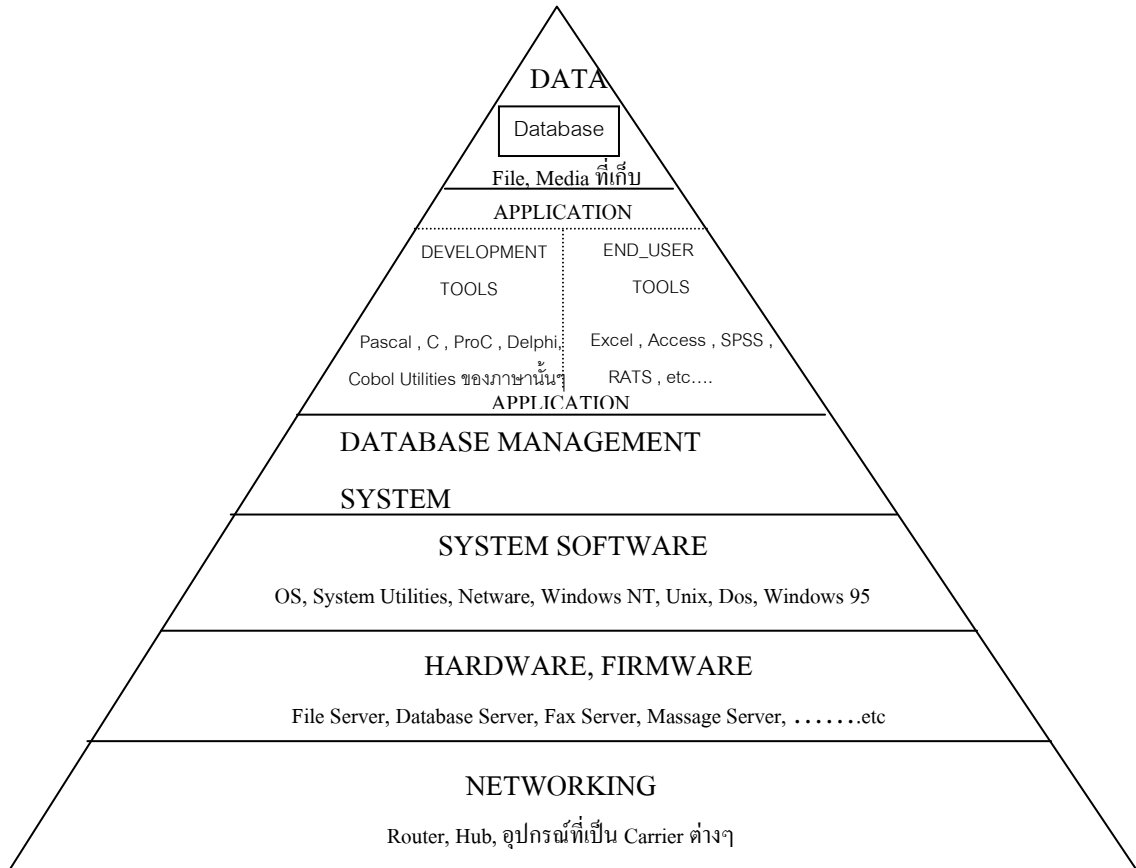
: แสดงถึง Total System Approaches ของระบบงานในภาพกว้าง ๆ ขององค์กรที่ใช้เทคโนโลยีสารสนเทศ ซึ่งต้องการความร่วมมือและการประสานงานจากผู้เชี่ยวชาญกับผู้บริหารงานขององค์กรอย่างเข้าใจจริงทั้งทางด้าน IT, non-IT, ITG และการบริหารความเสี่ยงโดยรวม ซึ่งองค์กรควรจะได้พิจารณาในการบริหารความเสี่ยงและการตรวจสอบแบบบูรณาการที่เกี่ยวข้องกับ business process เพื่อก้าวไปสู่ Business Objective โดยรวม

โดย อาจารย์ เมธา สุวรรณสาร

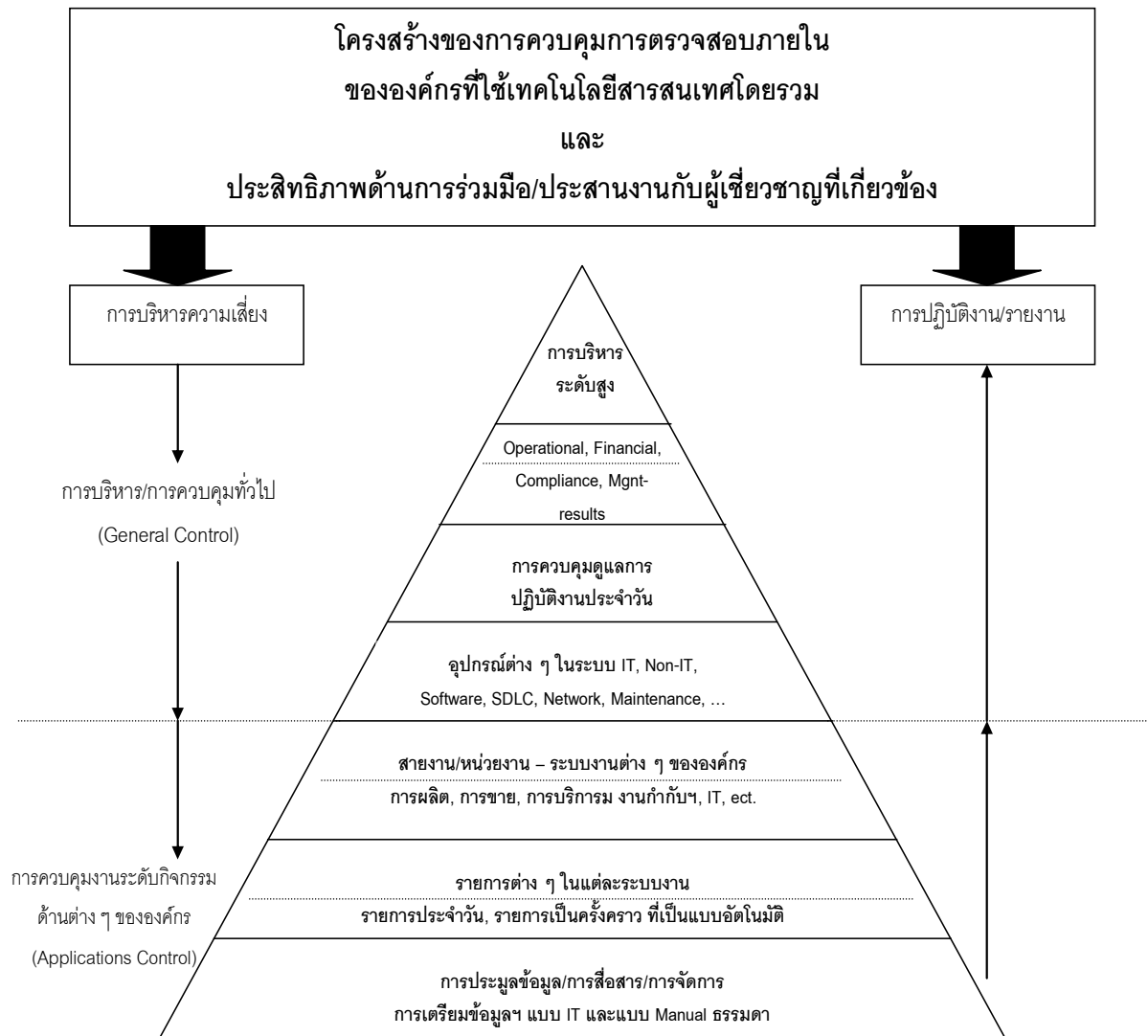
## การตรวจสอบและความเข้าใจผลกระทบทางด้าน Information Technology (IT)

และ

## การจัดการงานตรวจสอบภายใน/การประสานงานที่ดีเป็นสิ่งจำเป็น



ภาพแสดงโดยรวมของ IT บางมุมมองเพื่อให้ทราบว่า Technology ไม่ได้กระทบมาตรฐานวิชาชีพการปฏิบัติงานตรวจสอบภายในโดยตรง แต่การประสานงานระหว่างผู้เชี่ยวชาญอาจมีจุดอ่อนที่ก่อให้เกิดความเสี่ยงต่อการจัดการรวมทั้งงานตรวจสอบภายในซึ่งอาจกระทบต่อมาตรฐานฯได้



