บทที่ 2
แนวคิด ทฤษฎี ผลงานวิจัยที่เกี่ยวข้อง

การวิจัยเรื่องศึกษาองค์ประกอบการบริหารจัดการเทคโนโลยีสารสนเทศตามกรอบงาน COBIT 5 จะเป็นสะท้อนมุมมองการกำกับดูแล การวางแผน การจัดหาหรือสร้างระบบสารสนเทศ การส่งมอบ สนับสนุนการบริการ และการติดตาม ควบคุม ดูแลทางด้านเทคโนโลยีของผู้ปฏิบัติงานระบบสารสนเทศทางการเงินและบัญชีของหน่วยงานภาครัฐ นอกจากนั้น ยังเป็นการศึกษาความคิดเห็นของผู้ใช้งานระบบสารสนเทศที่ให้ความสำคัญต่อด้านกระบวนการบริหารเทคโนโลยีสารสนเทศทางการเงินและบัญชีของหน่วยงานภาครัฐส่วนกลางและส่วนภูมิภาค โดยผู้วิจัยได้ทำการค้นคว้าแนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้องกับกระบวนการบริหารเทคโนโลยีสารสนเทศตามกรอบงาน COBIT 5 และการควบคุมการใช้งานระบบสารสนเทศทางการเงินและบัญชี ดังนี้

2.1 แนวคิดเรื่องการควบคุมทั่วไปของระบบสารสนเทศทางบัญชี

การควบคุมทั่วไปของระบบสารสนเทศ เป็นควบคุมที่มีความเกี่ยวข้องกับสภาพแวดล้อมของการควบคุมภายใน (Internal control environment) ในด้านนโยบายและวิธีการควบคุมระบบสารสนเทศ แบ่งหน้าที่ส่วนงาน รวมทั้งวิธีการปฏิบัติงานของเจ้าหน้าที่ที่มีความเกี่ยวข้องกับระบบ ซึ่งเป็นการควบคุมภายในขององค์กร หรือควบคุมส่วนที่มีความเกี่ยวข้องกับระบบสารสนเทศ โดยมีวัตถุประสงค์สร้างความมั่นใจว่าระบบคอมพิวเตอร์โดยรวมขององค์กรมีเสถียรภาพมีระบบการจัดการสารสนเทศที่ดี (พลพธู ปียวรรณและกัญนิภัทธ์ นิธิโรจน์ธนัท, 2558) นอกจากนั้น ช่วยป้องกันภัยคุมคามทางระบบสารสนเทศทางการบัญชี โดยมีการควบคุมขั้นพื้นฐานเป็นหลัก ถ้ามีการควบคุมทั่วไปไม่รัดกุมอย่างเพียงพอ ย่อมส่งผลกระทบต่อการควบคุมเฉพาะระบบด้วยเช่นกัน หลักการควบคุมทั่วไปประกอบด้วยการควบคุม 9 ด้าน และแต่ละด้านจะต้องมีการควบคุม เพื่อให้ผู้ใช้งานเกิดความมั่นใจในการใช้งานระบบ มีดังนี้

1. การควบคุมระบบปฏิบัติการ

เป็นหน้าที่สำคัญของผู้ดูแลระบบ (System administrator) ควรทราบถึงการทำงานของระบบต่างๆ และหลักการควบคุมการเข้าใช้งานระบบปฏิบัติการที่เกี่ยวข้องกับระบบสารสนเทศทางการบัญชี เพื่อป้องกันความเสี่ยงหรือภัยคุกคามต่อระบบสารสนเทศทางการบัญชี (คณะกรรมการกลุ่มผลิตชุดวิชาเทคโนโลยีสารสนเทศสำหรับการบัญชีการเงินและการบัญชีเพื่อการจัดการ, 2555) สิ่งเหล่านี้ ขึ้นอยู่กับนโยบายการรักษาความปลอดภัย กระบวนการทำงาน และระบบการควบคุมการเข้าใช้งานในระบบ (อรุษ คงรุ่งโชค, 2551) โดยแบ่งเป็น

1.1 ควบคุมการให้สิทธิ์ในการเข้าถึง (Controlling Access Privilege) ต้องมีการบันทึกข้อมูลการให้สิทธิในการเข้าระบบของผู้ใช้งานแต่ละคน หรือกลุ่มผู้ใช้งาน ในแต่ละระบบงาน และผู้ดูแลระบบจะต้องมีการควบคุมโดยมีเครื่องคอมพิวเตอร์สำหรับการใช้งานเรื่องการบริหารจัดการสิทธิ์การเข้าใช้งานระบบ (คณะกรรมการกลุ่มผลิตชุดวิชาเทคโนโลยีสารสนเทศสำหรับการบัญชีการเงินและการบัญชีเพื่อการจัดการ, 2555) และมีการควบคุมการให้สิทธิ์ โดยใช้การควบคุมการเข้าใช้งานแบบเมตริก (Access Control Matrix) ตามรูปแบบดังนี้

ตารางที่ 2.1 ตารางควบคุมการให้สิทธิ์การเข้าถึงเอกสาร และระบบปฏิบัติการแบบเมตริก (Access Control Matrix) (Romney and Steinbart, 2015)

User	**File**			**Program**			
User ID	**A**	**B**	**C**	**1**	**2**	**3**	**4**
NHale	0	0	1	0	0	0	0
JPJone	0	2	0	0	0	0	1
BArnold	1	1	0	1	1	0	0

Codes for File Access:

0 = No Access

1 = Read/display only

2 = Read/display and update

3 = Read/display, update, create and delete

Codes for Program Access:

0 = No Access

1 = Execute

จากตารางดังกล่าว แสดงให้เห็นว่า รหัสผู้ใช้งานแต่ละคนมีสิทธิการเข้าถึงข้อมูลรายงานและการใช้การทำงานในระบบปฏิบัติการไม่เหมือนกัน เพื่อป้องกันล่วงรู้ข้อมูลของผู้ไม่มีสิทธิในการเข้าใช้งานในระบบได้ นอกจากนั้น สามารถนำไปประยุกต์ใช้ในการรักษาความปลอดภัยในการเข้าใช้งานอุปกรณ์อิเล็กทรอนิกส์ และเป็นส่วนหนึ่งของเพิ่มความปลอดภัยของการป้องกันข้อมูลเชิงลึก (Romney and Steinbart, 2015)

1.2 การควบคุมด้วยรหัสผ่าน (Password Control)

การเข้าใช้งานระบบปฏิบัติการ โดยส่วนใหญ่นิยมใช้รหัสผ่าน เป็นเครื่องมือในการตรวจสอบสิทธิ์ในการเข้าถึงระบบงานแฟ้มข้อมูล รายงาน (อรุษ คงรุ่งโชค, 2551) ซึ่งการใช้รหัสผ่าน (Password) หรือตัวเลขเฉพาะส่วนบุคคล (Personal Identification Numbers : PINs) เป็นวิธีการพิสูจน์ตัวตนที่สะดวกต่อการใช้งาน แต่มีความเสี่ยงต่อการสูญหาย หรือ การเผยความลับให้บุคคลอื่นล่วงรู้ (Romney and Steinbart, 2015) จะต้องผ่านกระบวนการ ดังต่อไปนี้

1.2.1 กระบวนการการเข้าใช้งานระบบสารสนเทศทางบัญชี (Log onProcedure)

เป็นขั้นตอนแรกของการเข้าใช้งานระบบ โดยใช้รหัสผู้ใช้งานและรหัสผ่านในการใช้งานระบบสารสนเทศทางบัญชี และในขณะเดียวกันรหัสผู้เข้าใช้งานหรือรหัสผ่านไม่ถูกต้อง ระบบจะทำการแจ้งเตือนไปยังผู้มีสิทธิในการใช้งานได้รับทราบปัญหา (Jame A. Hall, 2011) หรือผู้ใช้งานใส่รหัสผ่านไม่ถูกต้อง ระบบจะทำการปฏิเสธการเข้าถึง (คณะกรรมการกลุ่มผลิตชุดวิชาเทคโนโลยีสารสนเทศสำหรับการบัญชีการเงินและการบัญชีเพื่อการจัดการ, 2555)

1.2.2 กระบวนการเข้าใช้งานอุปกรณ์ (Access Token)

หลังจากเข้าระบบปฏิบัติได้แล้ว Access Token เป็นข้อมูลสำคัญเกี่ยวกับผู้มีสิทธิในการเข้าใช้งานระบบรวมทั้ง รหัสผู้ใช้งาน รหัสผ่าน กลุ่มผู้ใช้งาน นอกจากนั้น ผู้มีสิทธิใน Access Token สามารถทำการใช้งานระบบได้ (Jame A. Hall, 2011)

1.2.2.1 รหัสผ่านที่สามารถใช้ซ้ำได้ ซึ่งผู้ดูแลระบบหรือผู้ใช้งานสามารถกำหนดรหัสผ่านในการเข้าใช้งานระบบ ในขณะเดียวกันผู้ดูแลระบบควรตรวจสอบตารางที่เก็บรหัสผ่านอัตโนมัติ พร้อมแจ้งเตือนให้ผู้ใช้งานทราบกำหนดการเปลี่ยนรหัสผ่าน ซึ่งการสร้างรหัสผ่านที่ดี มีความมั่นคง และป้องกันการถูกเจาะข้อมูล มีดังนี้

1.2.2.2 ความยาวของรหัสผ่าน ควรใช้รหัสผ่านที่มีความยาวมาก และง่ายต่อการจดจำ

1.2.2.3 รูปแบบลักษณะของรหัสผ่าน ควรมีทั้งตัวเลข ตัวอักษรภาษาอังกฤษพิมพ์เล็ก พิมพ์ใหญ่ และอักษรลักษณะพิเศษ ทำให้รหัสผ่านมีความแข็งแรงมั่นคงมากขึ้น

1.2.2.4 การสุ่มรหัสผ่าน รหัสผ่านที่ดีไม่ควรเป็นคำที่ผู้คนจดจำได้ง่าย อย่างเช่น คำที่อยู่ในพจนานุกรม เป็นต้น ควรเป็นรหัสผ่านที่เกี่ยวกับสิ่งที่สนใจ หรือ งานอดิเรกของผู้ใช้งานที่ไม่ได้บอกใคร

1.2.2.5 ความถี่ในการเปลี่ยนรหัสผ่าน ควรเปลี่ยนรหัสผ่านอย่างน้อย 90 วัน

1.2.2.6 การเก็บรักษาความลับ รหัสผ่านที่ดีควรเก็บเป็นความลับ โดยการจดเก็บไว้ในสมุดหรือที่ซ่อนที่ผู้ใช้งานหาได้สะดวก และไม่ควรเปิดเผยให้ผู้ใช้งานคนอื่นได้รับรู้ (Romney and Steinbart, 2015)

1.2.2.7 รหัสผ่านครั้งเดียว (One time password) จะสามารถใช้งานได้ในกรณีผู้ใช้งานลืมรหัสผ่านที่เข้าใช้งานระบบ หรือมีบุคคลอื่นแอบมาใช้รหัสผ่านเข้าระบบ รหัสผ่านแบบนี้สามารถใช้งานได้แค่ 1 ครั้งเท่านั้น จึงต้องมีการเปลี่ยนแปลงรหัสผ่านอยู่ตลอดเวลาโดยไม่ซ้ำกัน และไม่สามารถนำรหัสผ่านนี้มาใช้งานได้อีก เนื่องจากมีระยะเวลากำหนดที่ชัดเจน

นอกจากมีการกำหนดรหัสผ่านการเข้าใช้งานระบบ และแฟ้มข้อมูลภายในแล้ว องค์กรควรมีการกำหนดให้มีการรักษาความปลอดภัยในการเข้าถึงข้อมูลของบุคคลภายนอกที่มีหน้าที่เกี่ยวข้องกับองค์กร อย่างเช่น ผู้สอบบัญชี หรือผู้พัฒนาระบบงาน เป็นต้น โดยองค์กรจะให้อนุญาตบุคคลเหล่านี้สามารถเข้าถึงข้อมูลในระบบเฉพาะรายการเท่านั้น ส่วน อุปกรณ์ระยะไกล ได้แก่ เครื่องเทอร์มินอล หรือคอมพิวเตอร์ที่เข้าใช้งานระบบสารสนเทศทางบัญชี ควรมีการกำหนดให้มีระบบการรักษาความปลอดภัย โดยให้เจ้าหน้าที่ที่ได้รับอุปกรณ์ดังกล่าวรับผิดชอบดูแลรักษาอุปกรณ์ให้อยู่สถานที่ปลอดภัย รวมทั้งการยืนยันตัวตนผู้ใช้งาน ถ้าพบว่าอุปกรณ์สูญหาย หรือมีการเปลี่ยนแปลงข้อมูลในระบบโดยไม่รับอนุญาต เจ้าหน้าที่ที่ดูแลอุปกรณ์จะต้องรับผิดชอบในความเสียหายที่เกิดขึ้น (วัชนีพร เศรษฐสักโก, 2560)

2.2 แนวคิดเรื่อง กรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร (COBIT)