ความเสี่ยงทางการร่วมมือ/ประสานงาน (Coordination Risk) กับผู้เชี่ยวชาญพิเศษ/ที่ปรึกษาอื่นๆที่อาจมีความเข้าใจในวัตถุประสงค์รวมแตกต่างกัน ทั้งทางด้านการบริหารความเสี่ยง-การควบคุมและตรวจสอบที่อาจเกิดมีช่องว่างมากขึ้นทางด้าน Audit

การพัฒนาผู้ตรวจสอบให้มีความรู้ทางด้าน IT เพิ่มขึ้นและเข้าใจงานทั้ง IT Governance ซึ่งเป็นส่วนหนึ่งของ Good Corporate Governance จะช่วยลด Audit Risks ที่เกิดจาก Coordination Risk ได้อย่างน่าสนใจ แต่คงไม่ถึงกับขัดหลัก Code of Ethics ที่ว่าด้วย “คุณภาพของผู้ตรวจสอบภายใน” ที่ระบุไว้ว่า ผู้ตรวจสอบภายในควรมีส่วนเกี่ยวข้องในกิจกรรมที่ตนมีความรู้ ทักษะ และประสบการณ์เท่านั้น แต่ภาพนี้พยายามสื่อให้ถึงประเด็นของการประสานงานกับผู้เชี่ยวชาญที่ผู้บริหารงานตรวจสอบควรระวัง

## บทสรุปสำคัญของผู้บริหาร

ความยุ่งยากซับซ้อน การเชื่อมโยงประสานสัมพันธ์กัน และการรวมเป็นหนึ่งเดียวกันของกิจกรรมต่าง ๆ ที่เพิ่มขึ้นอยู่เสมอ และการเปลี่ยนแปลงอย่างรวดเร็วพลิกผันมากมายย่อมหนีไม่พ้นที่จะเข้าไปเกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Information Technology – IT) ซึ่งจะส่งผลกระทบต่อที่มีนัยสำคัญต่อต้นทุนค่าใช้จ่าย จำนวนมหาศาลและความเสี่ยงต่าง ๆ ที่จะเกิดขึ้นตามมาอย่างมาก แต่ในขณะเดียวกัน IT ก็สามารถก่อให้เกิด “โอกาส” พิเศษต่าง ๆ ที่จะเป็นตัวขับเคลื่อนและปฏิรูปธุรกิจ อย่างไรก็ตามต้นทุน ค่าใช้จ่าย และโอกาสไม่เพียงแต่ทำให้กลยุทธ์ทาง IT มีผลต่อการเจริญเติบโตและความสำเร็จขององค์กรเท่านั้น แต่ยังมีผลที่สำคัญยิ่งต่อ “ความอยู่รอด” ขององค์กรด้วย

คนส่วนใหญ่มักเชื่อกันว่า IT เป็นตัวขับเคลื่อนความมั่งคั่งทางเศรษฐกิจที่สำคัญในศตวรรษที่ 21 ในขณะที่ประเด็นดังกล่าวยังเป็นที่ยกเถียงกันอยู่ว่าเป็นความจริงหรือไม่ ก็เป็นที่แน่ชัดว่าองค์กรใดที่พึ่งพา IT เพื่อประโยชน์ในการแข่งขัน องค์กรนั้นจะต้องอยู่ภายใต้การกำกับดูแลทางการเงินและการกำกับดูแลที่ดีในภาพรวมขององค์กรด้วย ซึ่งเป็นหน้าที่และความรับผิดชอบโดยตรงของคณะกรรมการองค์กรและคณะกรรมการ IT ที่จะต้องควบคุมดูแลกิจการอย่างใกล้ชิด

หลักการที่สำคัญคือ การกำกับดูแลกิจการที่ดีด้านเทคโนโลยีสารสนเทศ (IT Governance – ITG) เกี่ยวข้องกับความรับผิดชอบ 2 ประการ คือ

1. IT จะต้องสร้างคุณค่าและส่งเสริมความสามารถทางธุรกิจ
2. ความเสี่ยงที่เกี่ยวข้องกับ IT จะต้องได้รับการบรรเทาให้ลดน้อยลง

**ทำไม IT จึงมีความสำคัญต่อองค์กร**

### 1. IT มีผลต่อมูลค่าทางการตลาด

ประการสำคัญ คือมูลค่าของสารสนเทศ (Information) และทรัพย์สินที่ไม่มีตัวตนทั้งหลาย เช่น คุณค่าของทรัพยากรบุคคล ชื่อยี่ห้อ คุณภาพการบริหารงาน ฯลฯ ล้วนเป็นส่วนหนึ่งของการแข่งขัน ซึ่งสิ่งเหล่านี้เกี่ยวพันกับการใช้ IT ทั้งสิ้น ความสามารถทางธุรกิจที่มาจากการใช้ IT จะนำไปสู่ความสำเร็จที่สำคัญในการเพิ่มเครือข่าย การซื้อขายทางการตลาด ฝ่ายการจัดการต้องเพิ่มความตระหนักถึงมูลค่าของทรัพย์สิน สารสนเทศขององค์กร และความสามารถในการใช้ประโยชน์จากสารสนเทศนั้น เมื่อทรัพย์สินไม่มีตัวตนมีความสำคัญมาก

ขึ้น ฝ่ายจัดการยังจำเป็นต้องชี้ให้เห็นถึงผลกระทบของ IT ที่มีต่อมูลค่าของผู้ถือหุ้น ในเรื่องนี้ Alan Greenspan ผู้ว่าการธนาคารสหรัฐฯ เคยกล่าวไว้ว่า องค์กรจะมีความเปราะบางถ้ามูลค่าเพิ่มขององค์กรมาจากทรัพย์สินที่มีตัวตนเป็นหลัก พร้อมทั้งยกตัวอย่างว่า ความเชื่อถือไว้วางใจและชื่อเสียงขององค์กรสามารถอันตรายไปได้เพียงชั่วข้ามคืน ซึ่งรวดเร็วกว่าความเสียหายของทรัพย์สินที่มีตัวตนเสียอีก

## 2. IT มีความสำคัญต่อการบรรลุเป้าหมายทางธุรกิจ

เป้าหมายทางธุรกิจจะไม่สามารถบรรลุผลได้โดยถ้าปราศจากการดำเนินงานอย่างต่อเนื่องของ IT ตัวอย่างของธุรกิจที่ต้องพึ่งพา IT คือ ธุรกิจการบิน การธนาคารการเงิน ตลาดหลักทรัพย์ และการประชาสัมพันธ์ การสื่อสารสาร ธุรกิจที่ต้องใช้ IT ในการดำเนินการเพื่อคาดการณ์ทางธุรกิจ และนับวันจะมีความสำคัญเพิ่มขึ้นมากในอนาคต แม้กระทั่งธุรกิจ SMEs หลายหมื่นรายในประเทศไทย

### ความมุ่งเน้นไปที่ IT Governance (ITG)

IT Governance คือการบริหารที่มีและเพิ่มคุณค่าเพื่อการเติบโตอย่างยั่งยืนระดับประเทศ ระดับองค์กร โดยการใช้เทคโนโลยีสารสนเทศผสมผสานในกระบวนการจัดการกับการบริหารความเสี่ยงระดับต่าง ๆ อย่างเหมาะสม คุ่มค่าอย่างเข้าใจจริงจัง ความได้เปรียบของศักยภาพของเทคโนโลยีสารสนเทศ (IT) เพื่อบรรลุถึงนโยบาย เป้าหมาย และวัตถุประสงค์ต่าง ๆ ขององค์กร

ในการประชุมคณะกรรมการและผู้บริหารระดับสูงจะต้องมีเรื่อง IT บรรจุอยู่ในวาระการประชุมเสมอ นักลงทุนบางรายตระหนักถึงความสำคัญของการกำกับดูแลที่ดี (Good Governance) โดยยินดีที่จะจ่ายบางส่วนเกินมูลค่าหุ้นถึง 20 เปอร์เซ็นต์ หรือมากกว่านั้นในสารสนเทศที่กำลังพัฒนา สารสนเทศและเทคโนโลยีที่นำมาใช้สนับสนุนการดำเนินงานขององค์กรเป็นสิ่งจำเป็นต่อความอยู่รอดและการเจริญเติบโตขององค์กรได้ กลายเป็นส่วนสำคัญของภาวะความรับผิดชอบต่อสังคมในการกำกับดูแลที่ดี ที่ต้องการความเข้าใจในการบูรณาการระหว่าง IT Governance กับ Good Corporate Governance การบริหารความเสี่ยง การควบคุมภายในและการตรวจสอบภายในตามฐานความเสี่ยงอย่างมาก

ไม่ใช่เพียงนักลงทุนเท่านั้นที่ส่งสัญญาณถึงเรื่องการกำกับดูแล สังคมที่ออกมาเรียกร้องความรับผิดชอบต่อความใส่ใจจากผู้บริหารและคณะกรรมการทั้งภาครัฐและภาคเอกชน ผู้กำหนดกฎระเบียบต่าง ๆ ไม่ว่าจะเป็น BIS (Bank of International Settlement ธนาคารเพื่อการชำระหนี้ระหว่างประเทศ) หรือคณะกรรมการของบริษัทที่จดทะเบียนในตลาดหลักทรัพย์ต่าง ๆ โดยเฉพาะของอังกฤษและอเมริกาต่างก็ให้ความสำคัญกับเรื่องนี้

อย่างไรก็ดี IT Governance ไม่ค่อยจะได้รับความสนใจหรือการใส่ใจเท่าที่ควร เนื่องจากการสอดคล้องดูแลทางด้าน IT แตกต่างจากการสอดคล้องดูแลเรื่องกลยุทธ์และความเสี่ยงทางธุรกิจ เพราะ

- IT เป็นเรื่องทางเทคนิค ยากที่จะเข้าใจได้ง่าย ๆ โดยเฉพาะผู้บริหารผู้บริหารที่มีเวลาน้อยมาก ก่อให้เกิดความเสี่ยงและโอกาสแก่องค์กรได้อย่างไรและควรเข้าไปเกี่ยวข้องกับเมื่อใด
- สายงาน IT มักถูกแยกหน่วยงานออกมาจากหน่วยงานทางธุรกิจ
- IT ยุ่งยากซับซ้อน โดยเฉพาะในช่วงที่ขยายเครือข่ายทางธุรกิจและการบริหาร Organization Governance Procedure ขององค์กร
- ระดับบริหารมีความรู้เกี่ยวกับ IT ค่อนข้างจำกัด

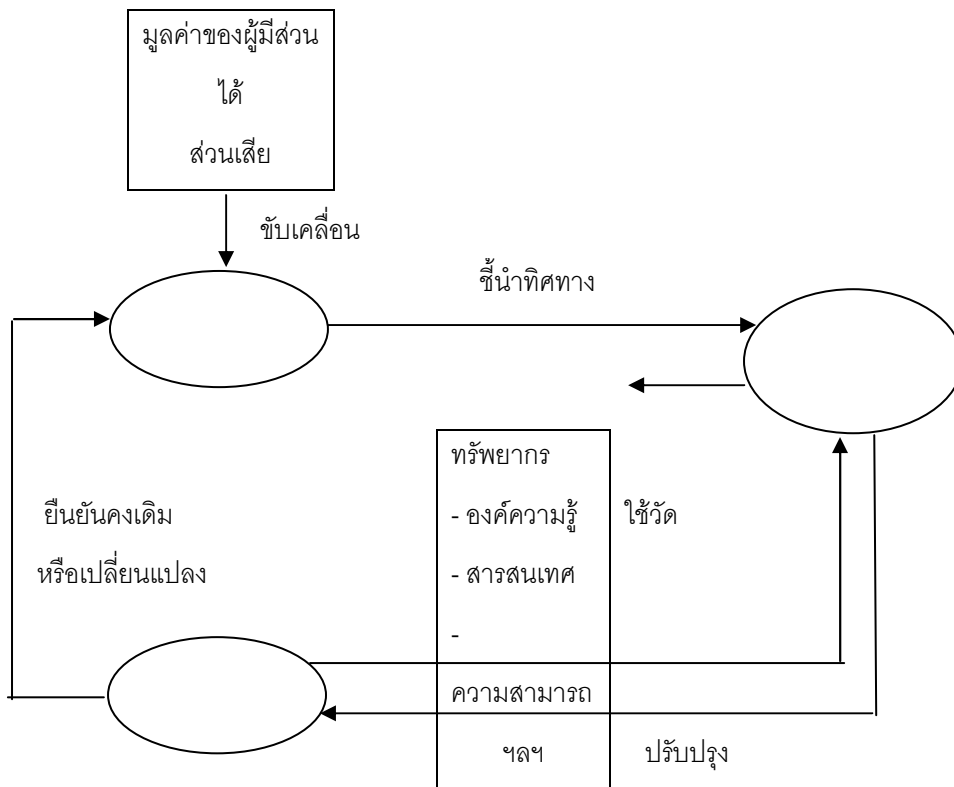
นั่นคือ คณะกรรมการ และอาจหมายรวมถึงผู้บริหารมักลังเลที่จะเข้าไปยุ่งเกี่ยวกับเรื่อง IT Governance อย่างไรก็ดีความไม่แน่ใจของฝ่ายบริหารไม่มีข้อสนับสนุนใด ๆ เนื่องจาก IT Governance มุ่งให้องค์กรมีการตัดสินใจที่ดี มีกระบวนการทำงานชัดเจน มีความเป็นผู้นำ ซึ่งล้วนแต่เป็นภาวะและความรับผิดชอบของคณะกรรมการและผู้บริหาร

สิ่งที่น่าสลดใจในเรื่อง IT Governance หรือ IT ก็คือประสบการณ์ในอดีตของคณะกรรมการที่มีต่อ IT มักจะเป็นในทางลบ ไม่ว่าจะเป็นความล้มเหลว หรือการทำผิดสัญญาต่าง ๆ ซึ่งมีอยู่อย่างแพร่หลายในแทบทุกอุตสาหกรรม

### IT Governance เหมาะสมกับจุดใดในองค์กร

IT Governance ไม่ใช่ปัจจัยแยกออกมาต่างหาก แต่เป็นองค์ประกอบของการกำกับดูแลที่ดีของทั้งองค์กร (Enterprise Governance) โดยมีความรับผิดชอบที่สำคัญ คือ

1. ในการกำหนดกลยุทธ์ขององค์กรจะคำนึงถึงมูลค่าของผู้มีส่วนได้ส่วนเสียเสมอ
2. ชี้นำทิศทางในกระบวนการที่นำกลยุทธ์มาดำเนินงาน
3. ดำเนินการให้มีความมั่นใจว่ากระบวนการปฏิบัติงานก่อให้เกิดสิ่งที่สามารถวัดผลได้
4. มีการรายงานผลและกระตุ้นให้เกิดความใส่ใจ
5. ดำเนินการให้มีความมั่นใจว่ามีการดำเนินการต่อผลที่ได้รับรายงาน



รายงาน

- ผลการปฏิบัติงาน
- ผลลัพธ์ที่ได้
- ความเสี่ยงที่เกิดขึ้น
- ทรัพย์สินต่างๆ

IT Governance มีส่วนเกี่ยวข้องกับการประยุกต์หลักการของการกำกับดูแลกิจการที่ดีองค์กร มาใช้ในการสั่งการและควบคุมการดำเนินงานของ IT โดยเฉพาะอย่างยิ่งจะเน้นในเรื่องต่อไปนี้

1. ศักยภาพของ IT ในการเพิ่มผลประโยชน์ทางการเงินและมีอิทธิพลเหนือสินทรัพย์ที่ไม่มีตัวตน เช่น สารสนเทศ องค์ความรู้ ความเชื่อถือไว้วางใจ
2. การดำเนินงานด้าน IT สอดคล้องและเป็นไปในแนวทางเดียวกับกลยุทธ์ขององค์กร
3. การสอบทานและอนุมัติในเรื่องการลงทุนทางด้าน IT
4. ความเชื่อมั่นในเรื่องความโปร่งใสของความเสี่ยงที่เกี่ยวข้องกับ IT
5. การวัดผลการดำเนินงานด้าน IT

IT Governance เป็นความรับผิดชอบของคณะกรรมการ คณะกรรมการจะแสดงความรับผิดชอบได้โดยการชี้แนะและสนับสนุนด้าน IT และขยายกลยุทธ์และวัตถุประสงค์ขององค์กรให้ครอบคลุมถึง IT ด้วย