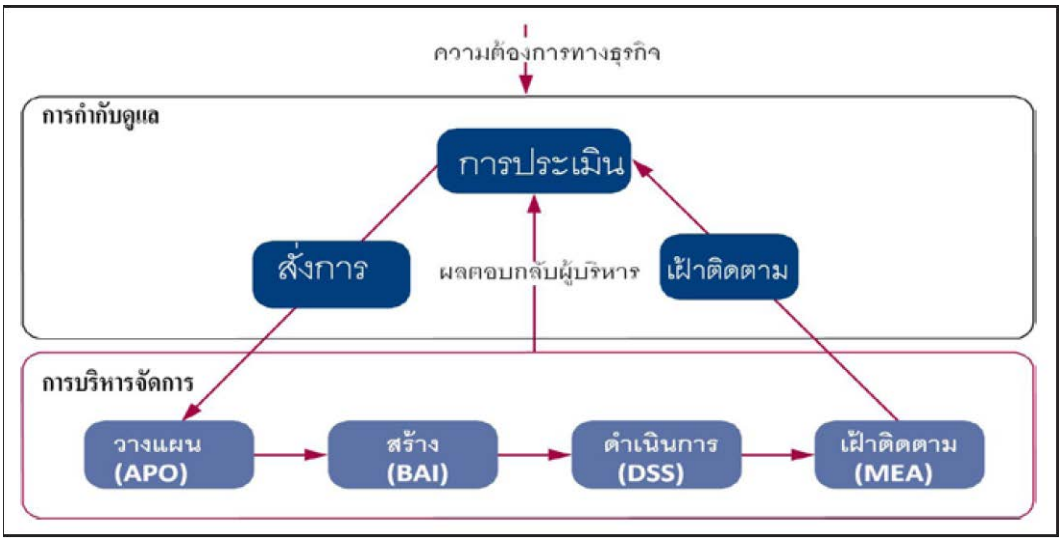
กรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร ตามวัตถุประสงค์การควบคุมภายในด้านสารสนเทศและเทคโนโลยีที่เกี่ยวข้อง(Control Objectives for Information and related Technology : COBIT) เป็นกรอบงานการดำเนินงานสำหรับหลักธรรมาภิบาลและ การบริหารจัดการด้านเทคโนโลยีสารสนเทศที่ได้รับการยอมรับทั่วไป และ COBIT5 เป็นกรอบการดำเนิน COBIT รุ่นล่าสุด เกิดจากการปรับปรุงกรอบการดำเนินของ COBIT 4.1 โดยนำกรอบการดำเนินการกำกับดูแลเทคโนโลยีสารสนเทศมีบูรณาการร่วมกัน อย่างเช่น มาตรฐานสากลของ ISO, ISACA's Val IT และRisk IT และมาตรฐาน ITIL เป็นต้น (Richardson, Chang and Smith, 2017) ในขณะเดียวกันกรอบการดำเนิน COBIT มีการแบ่งแยกระหว่างการกำกับดูแลองค์กรกับการจัดการด้านเทคโนโลยีสารสนเทศ ซึ่ง COBIT 5 มีการอธิบายความแตกต่างของการกำกับดูแลองค์กรและการบริหารจัดการ ดังนี้

กระบวนการการกำกับดูแลองค์กร (Governance Process) เป็นกระบวนงานที่มีการเชื่อมโยงกับวัตถุประสงค์ของการกำกับดูแลผู้มีส่วนได้ส่วนเสีย ได้แก่ การส่งมอบคุณค่า (Value Delivery), การบริหารจัดการความเสี่ยงที่เหมาะสม (Risk Optimization) และการบริหารจัดการทรัพยากรในองค์กรอย่างเหมาะสม (Resource Optimization) รวมทั้งแนวทางและกิจกรรมในกลยุทธ์การประเมินผลด้านเทคโนโลยีสารสนเทศ

กระบวนการการบริหารจัดการ (Management Process) เป็นกระบวนการด้านการบริหารจัดการเทคโนโลยีสารสนเทศภายใต้ความรับผิดชอบของการวางแผน (Plan), การสร้าง (Build), การดำเนินการ (Run) และการติดตาม (Monitor) หรือ การบริหารเทคโนโลยีสารสนเทศแบบ PBRM (ISACA, 2012)

องค์ประกอบการกำกับดูแลและการบริหารจัดการเชิงเทคโนโลยีสารสนเทศ

กรอบของโคบิต 5 ได้แสดงแผนผังการทำงานของกระบวนงานด้านการกำกับดูแล และการบริหารจัดการเชิงเทคโนโลยีสารสนเทศ เพื่อองค์กรนำแผนผังดังกล่าวมาใช้งานด้านการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ดังภาพแผนผังต่อไปนี้



ภาพที่ 2.1 แผนผังความสัมพันธ์ระหว่างการกำกับดูแลและการบริหารจัดการ (ISACA, 2012)

นอกจากนั้น กรอบของ COBIT 5 ได้มีการกำหนดกระบวนการต่าง ๆ ในด้านการกำกับดูแล และการบริหารจัดการเทคโนโลยีสารสนเทศ ได้มีการอ้างอิงกระบวนการทำงานมาจากหลักการของ COBIT 4.1 มาใช้ในการกำหนดกระบวนการควบคุมกำกับดูแลเทคโนโลยีสารสนเทศระดับขององค์กร ซึ่งบางกระบวนการที่มีการแบ่งแยก เพื่อกำหนดแนวทางกิจกรรมการบริหารจัดการเทคโนโลยีสารสนเทศเฉพาะเจาะจงมากขึ้น (Loai Al Omari, Paul Barnes and Grant Pitman, 2012) นอกจากนั้น COBIT 5 มีการปรับปรุงกระบวนการให้เหมาะสมกับการใช้งานขององค์กรได้ดังต่อไปนี้

การปรับเปลี่ยนกระบวนการจาก 4 กระบวนการ มาเป็น 5 กระบวนการ มีการเพิ่มกระบวนการด้านการกำกับดูแลองค์กรมาเป็นส่วนหนึ่งของกระบวนการควบคุมกำกับดูแลเทคโนโลยีสารสนเทศ

1. มีการเปลี่ยนรหัสกระบวนการจาก 2 ตัว มาเป็น 3 ตัว ดังนี้

   1.1 EDM (Evaluation, Direct and Monitor)

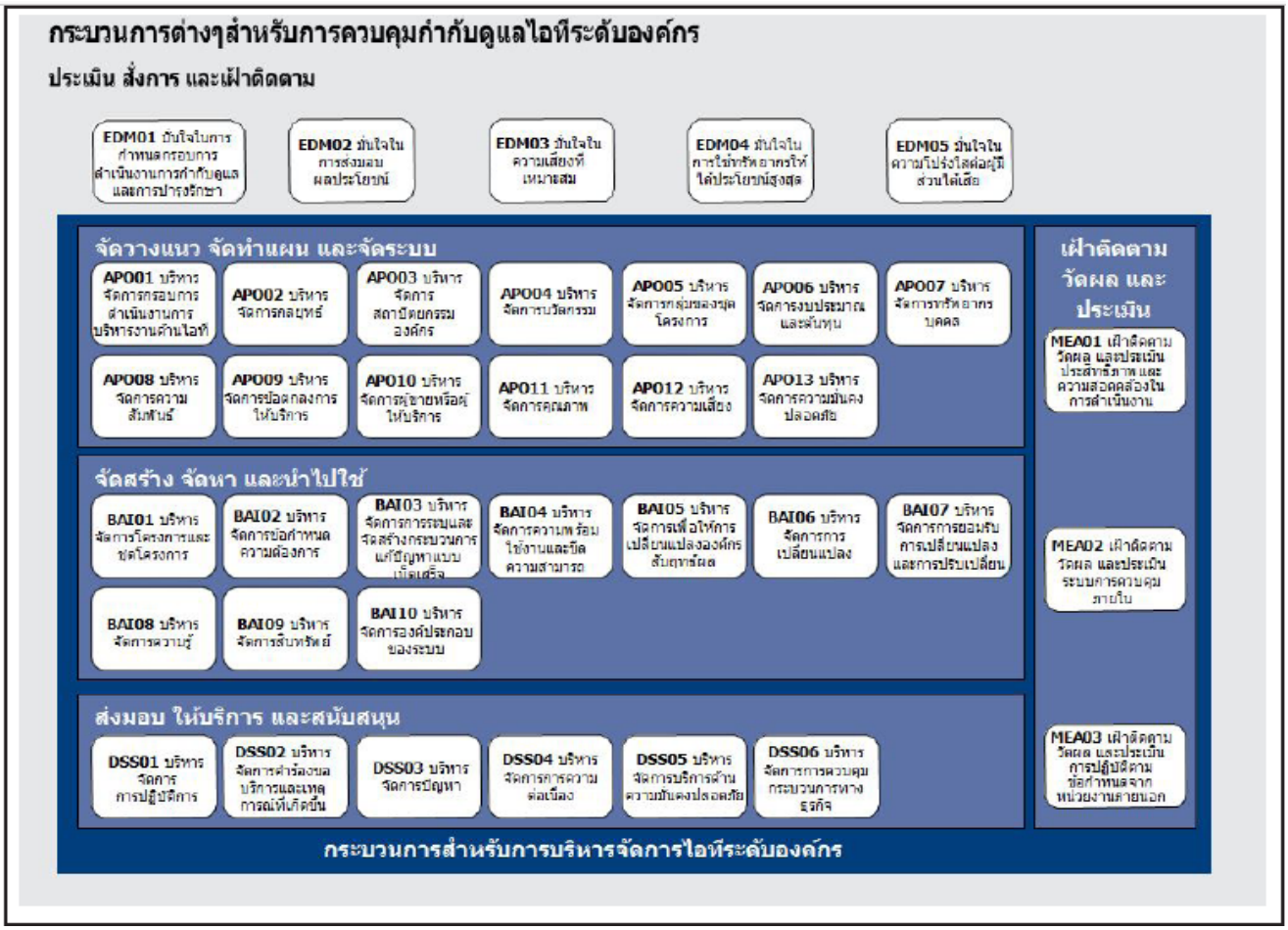
   1.2 APO (Align, Plan and Organize)

   1.3 BAI (Build, Acquire and Implement)

   1.4 DSS (Deliver, Service and Support)

   1.5 MEA (Monitor, Evaluation and Access)

2. มีการเพิ่มกระบวนงานบริหารจัดการจาก 34 กระบวนงาน มาเป็น 37 กระบวนงาน



ภาพที่ 2.2 โครงสร้างกระบวนการสำหรับการกำกับดูแล และการบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร (ISACA, 2012)

กรอบการดำเนินงานโคบิตมีกระบวนงานด้านการกำกับดูแลเทคโนโลยีสารสนเทศและด้านการบริหารจัดการมีการแบ่งตามกิจกรรม จำนวน 5 กระบวนงานหลัก คือ การกำกับดูแล (EDM), การวางแผน (Planning), การสร้าง (Building), การดำเนินงาน (Running) และการติดตาม (Monitoring) ซึ่งผู้บริหารจะเป็นคนวางแนวทางปฏิบัติให้สอดคล้องกับวัตถุประสงค์ของหน่วยงานในด้านการเทคโนโลยีสารสนเทศให้ประสบผลสำเร็จ และบรรลุตามเป้าหมายที่ได้กำหนดไว้ ซึ่งหลักการควบคุมมีดังนี้

1. การกำกับดูแล (Governance: EDM) แบ่งเป็น การประเมิน (Evaluation), การสั่งการ (Direct) และการติดตาม (Monitor) มี 5 กระบวนการ ดังนี้

1.1 EDM01 มั่นใจในการกำหนดกรอบการดำเนินงานการกำกับดูแลและการบำรุงรักษา

เป็นการให้ความเชื่อมั่นในการกำหนดกรอบการดำเนินงานของระบบสารสนเทศทางการเงินและบัญชีภาครัฐ ซึ่งหน่วยงานส่วนกลางที่จัดทำระบบจะต้องกำหนดกรอบการดูแลระบบสารสนเทศทางการเงินและบัญชี ตามขอบเขตที่ได้มีการกำหนดไว้ รวมทั้งการบำรุงรักษาระบบ, เครื่องเทอร์มินอล และอุปกรณ์การเข้าใช้งานระบบสารสนเทศทางการเงินและบัญชีของหน่วยงานภาครัฐ ให้สามารถปฏิบัติงานด้านการเงินการคลังได้อย่างต่อเนื่อง ให้ครอบคลุมกับการทำงานของหน่วยงานภาครัฐแต่ละแห่งให้เป็นไปตามความต้องการของผู้ใช้งานระบบอย่างแท้จริง

1.2 EDM02 มั่นใจในการส่งมอบผลประโยชน์

เป็นให้ความเชื่อมั่นในเรื่องการจัดทำระบบสารสนเทศทางการเงินและบัญชีเพื่อช่วยในการดำเนินงานด้านการเงินการคลังภาครัฐของหน่วยงานภาครัฐมีความรวดเร็ว, ทันต่อเวลาและข้อมูลทางการเงินมีความถูกต้องครบถ้วนและเป็นปัจจุบัน ในขณะเดียวกันผู้รับบริการที่ใช้งานระบบทราบถึงข้อดีของระบบงาน เพื่อเป็นประโยชน์ต่อการนำไปใช้งานได้

1.3 EDM03 มั่นใจในความเสี่ยงที่เหมาะสม

ในการจัดทำระบบสารสนเทศทางการเงินและบัญชีภาครัฐจะต้องมีการวิเคราะห์ความเสี่ยงและแนวโน้มในการนำระบบสารสนเทศทางการเงินและบัญชีมาใช้ในหน่วยงานภาครัฐในอนาคต เพื่อกำหนดแนวทางและหลักการในการใช้งานระบบสารสนเทศทางการเงินและบัญชี ให้มีความรอบคอบ, รัดกุม, ปลอดภัย และเป็นไปตามหลักการควบคุมภายในที่ดีของหน่วยงานภาครัฐ ซึ่งผู้ใช้งานจะต้องรับรู้ปัญหาในการใช้งานระบบ เพื่อให้เจ้าหน้าที่สามารถนำปัญหาไปปรับปรุง