### คณะกรรมการควรดำเนินการอย่างไร

คณะกรรมการไม่จำเป็นต้องเป็นผู้เชี่ยวชาญทางเทคโนโลยี แต่จำเป็นต้องพัฒนาและปรับตนเองให้สามารถเข้าใจอย่างถ่องแท้ว่าบทบาทและความรับผิดชอบต่อ IT ได้เปลี่ยนแปลงไปโดยคำนึงถึงการสอดส่องดูแลด้าน IT และคิดหาวิธีการที่จะผลักดันและจูงใจให้คณะกรรมการมีความเชี่ยวชาญทางธุรกิจเกี่ยวข้องกับ IT มากขึ้น

ประการแรก คณะกรรมการจะต้องถามคำถามยาก ๆ เกี่ยวกับ IT ถามถึงต้นทุนค่าใช้จ่าย ความเสี่ยง และโอกาสที่เกี่ยวข้อง ควรถามว่างาน IT บรรลุเป้าหมายหรือไม่ ผลประโยชน์ตอบแทนเป็นอย่างไร โดยควรจะศึกษาอย่างละเอียดเกี่ยวกับการดำเนินการให้กลับสู่สภาพเดิมเมื่อมีความเสี่ยงเพิ่มมากขึ้น และจะเพิ่มโอกาสในยุคของสารสนเทศได้อย่างไร

อีกประการหนึ่ง คณะกรรมการควรแต่งตั้งคณะกรรมการกำหนดกลยุทธ์ด้าน IT คณะกรรมการบางคณะไม่แน่ใจที่จะแต่งตั้งคณะกรรมการชุดนี้เนื่องจากเกรงว่าจะถูกมองว่าเป็นคณะกรรมการด้าน “เทคนิค” และ/หรือ CEO อาจเกรงว่าจะต้องติดต่oprสานวาทกับคณะกรรมการอีกคณะหนึ่ง

อย่างไรก็ดี ความสำคัญของคณะกรรมการกำหนดกลยุทธ์ด้าน IT ก็คือจะต้องขจัดอุปสรรค ข้อโต้แย้งเหล่านี้ให้หมดไป โดยทำหน้าที่สอบถามและอนุมัติกลยุทธ์ด้าน IT กำหนดทิศทางในระดับสูง และควบคุมมูลค่าที่ IT จะต้องก่อให้เกิด และความเสี่ยงด้าน IT ที่ต้องมีการจัดการอย่างเป็นรูปธรรม

### ฝ่ายบริหารควรจะทำอย่างไรบ้าง

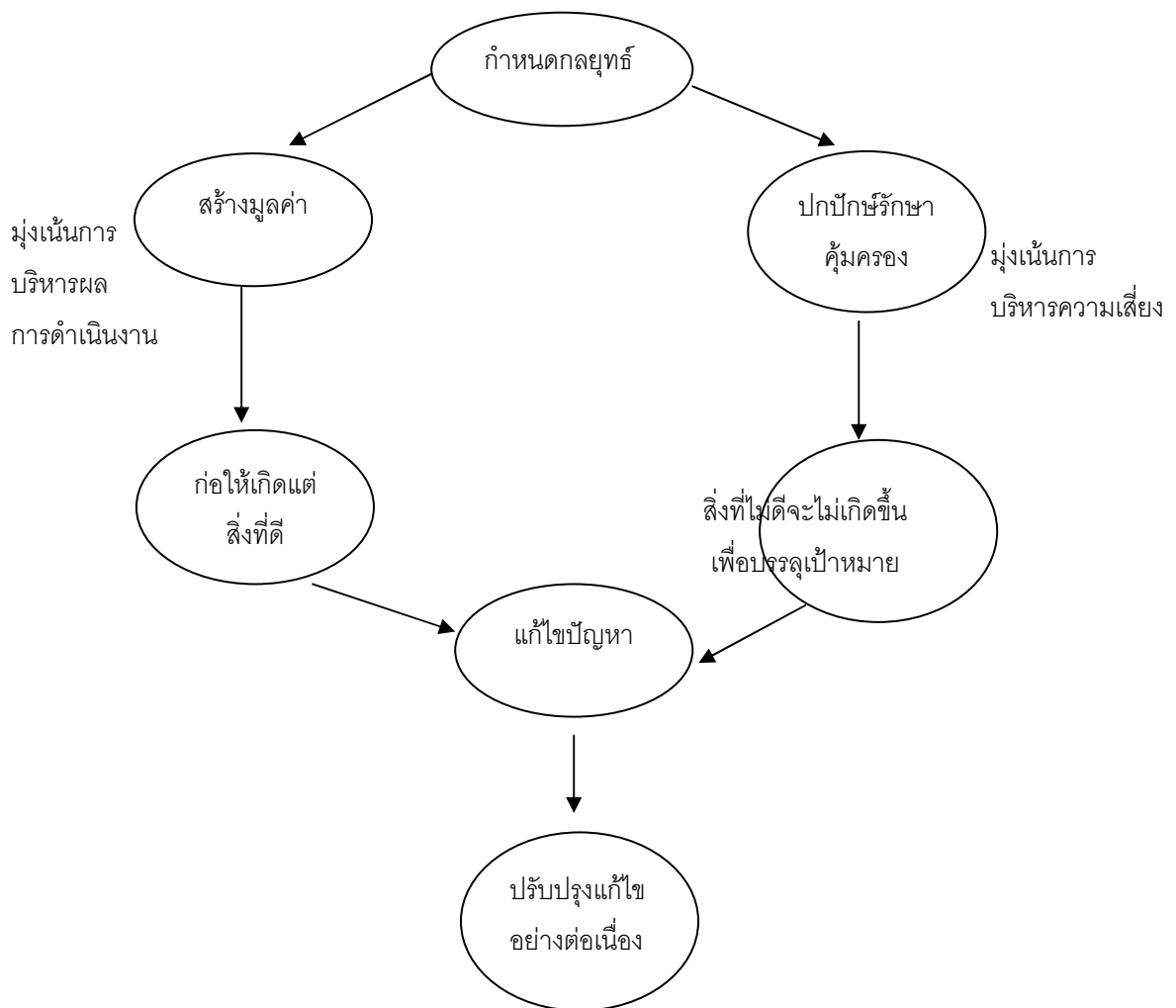
ขั้นตอนในการดำเนินงานควรมี ดังนี้

1. ฝ่ายบริหารควรกำหนดกลยุทธ์ด้าน IT ให้สอดคล้องเป็นไปในแนวทางเดียวกับกลยุทธ์ขององค์กร ผลักดันกลยุทธ์และเป้าหมายจากระดับสูงลงมาสู่ระดับล่างตามลำดับทั่วทั้งองค์กร และแปลงไปสู่ภาคปฏิบัติสำหรับพนักงานทุกระดับชั้น
2. ฝ่ายบริหารควรจัดองค์กรทางด้าน IT ให้สอดคล้องและเป็นไปในแนวทางเดียวกับการจัดองค์กรทางธุรกิจ ส่งเสริมให้มีความรับผิดชอบต่อร่วมกัน (ระหว่าง IT กับธุรกิจ) เพื่อความสำเร็จของโครงการด้าน IT และส่งผลตอบแทนคือมูลค่าทางธุรกิจแก่องค์กรและผู้มีผลประโยชน์ร่วม (Stakeholder)

3. ฝ่ายบริหารต้องมั่นใจว่าการวิเคราะห์ความเสี่ยงเป็นส่วนสำคัญของกระบวนการวางแผนโดยมุ่งเน้นที่จุดประจําบางของโครงสร้างพื้นฐานทาง IT ผลของทรัพย์สินที่ไม่มีตัวตนที่มีต่อการรักษาความปลอดภัยและความเสี่ยงในการดำเนินงาน และความเสี่ยงที่โครงการ IT จะล้มน้ลว

4. ฝ่ายบริหารควรนําการวัดผลการดำเนินงานออกมาใช้จริง โดยอิงกับกลยุทธ์และเป้าหมายเป็นสําคัญ เครื่องมือนําสมาัยที่เป็นที่ปรากฏในการวัดผลการดำเนินงาน คือ “Balanced Business Scorecard” โดยจะต้องแน่ใจว่าเมื่อนํา IT Scorecard มาใช้งานมูลค่าของข้อมูลสารสนเทศจะไม่ขัดแย้งกับตารางการวัดผลทางธุรกิจแบบดั้งเดิม