1.4 EDM04 มั่นใจในการใช้ทรัพยากรให้เกิดประโยชน์สูงสุด

เป็นการตรวจสอบและประเมินการใช้ทรัพยากรในการดำเนินงานสร้างระบบสารสนเทศทางการเงินและบัญชีภาครัฐ ให้มีความคุ้มค่าใน ด้านบุคลากร, ด้านความรู้ความสามารถด้านการเงินการคลัง, ด้านกระบวนการทำงานในระบบสารสนเทศให้มีความรัดกุม,เป็นไปตามหลักการควบคุมภายในของหน่วยงาน และความต้องการใช้งานของหน่วยงานภาครัฐ, ความพร้อมด้านการใช้งานเทคโนโลยีสารสนเทศจัดทำระบบสารสนเทศทางการเงินและบัญชีให้มีความคุ้มค่าและช่วยให้สามารถดำเนินงานได้ตามแผนที่ได้กำหนดไว้

1.5 EDM05 มั่นใจในความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย

เป็นการตรวจสอบสมรรถนะด้านเทคโนโลยีสารสนเทศของระบบ ให้มีความสอดคล้องกับสภาพการใช้งานระบบสารสนเทศทางการเงินและบัญชีของหน่วยงานภาครัฐ และเป้าหมายในการดำเนินงานด้านการเงินการคลังของหน่วยงานตามนโยบายรัฐบาลในปัจจุบัน ซึ่งประสิทธิภาพของการบริหารจัดการทางระบบสารสนเทศทางการเงินและบัญชีภาครัฐนั้นด้านความโปร่งใสผู้บริหารและผู้ที่มีส่วนเกี่ยวข้องกับระบบสารสนเทศทางการเงินและบัญชีภาครัฐนั้นสามารถตรวจสอบการทำงานทุกขั้นตอน และใช้งานระบบได้ (ภิรมย์พร เยาดำ, 2559)

2. การวางแผน (Plan: APO) แบ่งเป็น การวางแนวทาง (Align), การวางแผน (Plan) และการจัดการองค์กร (Organize) มีทั้งหมด 13 กระบวนงาน ดังนี้

2.1 APO01 บริหารจัดการกรอบการดำเนินงานด้านบริหารงานด้าน IT

เป็นการชี้แจงและรักษาหลักการกำกับดูแลด้านเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงการคลัง, กรมบัญชีกลาง และหน่วยงานภาครัฐ รวมทั้งกลไกการทำงานในการบริหารจัดการข้อมูลการเงินการคลัง และการใช้เทคโนโลยีสารสนเทศของหน่วยงาน โดยสนับสนุนวัตถุประสงค์ให้สอดคล้องกับหลักการและนโยบายในด้านสิทธิการเข้าใช้งานระบบสารสนเทศทางการเงินและบัญชี

2.2 APO02 บริหารจัดการกลยุทธ์

สำนักงานปลัดกระทรวงการคลังและกรมบัญชีกลางสามารถกำหนดทิศทางในการสร้างและพัฒนาระบบสารสนเทศทางการเงินและบัญชีภาครัฐ โดยมีการประเมินสภาพแวดล้อมและความสามารถของบุคลากรในหน่วยงานภาครัฐ ใช้ในการกำหนดเทคโนโลยีที่ต้องการนำมาและแผนการดำเนินงานสร้างระบบสารสนเทศทางการเงินและบัญชีภาครัฐ ให้มีความสอดคล้องกับนโยบายของรัฐบาลด้านการเงินการคลังภาครัฐในปัจจุบัน

2.3 APO03 บริหารจัดการสถาปัตยกรรมองค์กร

สำนักงานปลัดกระทรวงการคลังและกรมบัญชีกลางจะมีการสร้างโครงสร้างการเข้าใช้งานระบบและรูปแบบการทำงานในระบบสารสนเทศทางการเงินและบัญชีของหน่วยงานภาครัฐ โดยอ้างอิงกฎระเบียบและหนังสือเวียนที่ได้กำหนดการใช้งานระบบสารสนเทศทางการเงินและบัญชีภาครัฐไว้

2.4 APO04 บริหารจัดการนวัตกรรม

เป็นการนำความรู้ทางเทคโนโลยีสารสนเทศของหน่วยงานและแนวโน้มการให้บริการระบบสารสนเทศทางการเงินและบัญชีภาครัฐ รวมทั้งวิเคราะห์โอกาสและประโยชน์ที่ได้รับจากการทำนวัตกรรม มาใช้ในการวางแผนจัดทำนวัตกรรมในการสร้างระบบมาช่วยอำนวยความสะดวกในการทำงานของเจ้าหน้าที่ผู้ให้บริการหรือ การปรับปรุงกระบวนการทำงานของระบบสารสนเทศให้มีประสิทธิภาพมากยิ่งขึ้น และผู้รับบริการสามารถใช้งานได้สะดวก

2.5 APO05 บริหารจัดการกลุ่มของชุดโครงการ

ผู้บริหารระดับสูงจะทำการทบทวนและกำหนดเป้าหมายในการพัฒนาระบบสารสนเทศทางการเงินและบัญชีภาครัฐ รวมทั้งการให้บริการแก่หน่วยงานภาครัฐให้มีความชัดเจน รวมทั้ง กำหนดวิธีการในการจัดซื้อจัดจ้างหาผู้ทำระบบสารสนเทศได้อย่างเหมาะสม,มีความเป็นธรรมและเป็นไปตามหลักการในพระราชบัญญัติการจัดซื้อจัดจ้าง พ.ศ. 2560

2.6 APO06 บริหารจัดการงบประมาณและต้นทุน

เป็นการบริหารจัดการกิจกรรมทางการเงินและต้นทุนในการจัดทำระบบสารสนเทศทางการเงินและบัญชีภาครัฐ โดยหน่วยงานภาครัฐที่จัดสร้างระบบเป็นผู้ดำเนินงานด้านการจัดซื้อจัดจ้างการทำระบบ และอุปกรณ์คอมพิวเตอร์ รวมทั้งเป็นผู้ดูแลเรื่องสิทธิการเข้าใช้งานและขั้นตอนการใช้งานระบบสารสนเทศทางการเงินและบัญชีภาครัฐ ให้มีประสิทธิภาพ และช่วยประหยัดต้นทุนในการใช้ทรัพยากรในหน่วยงานภาครัฐให้คุ้มค่ากับเงินงบประมาณที่ได้จัดทำระบบ

2.7 APO07 บริหารจัดการทรัพยากรบุคคล

เป็นการบริหารจัดการสรรหาบุคลากรตรงตามตำแหน่งที่ต้องการ,ความรู้ความสามารถด้านการเงินการคลัง และประสบการณ์การใช้งานระบบสารสนเทศทางการเงินและบัญชีของหน่วยงานภาครัฐ เพื่อให้ข้อมูลทางการเงินของหน่วยงานภาครัฐมีความถูกต้อง ครบถ้วน และผู้บริหารสามารถนำข้อมูลเหล่านี้มาใช้งานได้ นอกจากนั้น หน่วยงานผู้เป็นเจ้าของระบบสารสนเทศทางการเงินและบัญชีภาครัฐจะต้องมีการอบรมให้ความรู้เรื่องการใช้งานระบบสารสนเทศดังกล่าวแก่ผู้ปฏิบัติงานการเงินการคลังอย่างต่อเนื่อง และคอยแจ้งข่าวสารข้อมูล หรือการเปลี่ยนแปลงการทำงานของระบบให้ผู้รับบริการได้รับทราบ เพื่อป้องกันข้อผิดพลาดในการปฏิบัติงานในระบบ

2.8 APO08 บริหารจัดการความสัมพันธ์

เป็นบริหารด้านความสัมพันธ์ระหว่างการปฏิบัติงานของหน่วยงานภาครัฐและเทคโนโลยีสารสนเทศ ให้มีความโปร่งใส และเป็นไปตามกำหนดในการดำเนินงานด้านการเงินการคลังผ่านระบบสารสนเทศทางการเงินและบัญชีภาครัฐ โดยหน่วยงานได้ให้ความมั่นใจว่าการปฏิบัติงานด้านการเงินการคลังในระบบ GFMIS หรือระบบงานอื่น ๆ ที่เกี่ยวข้องทางด้านการเงินและบัญชีภาครัฐจะสามารถใช้งานได้อย่างต่อเนื่อง รวมทั้งกรมบัญชีกลางจะต้องมีการสื่อสารเรื่องหลักเกณฑ์การดำเนินงานระบบสารสนเทศทางการเงินและบัญชีภาครัฐช่วงสิ้นปีงบประมาณให้หน่วยงานได้รับทราบ และปฏิบัติตามหลักเกณฑ์ได้อย่างถูกต้อง

2.9 APO09 บริหารจัดการข้อตกลงการให้บริการ

การปรับระดับการบริการและการให้บริการด้านเทคโนโลยีสารสนเทศการใช้งานระบบสารสนเทศทางการเงินและบัญชีให้สอดคล้องกับความต้องการและความคาดหวังของหน่วยงานภาครัฐ รวมทั้ง การกำหนดข้อกำหนด, การออกแบบกระบวนการให้บริการ,การเผยแพร่คู่มือการใช้งาน และตรวจสอบการบริการด้านเทคโนโลยีสารสนเทศของเจ้าหน้าที่ผู้ให้บริการ โดยใช้ตัวชี้วัดประสิทธิภาพในการดำเนินงานด้านระบบสารสนเทศทางการเงินและบัญชีภาครัฐ ตามภารกิจได้รับมอบหมาย

2.10 APO10 บริหารจัดการผู้ขายหรือผู้ให้บริการ

หน่วยงานที่เป็นผู้ให้บริการระบบสารสนเทศทางการเงินจะให้บริการด้านการปฏิบัติงานระบบบริหารจัดการด้านการใช้งานระบบสารสนเทศกับหน่วยงานที่เกิดขึ้นใหม่ โดยจะต้องทำการติดต่อประสานงานกับหน่วยงานที่เกี่ยวข้อง และแจ้งปัญหาในการใช้งานระบบสารสนเทศทางการเงินและบัญชีภาครัฐให้บริษัทภายนอกที่เป็นผู้สร้างระบบได้รับทราบ และทำการปรับปรุงระบบการทำงานให้มีประสิทธิภาพมากขึ้น

2.11 APO11 บริหารจัดการคุณภาพ

หน่วยงานภาครัฐที่เป็นเจ้าของระบบสารสนเทศทางการเงินและบัญชีภาครัฐมีการกำหนดกระบวนการการให้บริการการใช้งานระบบให้เป็นไปตามหลักปฏิบัติการบริหารจัดการคุณภาพที่ดีขององค์กร หรือ PMQA และมีการตรวจสอบความถูกต้องของข้อมูลแบบฟอร์มเอกสารคำร้องใช้บริการของหน่วยงานภาครัฐตามที่หน่วยงานภาครัฐที่เป็นเจ้าของระบบได้กำหนดไว้ในขั้นตอนการขอใช้บริการระบบสารสนเทศทางการเงินและบัญชีภาครัฐให้เป็นไปตามแนวทางการควบคุมภายในที่ดีของหน่วยงานภาครัฐ

2.12 APO12 บริหารจัดการความเสี่ยง

หน่วยงานภาครัฐมีการระบุและประเมินความเสี่ยงการนำระบบสารสนเทศทางเงินและบัญชีภาครัฐมาใช้ในการบริหารการเงินการคลังภาครัฐ เพื่อสามารถกำหนดหลักการควบคุมความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศทางการเงินและบัญชีภาครัฐ ซึ่งหน่วยงานจะต้องมีการทบทวนกระบวนการให้บริการของหน่วยงานและประเมินการควบคุมภายในด้านการบริการระบบสารสนเทศทางการเงินและบัญชีภาครัฐเป็นประจำทุกปี เพื่อนำปัญหาที่พบ

ดังกล่าวมาปรับปรุงประสิทธิภาพในการให้บริการและการทำงานของระบบสารสนเทศให้ดียิ่งขึ้น

2.13 APO13 บริหารจัดการความมั่นคงปลอดภัย

การกำหนดการใช้งานและตรวจสอบระบบเพื่อจัดการข้อมูลสารสนเทศ ซึ่งหน่วยงานที่เป็นเจ้าของระบบสารสนเทศได้กำหนดวิธีการบันทึกรายการข้อมูลในระบบสารสนเทศทางการเงินและบัญชีภาครัฐและ ผู้มีสิทธิในการเข้าเอกสารและระบบการทำงานตามลำดับชั้นการดำเนินงานทางการเงินคลัง ให้สอดคล้องกับหลักการควบคุมภายในที่ดีของหน่วยงานภาครัฐ นอกจากนั้นหน่วยงานที่เป็นเจ้าของระบบสารสนเทศทางการเงินและบัญชีภาครัฐจะต้องดำเนินการเกี่ยวกับอุปกรณ์การเข้าใช้งานระบบ การสร้างคลังข้อมูล รวมทั้ง ออกแบบระบบการรักษาความปลอดภัยเพื่อป้องกันการโจรกรรมข้อมูลจากภายนอก หรือการเกิดเหตุการณ์ภัยทางธรรมชาติ เพื่อให้ระบบสามารถให้บริการได้อย่างต่อเนื่อง

3. การสร้าง (Build: BAI) แบ่งเป็น การสร้าง (Build), การจัดหา (Acquire) และการนำไปใช้ (Implement) มี 10 กระบวนงาน ดังนี้