5. ผู้บริหารระดับสูงทาง IT (CIO : Chief Information Officer) มีหน้าที่ต้องชี้แนะทางความคิดหรือโน้มน้าวให้ชั้นตอนต่าง ๆ ที่กล่าวมาข้างต้นเกิดขึ้นมาได้จริง ต้องอยู่ในฐานะที่มีอำนาจในองค์กรและสามารถปฏิเสธสิ่งที่ไม่เห็นด้วย หรือไม่ชอบบรรม



## อนาคตเป็นอย่างไร

ประเด็นต่าง ๆ ในการบริหาร IT จะเปลี่ยนแปลงจากเทคโนโลยีไปสู่สิ่งดีพิมพ์ที่เกี่ยวกับการบริหาร โดยทั่วไป ซึ่งจะนำไปสู่ความสำเนียงรบผิดชอบของ ITG ดังนี้

1. ปรับ IT ให้เป็นแนวทางเดียวกับกลยุทธ์ขององค์กร  
มุ่งเน้นที่จะปรับ IT ให้เข้ากับธุรกิจและให้ความร่วมมือช่วยเหลือซึ่งกันและกัน
2. การสร้างมูลค่าเพิ่ม  
มุ่งเน้นการทำให้ค่าใช้จ่ายเกิดประโยชน์สูงสุดและพิสูจน์ให้เห็นถึงมูลค่าของ IT อย่าง แท้จริง
3. การบริหารสินทรัพย์ IT  
มุ่งเน้นที่องค์ความรู้และโครงสร้างพื้นฐานทาง IT
4. การบริหารความเสี่ยง

กล่าวถึงการปกป้องดูแลทรัพย์สินทาง IT ทั้งทางด้าน Logical และ Physical และการฟื้นฟูภัยธุรกิจเมื่อเกิดเหตุฉุกเฉิน นอกจากนี้สิ่งที่กล่าวมาทั้งหมดจะไม่สามารถดำเนินการได้อย่างเหมาะสมในสภาพแวดล้อมทางเศรษฐกิจและการเมืองที่ซับซ้อน หากปราศจากความรู้ ความเข้าใจของความสัมพันธ์ระหว่าง Good Corporate Governance IT Governance การบริหารความเสี่ยง การควบคุมภายในและการตรวจสอบภายในตามฐานความเสี่ยง

5. การวัดผลการดำเนินงาน

มุ่งเน้นที่ความสำเร็จทั้งความเป็นผู้นำทางธุรกิจและ IT ที่จะนำไปสู่กลยุทธ์ขององค์กร นั่นคือการนำ IT Balanced Scorecard มาใช้ในองค์กรชั้นนำ

## บทสรุป

IT ได้เคลื่อนย้ายจากประเด็นทางเทคนิคไปสู่ประเด็นทางการบริหารและการกำกับดูแลที่ดี ผลกระทบของ IT และการบริหาร ITG ที่มีต่อทรัพย์สินที่ไม่มีตัวตน บทบาทที่สำคัญของ IT เพื่อความอยู่รอดและความจำเป็นที่จะทำให้มูลค่าของ IT มีค่าสูงสุด องค์กรประกอบ ทั้งสามอย่างนี้ทำให้เกิดความจำเป็นที่หลีกเลี่ยงไม่ได้ที่จะนำหัวข้อ IT Governance บรรจุไว้ในวาระการพิจารณาของคณะกรรมการ เนื่องจากเป็นส่วนที่จำเป็นสำหรับการกำกับดูแลที่ดี การกำกับดูแลหรือธรรมาภิบาลมีผลกระทบต่อมูลค่าผู้ถือหุ้นและผู้มีผลประโยชน์ร่วมอย่างแน่นนอนขึ้นกับว่าองค์กรมีความสนใจความสัมพันธ์ที่ปฏิเสธไม่ได้แล้วหรือยัง

สำหรับองค์กรที่มีหรือใช้ IT เป็นส่วนน้อย การนำ IT Governance หรือการบริหารควบคุม IT มาใช้ในองค์กรอาจดูเหมือนเป็นภาระอันหนักหน่วง แต่ที่แท้จริงแล้วคณะกรรมการตระหนักดีว่า IT ไม่เพียงแต่สามารถช่วยองค์กรให้ทำงานง่ายและสะดวกขึ้น แต่ยังช่วยปฏิรูปแปรสภาพองค์กรได้อีกด้วย

ความเข้าใจในเรื่อง IT Governance รวมทั้งเรื่องที่เกี่ยวข้องข้างต้น และประโยชน์ที่ได้รับจากเรื่องนี้ที่ต้องใช้คู่กันไปกับ Corporate Governance และองค์ประกอบอื่นๆที่สัมพันธ์กันนั้น จะนำองค์กรก้าวไปสู่การบริหารที่สามารถสร้างคุณค่าเพิ่ม ความสามารถในการแข่งขัน ความไว้วางใจจากผู้มีผลประโยชน์ร่วมทุกฝ่าย ตามแนวทางการบริหาร แบบ Consolidated-Single Framework ซึ่งเป็นการขับเคลื่อน Integrity-Driven Performance ตามหลักการ และแนวทางการบริหารยุคใหม่ที่เรียกว่า GRC ซึ่งเป็นคำย่อของ Governance-Risk Management-Compliance ที่ท้าทายต่อผู้บริหารทุกองค์กรในยุคปัจจุบันต่อไป

\*\*\*\*\*



## ประวัติ นายเมธา สุวรรณสาร



1. วุฒิบัตรและการศึกษา
  - 1.1 วุฒิบัตรอาชีพ บรรษัทภิบาลด้านเทคโนโลยีสารสนเทศสากล [ ITG] ( CGEIT – Certified in the Governance of Enterprise IT, USA)
  - 1.2 วุฒิบัตรอาชีพ ผู้ตรวจสอบภายในรับอนุญาตสากล ( CIA – Certified Internal Audit, USA)
  - 1.3 วุฒิบัตรอาชีพ ผู้สอบบัญชีรับอนุญาต ( CPA – Certified Public Accountant, ประเทศไทย)
  - 1.4 ประกาศนียบัตรการตรวจสอบคอมพิวเตอร์จาก Federal Deposit Insurance Corporation (FDIC-USA)
  - 1.5 ประกาศนียบัตรด้าน Management จาก University of California at Berkeley-USA
  - 1.6 ประกาศนียบัตร Advanced Management จาก Harvard University Graduate School of Business Administration ประเทศสหรัฐอเมริกา
  - 1.7 วุฒิบัตรของสถาบันกรรมการบริษัทไทย (IOD) และ Australian Institute of Company Directors (AICD) ในหลักสูตร Directors Certification Program-DCP
  - 1.8 ประกาศนียบัตร New Era Governance ของ Audit Committee จาก Harvard Business School
  - 1.9 บัณฑิตบัณฑิต จากมหาวิทยาลัยธรรมศาสตร์
  - 1.10 พาดิษยศาสตร์บัณฑิต จากมหาวิทยาลัยธรรมศาสตร์
2. ปัจจุบัน.... ( เมษายน พ.ศ. 2553)
  - 2.1 อุปนายกสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA - Thailand Information Security Association)
  - 2.2 ประธานตรวจสอบสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ-ภาคพื้นกรุงเทพฯ Audit Chair-ISACA-Information Systems Audit and Control Association - Bangkok Chapter

- 2.3 กรรมการวิชาการมาตรฐานการรักษาความมั่นคงในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC – National Electronics and Computer Technology Center)
- 2.4 ผู้เชี่ยวชาญด้าน IT Examination ของ ฐปท.
- 2.5 คณะทำงานศึกษากระบวนการรับรองหน่วยงานมาตรฐาน Certified Body และมาตรฐานที่เกี่ยวข้องในการกำกับดูแลผู้ให้บริการออกไปรับรองอิเล็กทรอนิกส์ (Certification Authority : CA) สวทช.
- 2.6 ประธานกรรมการสรรหาและกำหนดผลตอบแทน, กรรมการอิสระและกรรมการตรวจสอบ ธนาคารไทยเครดิต
- 2.7 ประธานกรรมการสรรหาและกำหนดผลตอบแทน กรรมการอิสระและกรรมการตรวจสอบ บริษัท ศรีอยุธยาประกันภัย จำกัด (มหาชน)
- 2.8 อุปนายก สมาคมผู้ตรวจสอบภายใน แห่งประเทศไทย- สตท
- 2.9 อนุกรรมการมาตรฐาน พัฒนา วิจัยเกี่ยวกับการทำธุรกรรมทางอิเล็กทรอนิกส์ ก. ICT
- 2.10 ผู้บรรยาย Risk & Financial Management หลักสูตร ปรัชญาดุสิตบัณฑิต สาขาวิชาการสารสนเทศศึกษา วิชา Management of Information and communication Technology คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัย ขอนแก่น และองค์กรต่าง ๆ ทั้งภาครัฐและภาคเอกชน
- 2.11 ผู้บรรยาย ทางด้าน Corporate Governance, IT Governance, GRC การบริหารความเสี่ยง, การควบคุมและการตรวจสอบภายในตามฐานความเสี่ยง และการตรวจสอบด้านคอมพิวเตอร์
- 2.12 เขียนบทความต่าง ๆ ที่เกี่ยวข้องกับ 2.11 เผยแพร่ส่วนใหญ่ที่ สมาคมผู้ตรวจสอบภายใน แห่งประเทศไทย (สตท) ในปี 2551 เขียน Road Map ในการก้าวสู่ IT Governance และ เรื่อง การประเมินตนเอง (CSA) เพื่อก้าวไปสู่คุณภาพของการกำกับที่ดี 2552 เขียนแนวทางการบริหารความเสี่ยง ตามแนวทางของ COSO v.2
- 2.13 จัดทำ Website: [www.itgthailand.wordpress.com](http://www.itgthailand.wordpress.com); [www.itgthailand.com](http://www.itgthailand.com) เมื่อปี พ.ศ. 2552 ถึงปัจจุบัน เพื่อเสริมสร้างและแลกเปลี่ยนความคิดเห็นใหม่ๆต่อสังคมแห่งการเรียนรู้ โดยมีหัวข้อต่างๆที่เกี่ยวกับ CG;+ ITG;+GRC;+COSO-ERM;+ IT- Audit & Non-IT Audit + วิเคราะห์ ความเสี่ยง+ การยกระดับความเสี่ยง + แนวทางการบริหารความเสี่ยงขององค์กรโดยทั่วไป + คุยกับผู้เขียน+++

3. การเป็นตัวแทนของไทยและธนาคารแห่งประเทศไทยในอดีต
  - 3.1 เป็นหัวหน้าคณะผู้แทนของไทย (Thailand Representative) ในการประชุมที่องค์การสหประชาชาติที่ New York ประเทศสหรัฐอเมริกาในปี 2532 เรื่อง Draft Model Rules on Electronic Funds Transfer ที่ UN จัดให้มีขึ้นเป็นครั้งแรก
  - 3.2 ประธานกรรมการ บริษัทเครดิตฟองซิเอร์สากลสยาม จำกัด
  - 3.3 ประธานคณะทำงานพิจารณากำหนดรายการและความหมายของรายการในงบดุลและบัญชีกำไรขาดทุนของบริษัทมหาชนที่ประกอบธุรกิจเงินทุน ธุรกิจหลักทรัพย์ ธุรกิจเงินทุนและหลักทรัพย์ และธุรกิจเครดิตฟองซิเอร์
  - 3.4 ประธานคณะทำงานด้านเศรษฐกิจและการเงินจังหวัดขอนแก่นในการเชื่อมความสัมพันธ์กับเมืองหนานหนิง ประเทศจีน ปี 2537
  - 3.5 หัวหน้าคณะทำงานศึกษาปัญหาการค้าชายแดนไทย-ลาว ปี 2537
  - 3.6 รองประธานคณะกรรมการพิจารณาผลตอบแทนและความเสี่ยงของบริษัทเงินทุนและสถาบันการเงิน
  - 3.7 ผู้ร่วมก่อตั้งและกรรมการที่ปรึกษาของสมาคมผู้ตรวจสอบงานคอมพิวเตอร์ ภาคพื้นกรุงเทพฯ (EDPPA – Bangkok Chapter) ปัจจุบัน เปลี่ยนชื่อเป็น ISACA
  - 3.8 อนุกรรมการสอบบัญชีกิจการที่ใช้คอมพิวเตอร์ กบ.ช.
  - 3.9 อนุกรรมการมารยาทผู้สอบบัญชีรับอนุญาต กบ.ช.
  - 3.10 ที่ปรึกษาของสมาคมผู้ตรวจสอบงานคอมพิวเตอร์ภาคพื้นกรุงเทพฯ (Information Systems Audit and Control Association (ISACA) – Bangkok Chapter)
  - 3.11 รองประธานกรรมการสหกรณ์ออกทรัพย์พนักงานธนาคารแห่งประเทศไทย
  - 3.12 ที่ปรึกษาด้านการเงินและการบัญชีสหกรณ์ออมทรัพย์พนักงานธนาคารแห่งประเทศไทย
  - 3.13 กรรมการพัฒนาจังหวัดขอนแก่น (กพจ.)
  - 3.14 กรรมการพัฒนาเทศบาลนครขอนแก่น
  - 3.15 ที่ปรึกษากิตติมศักดิ์โครงการศึกษาและจัดทำแผนลงทุนจังหวัดขอนแก่น กาฬสินธุ์ มหาสารคาม และหนองบัวลำภู
  - 3.16 ที่ปรึกษาคณะกรรมการศึกษารูปแบบการบริหารวิชาการของมหาวิทยาลัยขอนแก่น
  - 3.17 คณะทำงานศึกษาศักยภาพและแนวทางการพัฒนาเพื่อกระจายความเจริญสู่ภูมิภาค จังหวัดขอนแก่น
  - 3.18 กรรมการผู้ทรงคุณวุฒิประจำศูนย์บริการวิชาการ มหาวิทยาลัยขอนแก่น

- 3.19 กรรมการชุดต่าง ๆ ในธนาคารแห่งประเทศไทย
  - 3.20 กรรมการคณะทำงานแผนสำรวจฉุกเฉินเพื่อรองรับปัญหาปี ค.ศ. 2000
  - 3.21 กรรมการคณะทำงานแก้ไขปัญหาปี ค.ศ. 2000 งานด้านเทคโนโลยีสารสนเทศ
  - 3.22 กรรมการคณะทำงานแก้ไขปัญหาปี ค.ศ. 2000 ด้าน Non-IT
  - 3.23 กรรมการคณะทำงานกำกับตรวจสอบการแก้ไขปัญหาปี ค.ศ. 2000 ของสถาบันการเงิน
  - 3.24 กรรมการคอมพิวเตอร์
  - 3.25 กรรมการคณะทำงานปรับปรุงข้อมูล ฐานข้อมูล และระบบข้อมูลของธนาคาร
  - 3.26 กรรมการบริหารและประสานงานสาขาภาค
  - 3.27 กรรมการพัฒนาสถาบันการเงิน
  - 3.28 กรรมการเกี่ยวกับเอกสารและระบบของเอกสารของธนาคารแห่งประเทศไทยที่สถาบันการเงินต้องปฏิบัติ
  - 3.29 กรรมการระบบการชำระเงิน
  - 3.30 กรรมการโครงการพัฒนาระบบห้องค้าเงินฝ่ายการธนาคาร กรรมการการสื่อสารภายในธนาคาร
4. การเข้ามีส่วนร่วมในกิจกรรมของมหาวิทยาลัย กิจกรรมอุดมศึกษา และการบรรยายที่สำคัญ
    - 4.1 เป็นผู้ถวายรายงานเรื่อง – ภาคอีสานกับการพัฒนาเศรษฐกิจ สังคม และสิ่งแวดล้อม” แต่สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ณ มหาวิทยาลัยขอนแก่น(พ.ศ. 2538)
    - 4.2 ประธานคณะทำงานในการค้นคว้าวิจัยเรื่อง การกำกับดูแลที่ดินกับการตรวจสอบให้กับวิทยาลัยการจัดการ มหาวิทยาลัยขอนแก่น (พ.ศ. 2545)
    - 4.3 ผู้เขียนหนังสือเรื่อง การตรวจสอบคอมพิวเตอร์กับการทุจริต หน่วยที่ 14 ให้กับมหาวิทยาลัยสุโขทัยธรรมมาธิราช – มสธ. (พ.ศ. 2545)
    - 4.4 เป็นผู้บรรยายวิชาการบริหารความเสี่ยงให้กับนักศึกษาในระดับปริญญาเอกในมหาวิทยาลัยขอนแก่น (พ.ศ. 2548 – 2553)
    - 4.5 เป็นผู้บรรยายให้กับนักศึกษาระดับปริญญาโทในมหาวิทยาลัยธรรมศาสตร์ด้านการบริหารความเสี่ยงและการตรวจสอบคอมพิวเตอร์ วิทยาลัยบัณฑิตการศึกษารัฐบาล มหาวิทยาลัยขอนแก่น ระดับปริญญาตรีที่จุฬาลงกรณ์มหาวิทยาลัย มหาวิทยาลัยธรรมศาสตร์ และปริญญาตรีในมหาวิทยาลัยหลายแห่ง
    - 4.6 เป็นผู้บรรยายการตรวจสอบสถาบันการเงินที่ใช้คอมพิวเตอร์ของประเทศต่าง ๆ ใน SEACEN (กลุ่มธนาคารต่าง ๆ ในประเทศแถบเอเชีย รวมเกาหลีใต้และไต้หวัน)