3.1 BAI01 บริหารจัดการโครงการและชุดโครงการ

เป็นการจัดการโครงการและโปรแกรมจากข้อมูลค่าใช้จ่ายในการจัดทำระบบสารสนเทศทางการเงินและบัญชีภาครัฐของหน่วยงานภาครัฐที่เป็นเจ้าของระบบสารสนเทศทางการเงินและบัญชีภาครัฐ ให้เป็นไปตามนโยบายของคณะรัฐมนตรีในด้านการบริหารการจัดการการเงินการคลังแบบอิเล็กทรอนิกส์ และแนวทางด้านเทคโนโลยีสารสนเทศ เพื่อพัฒนาประเทศไทยให้อยู่ในยุคประเทศไทย 4.0

3.2 BAI02 บริหารจัดการข้อกำหนดความต้องการ

เป็นการระบุความต้องการการใช้งานระบบสารสนเทศของหน่วยงานภาครัฐ โดยมีการประสานงาน, ติดต่อและส่งหนังสือมาที่กรมบัญชีกลางในกรณีที่มีการเพิ่มและยุบหน่วยงาน, หน่วยเบิกจ่าย และศูนย์ต้นทุน รวมทั้งการเปลี่ยนแปลงชื่อหน่วยงานและศูนย์ต้นทุนให้สอดคล้องกับข้อมูลของกฎกระทรวงที่มีการประกาศใช้ รวมทั้ง สถานที่ตั้ง และช่องทางในการใช้งานระบบสารสนเทศทางการเงินและบัญชีภาครัฐของหน่วยงาน

3.3 BAI03 บริหารจัดการระบุและจัดสร้างกระบวนการแก้ปัญหาแบบเบ็ดเสร็จ

เป็นการกำหนดวิธีการแก้ไขปัญหาระบบสารสนเทศทางการเงินและบัญชีภาครัฐในด้านการใช้งานระบบ, ขั้นตอนการให้บริการ ด้านสิทธิการเข้าใช้งาน และปัญหาเรื่องของอุปกรณ์การเข้าใช้งานระบบ เพื่อให้การดำเนินงานด้านการเงินการคลังของหน่วยงานได้อย่างต่อเนื่อง รวมทั้งกำหนดหลักเกณฑ์การใช้งานระบบและเครือข่ายอินเทอร์เน็ตที่ใช้ในการทำงานเพื่อความปลอดภัยในการใช้งานระบบของหน่วยงานของรัฐ

3.4 BAI04 บริหารจัดการความพร้อมใช้งานและขีดความสามารถ

หน่วยงานที่เป็นเจ้าของระบบสารสนเทศทางการเงินและบัญชีภาครัฐควรมีการปรับปรุงกระบวนการบริการและการใช้งานระบบสารสนเทศอยู่สม่ำเสมอ พร้อมทั้งเก็บสถิติข้อมูลการให้บริการในแต่ละเดือน มาใช้ในการปรับปรุงการให้บริการให้ดียิ่งขึ้น และตรงตามความต้องการของผู้รับบริการ

3.5 BAI05 บริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล

ระบบสารสนเทศทางการเงินและบัญชีภาครัฐในปัจจุบัน มีการปรับเปลี่ยนด้านระบบการทำงานและขั้นตอนต่างๆ อย่างเช่น การรับเงิน, ชำระเงินและรับนำส่งเงินงบประมาณโดยใช้ระบบสารสนเทศอื่น ๆ มาช่วยในการดำเนินงานด้านธุรกรรมทางการเงินของภาครัฐ ไม่ว่าจะเป็นระบบรับชำระกลางของกรมบัญชีกลาง หรือระบบ KTB Corporate ของธนาคารกรุงไทย มาช่วยในการทำธุรกรรมทางการเงินของหน่วยงานภาครัฐมีความรวดเร็ว และข้อมูลทางการรับและชำระเงินมีการเคลื่อนไหวอยู่ตลอดเวลา นอกจากนั้น หน่วยงานภาครัฐอื่นๆ สามารถนำระบบการให้บริการทางการเงินการคลังที่ได้จัดทำขึ้นมาเชื่อมต่อกับการทำงานของระบบสารสนเทศทางการเงินและบัญชีภาครัฐได้เช่นเดียวกัน

3.6 BAI06 บริหารจัดการการเปลี่ยนแปลง

หน่วยงานภาครัฐที่เป็นเจ้าของระบบจะต้องมีการปรับปรุงขั้นตอนการให้บริการของหน่วยงานภาครัฐให้สอดคล้องกับระบบการทำงานของหน่วยงานภาครัฐแบบใหม่ และการนำระบบสารสนเทศทางการเงินและบัญชีภาครัฐมาใช้งานนั้น จะต้องสอดคล้องกับขั้นตอนในการให้บริการ หรือขั้นตอนการทำงานของหน่วยงานให้มีประสิทธิภาพมากยิ่งขึ้น

3.7 BAI07 บริหารจัดการการยอมรับการเปลี่ยนแปลงและการปรับเปลี่ยน

เป็นการยอมรับการเปลี่ยนแปลงกระบวนงานการนำระบบสารสนเทศทางการเงินและบัญชีภาครัฐมาใช้ในการดำเนินงานด้านการเงินการคลังของหน่วยงานภาครัฐ, การปรับเปลี่ยนกระบวนการทำงานด้านการเบิกจ่ายเงินของภาครัฐ และสิทธิในการเข้าใช้งานระบบสารสนเทศทางการเงินและบัญชีภาครัฐ รวมทั้งขั้นตอนการดำเนินงานช่วงสิ้นปีงบประมาณ ซึ่งกรมบัญชีกลางจะต้องสื่อสารหลักการดังกล่าวให้หน่วยงานภาครัฐได้รับทราบ และสามารถนำไปปฏิบัติงานได้อย่างถูกต้อง

3.8 BAI08 บริหารจัดการความรู้

เป็นการบริหารจัดการด้านความรู้เรื่องระบบสารสนเทศทางการเงินและบัญชีภาครัฐ ซึ่งกรมบัญชีกลางและหน่วยงานอื่นที่เป็นเจ้าของระบบจะเป็นผู้จัดทำความรู้และเผยแพร่ความรู้ให้กับหน่วยงานภาครัฐ โดยมีปรับปรุงความรู้ด้านขั้นตอนการใช้งานระบบ ให้เป็นไปตามรูปแบบการทำงานของหน่วยงานภาครัฐในปัจจุบัน นอกจากนั้น จะต้องสอดคล้องกับนโยบายรัฐบาล 4.0 โดยมีการให้ความรู้และคู่มือในการปฏิบัติงานสำหรับผู้ใช้งาน