- 4.7 เป็นผู้บรรยายให้กับธนาคารพาณิชย์ ธนาคารเฉพาะกิจ และองค์กรต่าง ๆ รวมทั้งสถาบันเทคโนโลยีแห่งเอเชีย (Asian Institute of Technology – AIT) ส่วนใหญ่เน้นหนักไปในเรื่อง Computer Audit/IT Audit ของ SEACEN ที่กรุงเทพฯ
  - 4.8 เป็น Course Director หลักสูตร Computer Audit (Advanced Level) ของ SEACEN ที่กรุงเทพฯ
  - 4.9 เป็น Deputy Principal หลักสูตร Inspection and Supervision of Financial Institution ของ SEACEN ที่ประเทศ Indonesia
  - 4.10 อาจารย์ที่ปรึกษาวิทยานิพนธ์ทางด้านคอมพิวเตอร์ 2 เรื่องและด้าน กฎหมาย 1 เรื่อง
  - 4.11 เป็นผู้บรรยายด้านเศรษฐกิจ การเงิน การธนาคาร การตรวจสอบสถาบันการเงินให้กับส่วนงานต่าง ๆ
  - 4.12 เป็นวิทยากรบรรยายเรื่อง เศรษฐกิจการเงินของภาคตะวันออกเฉียงเหนือแก่ คณะนักศึกษามหาวิทยาลัยขอนแก่น และอื่น ๆ
  - 4.13 เป็นวิทยากรบรรยายเรื่อง The Year 2000 Challenges and Solutions และหัวข้ออื่น ๆ ที่เกี่ยวกับปัญหาปี ค.ศ. 2000 ที่จัดโดยหน่วยงานต่าง ๆ รวมทั้ง Asian Institute of Technology – AIT
  - 4.14 เป็นวิทยากรบรรยายเรื่อง การตรวจสอบภายใน การประเมิน และการบริหารความเสี่ยง รวมทั้ง การตรวจสอบการทุจริต (IT และ Non – IT) ให้กับองค์กรต่าง ๆ
5. งานเขียนหนังสือและอื่น ๆ
- 5.0 ผู้เขียน- บทความต่าง ๆ ให้กับ สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย- สตท ปี 2548-2553
  - 5.1 ผู้เขียน – การบริหารความเสี่ยงกับ พรบ. บริษัทมหาชน จำกัด (พ.ศ. 2548)
  - 5.2 ผู้เขียน – IT Governance กับการสร้างมูลค่าเพิ่ม (พ.ศ. 2548)
  - 5.3 ผู้เขียน – IT Governance กับ Risk Management (พ.ศ. 2546)
  - 5.4 ผู้เขียน – การบริหารความเสี่ยงและการป้องกันการทุจริตกับ พรบ. บริษัทมหาชน จำกัด (พ.ศ. 2548)
  - 5.5 ผู้เขียน – การกำกับดูแลกิจการที่ดีกับการบริหารความเสี่ยง (พ.ศ. 2544)
  - 5.6 ผู้เขียน – การกำกับดูแลกิจการที่ดีกับการเปลี่ยนแปลง (พ.ศ. 2545)
  - 5.7 ผู้เขียน – ความเสี่ยงของการจัดการงานตรวจสอบภายในกับ IT Governance (พ.ศ. 2545)

- 5.8 ผู้เขียน – การพัฒนาความคิดเพื่อการกำกับดูแลกิจการที่ดี (พ.ศ. 2545)
- 5.9 ผู้เขียน – การบริหารทรัพยากรขององค์กร (Enterprise Resource Planning –ERP) กับการบริหารความเสี่ยง (พ.ศ. 2545)
- 5.10 ผู้เขียน – ปัญหาของโปรแกรมคอมพิวเตอร์ครั้งใหม่ New Software Crisis กับบทพิสูจน์คุณภาพการบริหารความเสี่ยงของทุกองค์กร (พ.ศ. 2545)
- 5.11 ผู้เขียน – สัญญาณการทุจริต (Red Flag) ในสถาบันการเงินต่าง ๆ (พ.ศ. 2545)
- 5.12 ผู้เขียนหนังสือ ปัญหาปี ค.ศ. 2000 (Y2K) กับผู้สอบบัญชี
- 5.13 ผู้เขียน ผู้จัดทำและเรียบเรียงหนังสือ การดำเนินงานและการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์ ซึ่งเป็นชุด 4 เล่ม ประกอบด้วย (พ.ศ. 2539)
- เล่มที่ 1 เรื่องคอมพิวเตอร์กับการบริหารและการดำเนินงาน
  - เล่มที่ 2 เรื่อง คอมพิวเตอร์กับการตรวจสอบ
  - เล่มที่ 3 เรื่อง คอมพิวเตอร์กับการทุจริต
  - เล่มที่ 4 เรื่อง คอมพิวเตอร์กับแผนฉุกเฉิน
- 5.14 ผู้เขียน การตรวจสอบคอมพิวเตอร์กับการทุจริต (หน่วยที่ 14) ของ มสท. ปี 2545
- 5.15 ผู้เขียนผู้จัดทำและเรียบเรียงหนังสือเรื่อง “การบริหารและประเมินความเสี่ยงแบบ RAS และ CAMEL กับการวัดประสิทธิภาพการจัดการของสหกรณ์ออมทรัพย์และสถาบันการเงิน
- 5.16 ผู้เขียน ผู้จัดทำและเรียบเรียงหนังสือ การจัดการระบบควบคุมภายในกับความเสี่ยงของสถาบันการเงิน
- 5.17 ผู้เขียน แนวความคิดและหลักการในการสร้างระบบเรียกเก็บเงินตามเช็คต่างจังหวัด (B/C) เสมือนหนึ่ง ONE-Day Clearing ทั่วประเทศ ปี พ.ศ. 2540
- 5.18 ผู้เขียน อาชญากรรมและการทุจริตด้านคอมพิวเตอร์ และบทความทางการเงินและการตรวจสอบอื่น ๆ
- 5.19 เป็นผู้ริเริ่มโครงการตรวจสอบด้านคอมพิวเตอร์ (Computer Audit) การทำ Off site back up และ Disaster Recovery Plan ให้กับธนาคารพาณิชย์ ธนาคารเฉพาะกิจ และสถาบันการเงินต่าง ๆ ในประเทศ (พ.ศ. 2527)

6. ประวัติการทำงานที่ธนาคารแห่งประเทศไทยและที่อื่น ๆ
- 6.1 2551 - ได้รับเชิญเป็นผู้เชี่ยวชาญการตรวจสอบเทคโนโลยีสารสนเทศ ของธนาคารแห่งประเทศไทย และร่วมการวิจารณ์ การทำคู่มือ การตรวจสอบด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน
- 6.2 2550 - 2551 - อนุกรรมการผู้ทรงคุณวุฒิ คณะอนุกรรมการพัฒนามาตรฐานการปฏิบัติหน้าที่ของผู้ตรวจสอบภายใน สำนักงานตรวจเงินแผ่นดิน
- 6.3 2550-2551 - กรรมการ กรรมการตรวจสอบและ ประธานกรรมการสรรหาและกำหนด ผลตอบแทน ธนาคารไทยเครดิตเพื่อรายย่อย
- 6.4 2550-2551 - กรรมการ กรรมการตรวจสอบและ ประธานกรรมการสรรหาและ กำหนดผลตอบแทน บริษัท ศรีอยุธยาประกันภัยจำกัด
- กรรมการปรับปรุงระบบการประเมินผล รัฐวิสาหกิจ ของ ก.คลัง
- 6.5 2549-2550 - ประธานคณะกรรมการตรวจสอบ สำนักงานส่งเสริมอุตสาหกรรมซอฟต์แวร์แห่งชาติ (องค์การมหาชน)
- กรรมการและกรรมการตรวจสอบ บริษัท ศรีอยุธยาประกันภัย จำกัด (มหาชน)
- หัวหน้าคณะที่ปรึกษาโครงการ IT Governance และ IT Management ของบริษัท ทีไอที จำกัด (มหาชน)
- หัวหน้าคณะที่ปรึกษาโครงการกำกับดูแลกิจการที่ดี (Good Corporate Governance) และการประเมินตนเองและการควบคุมความเสี่ยง (CSA – Control Self Assessment) ของกรมศุลกากรและสำนักงานศุลกากร ท่าเรือแหลมฉบัง
- 6.6 2548 - หัวหน้าคณะที่ปรึกษาโครงการกำกับดูแลกิจการที่ดี (Good Corporate Governance) และการประเมินตนเองและการควบคุมความเสี่ยง (CSA – Control Self Assessment) ของกรมศุลกากรและสำนักงานศุลกากร ท่าเรือแหลมฉบัง
- 6.7 2547 - กรรมการตรวจสอบในการไฟฟ้านครหลวง
- ที่ปรึกษาประธานคณะกรรมการ บริษัท ทีไอที จำกัด (มหาชน)
- ที่ปรึกษาคณะกรรมการตรวจสอบ บริษัท ทีไอที จำกัด (มหาชน)
- ประธานกลุ่มภารกิจด้านการเงิน บริษัท กสท. จำกัด

- ประธานคณะกรรมการควบคุมภายใน บริษัท กสท. จำกัด
  - ที่ปรึกษาคณะกรรมการตรวจสอบ บริษัท กสท. จำกัด
  - กรรมการและประธานคณะกรรมการตรวจสอบ บริษัท บริหารสินทรัพย์  
กรุงเทพพาณิชย์
  - กรรมการและกรรมการตรวจสอบบริษัทประกันสินเชื่ออุตสาหกรรม  
ขนาดย่อม (บสย.)
  - ที่ปรึกษาคณะกรรมการ IT บริษัทประกันสินเชื่ออุตสาหกรรมขนาด  
ย่อม (บสย.)
  - ที่ปรึกษาคณะกรรมการตรวจสอบการรถไฟแห่งประเทศไทย
- 6.8 2544
- ประธานคณะกรรมการ Advanced Technology Committee สมาคม  
ผู้ตรวจสอบภายในแห่งประเทศไทย
  - กรรมการสมาคมผู้ตรวจสอบภายในแห่งประเทศไทย
- 6.9 2543
- ประธานคณะกรรมการ Advanced Technology Committee (สตท.)
  - ผู้จัดการสมาคมผู้ตรวจสอบภายในแห่งประเทศไทย (สตท)
  - ประธานคณะกรรมการตรวจสอบธนาคารเกษตรและสหกรณ์  
การเกษตร
  - กรรมการบริหารบริษัทประกันสินเชื่ออุตสาหกรรมขนาดย่อม
- 6.10 2542
- ผู้อำนวยการอาวุโสโรงพิมพ์ธนบัตร
- 6.11 2540 - 2542
- ผู้อำนวยการอาวุโส ฝ่ายเทคโนโลยีสารสนเทศ ธปท
- 6.12 2537 - 2540
- ผู้อำนวยการอาวุโส ธปท. สำนักงานภาคตะวันออกเฉียงเหนือ –  
ขอนแก่น
- 6.13 2535 - 2537
- รองผู้อำนวยการฝ่ายกำกับและตรวจสอบบริษัทเงินทุนหลักทรัพย์
- 6.14 2533 - 2535
- รองผู้อำนวยการฝ่ายกำกับและตรวจสอบธนาคารพาณิชย์
- 6.15 2528 - 2533
- หัวหน้าสำนักงานตรวจสอบธนาคารพาณิชย์ด้านคอมพิวเตอร์
- 6.16 2523 - 2528
- หัวหน้าผู้ตรวจสอบฝ่ายกำกับและตรวจสอบธนาคารพาณิชย์
- 6.17 2518 - 2523
- ผู้ตรวจสอบฝ่ายกำกับและตรวจสอบธนาคารพาณิชย์
- 6.18 2510 - 2518
- ผู้ช่วยผู้ตรวจสอบฝ่ายกำกับและตรวจสอบธนาคารพาณิชย์
- 6.19 2508 - 2510
- สมุหบัญชี บริษัท คอลลินส์ เบริโอ จำกัด
- 6.20 2507 - 2508
- พนักงานบัญชี บริษัท สยามกลการ จำกัด

## 7. ประวัติการบรรยาย

- ธนาคารแห่งประเทศไทย
- การไฟฟ้านครหลวง
- การไฟฟ้าส่วนภูมิภาค
- การไฟฟ้าฝ่ายผลิต
- บมจ.ทีโอที
- บมจ. กสท โทรคมนาคม
- ม.จุฬาลงกรณ์
- ม.ธรรมศาสตร์
- ม. เชียงใหม่
- ม.สงขลานครินทร์
- ม.ขอนแก่น
- ม. มหาสารคาม
- ธ.ออมสิน
- ธ.เกษตรเพื่อสหกรณ์การเกษตร
- ธ.ธนชาติ
- ธ.กสิกรไทย
- ธ.อาคารสงเคราะห์
- ธ.ไทยเครดิตเพื่อรายย่อย
- ธ.เพื่อการส่งออกและนำเข้าแห่งประเทศไทย
- องค์การคลังสินค้า
- สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม
- องค์การจัดการน้ำเสีย
- การประปานครหลวง
- การประปาส่วนภูมิภาค
- องค์การสวนยาง
- ปตท
- บริษัทวิทยุการบินแห่งประเทศไทย จำกัด

- การทางพิเศษแห่งประเทศไทย
- กระทรวงการคลัง
- ทริส
- สมาคมผู้ตรวจสอบภายใน แห่งประเทศไทย
- โรงงานยาสูบ
- การทำเรือแห่งประเทศไทย
- บริษัทประกันสินเชื่อบุคคลสหกรณ์ขนาดย่อม
- บมจ.การบินไทย
- การเคหะแห่งชาติ
- การนิคมอุตสาหกรรม
- Acis Professional Center [ CDIC]
- ISACA
- Nectec
- Softwarepark
- AIT
- South East Asian Central Bank [SEACEN] Malaysia
- South East Asian Central Bank [SEACEN] Indonesia
- South East Asian Central Bank [SEACEN] Nepal
- South East Asian Central Bank [SEACEN] Srilanka
- บ. Oracle
- บ. SAS
- บริษัทขนส่ง จำกัด
- การรถไฟแห่งประเทศไทย
- บริษัทท่าอากาศยานไทย จำกัด (มหาชน)
- สถาบันการบินพลเรือน
- องค์การตลาดเพื่อการเกษตร
- องค์การส่งเสริมกิจการโคนมแห่งประเทศไทย
- บ.ศรีอยุธยาประกันภัย จำกัด (มหาชน)
- บ.ไทยคาร์ดีฟประกันภัย จำกัด

8. สถานที่ติดต่อ

992 - 993 ถนน นวมินทร์ 14 แยก 7 แขวงคลองจั่น

เขต บางกะปิ กรุงเทพฯ 10240

โทร. 02-3777276, 02-7347814-15, 086-3333413, 081-8555921 แฟกซ์ 02-3751326

E-mail : [suvasarn@gmail.com](mailto:suvasarn@gmail.com), [methasuvasarn@yahoo.com](mailto:methasuvasarn@yahoo.com)