3.9 BAI09 บริหารจัดการทรัพย์สิน

หน่วยงานภาครัฐจะบริหารจัดการดูแลและบำรุงรักษาอุปกรณ์การเข้าใช้งานระบบสารสนเทศทางการเงินและบัญชีภาครัฐ และระบบการเชื่อมต่อเครือข่ายการเข้าใช้งานระบบไม่ว่าจะเป็นระบบเครือข่ายแบบ Intranet ของหน่วยงานภาครัฐที่ต้องการเข้าใช้งานระบบ GFMIS หรือระบบสารสนเทศทางการเงินและบัญชีอื่นๆ ระบบ Interface ทางการเงินการคลังภาครัฐของหน่วยงานที่ทำหน้าที่ในการจัดเก็บเงินภาครัฐ หรือระบบการบริหารจัดการทรัพย์สินของกองทัพเรือซึ่งเชื่อมต่อกับระบบ GFMIS ในการบริหารจัดการด้านการเงินและบัญชีภาครัฐ เป็นต้น

3.10 BAI10 บริหารจัดการองค์ประกอบของระบบ

กรมบัญชีกลางมีการกำหนดกระบวนการในการเข้าใช้งานระบบสารสนเทศ, กระบวนการการใช้งานระบบสารสนเทศทางการเงินและบัญชีภาครัฐ และขั้นตอนการให้บริการให้แก่หน่วยงานภาครัฐ ส่วนเรื่องการติดตั้งโปรแกรมและแก้ไขปัญหาด้านเทคนิคทางคอมพิวเตอร์ให้หน่วยงานที่เป็นเจ้าของระบบเป็นคนกำหนดวิธีการติดตั้งโปรแกรม และการแก้ไขด้านเทคนิคที่หน่วยงานภาครัฐจำเป็นต้องรู้

4. การดำเนินการ (Run : DSS) แบ่งเป็น การส่งมอบ (Deliver), ให้บริการ (Service) และสนับสนุน (Support) มี 6 กระบวนงาน ดังนี้

4.1 DSS01 บริหารจัดการการปฏิบัติการ

กรมบัญชีกลางกำหนดกระบวนการให้บริการเรื่องการเข้าใช้งานระบบสารสนเทศทางการเงินและบัญชีภาครัฐ และช่องทางการติดต่อหน่วยงานภาครัฐ ตามหลักปฏิบัติการบริหารจัดการคุณภาพที่ดีขององค์กร หรือ PMQA หมวด 3 ด้านการบริการต่อผู้มีส่วนได้ส่วนเสีย

4.2 DSS02 บริหารจัดการคำร้องขอบริการและเหตุการณ์ที่เกิดขึ้น

กรมบัญชีกลางจะมีการดำเนินการจัดการคำร้องขอบริการใช้งานระบบสารสนเทศทางการเงินและบัญชีภาครัฐ ที่หน่วยงานภาครัฐได้ส่งแบบฟอร์มคำร้องตัวจริงทางไปรษณีย์, โทรสาร และไปรษณีย์อิเล็กทรอนิกส์ รวมทั้งมีการบันทึกข้อมูลการดำเนินงานให้บริการด้านสิทธิการเข้าใช้งานทางโทรศัพท์ พร้อมทั้งชี้แจงการผลดำเนินการแก้ไขปัญหาเป็นประจำทุกเดือน นอกจากนั้น ยังเป็นตัวชี้วัดผลการดำเนินงานของกรมบัญชีกลางตามภารกิจที่รับมอบหมายตามระยะเวลาที่กำหนด

4.3 DSS03 บริหารจัดการปัญหา

มีการระบุและจำแนกปัญหาระบบสารสนเทศทางการเงินและบัญชีภาครัฐตามสถานการณ์ที่เกิดขึ้น ซึ่งปัญหาสามารถแบ่งเป็นปัญหาจากผู้ให้บริการระบบ และปัญหาจากผู้รับบริการระบบ โดยปัญหาที่เกิดขึ้นจะต้องมีคู่มือการในการแก้ไขปัญหา และแนวทางในการแก้ไขปัญหาที่เกิดขึ้นในแต่ละวัน เพื่อให้ผู้ให้บริการสามารถให้คำแนะนำ และแนวทางแก้ไขปัญหาได้อย่างถูกต้อง

4.4 DSS04 บริหารจัดการความต่อเนื่อง

ระบบสารสนเทศทางการเงินและบัญชีภาครัฐควรมีการทำงานอย่างต่อเนื่อง เพื่ออำนวยความสะดวกแก่ผู้รับบริการ ถ้ามีเหตุขัดข้องควรมีการปรับปรุงแก้ไขระบบ และแจ้งให้ผู้รับบริการได้รับทราบถึงปัญหาที่เกิดขึ้น

4.5 DSS05 บริหารจัดการด้านความปลอดภัย

เป็นการป้องกันข้อมูลทางการเงินการคลังของหน่วยงานให้ความเสี่ยงด้านความปลอดภัยของข้อมูลอยู่ในระดับที่หน่วยงานยอมรับได้ ตามนโยบายการรักษาความปลอดภัยด้านการใช้งาน

ระบบของหน่วยงาน อย่างเช่น การกำหนดผู้มีสิทธิในการเข้าใช้งานระบบสารสนเทศทางการเงินและบัญชีภาครัฐ การจัดเก็บและการบำรุงรักษาอุปกรณ์การเข้าใช้งานระบบสารสนเทศทางการเงินและบัญชีภาครัฐ การตั้งรหัสผ่านการเข้าใช้งาน เป็นต้น

4.6 DSS06 บริหารจัดการการควบคุมกระบวนการทางธุรกิจ

หน่วยงานภาครัฐจะเป็นกำหนดหลักการการควบคุมการใช้งานระบบสารสนเทศทางการเงินและบัญชีภาครัฐ ซึ่งการกำหนดหลักการควบคุมด้านการทำงานระบบสารสนเทศทางการเงินและบัญชีภาครัฐนั้น ให้เป็นไปตามแนวทางการปฏิบัติงานในระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ (GFMIS) ที่กระทรวงการคลังกำหนดไว้, แนวทางในการใช้งานระบบอื่น ๆ ตามหนังสือเวียน และหลักการควบคุมภายในที่ดีของหน่วยงานภาครัฐ

5. การติดตาม (Monitor : MEA) แบ่งเป็น การติดตาม (Monitor), วัดผล (Evaluation), การประเมิน (Assess) มี 3 กระบวนงาน ดังนี้

5.1 MEA01 เฝ้าติดตาม วัดผลและประเมินประสิทธิภาพและความสอดคล้องในการดำเนินงาน

เป็นการรวบรวมข้อมูล, ตรวจสอบและประเมินการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศทางการเงินและบัญชีของหน่วยงานภาครัฐ รวมทั้งการตรวจสอบการดำเนินงานกระบวนการให้สามารถทำงานได้อย่างมีประสิทธิภาพ สิทธิการเข้าใช้งานระบบ รวมทั้งการปฏิบัติงานให้ตรงตามระเบียบการเงินการคลังที่กระทรวงการคลังกำหนดไว้

5.2 MEA02 เฝ้าติดตาม วัดผลและประเมินระบบการควบคุมภายใน

เป็นการตรวจสอบ ติดตาม และประเมินสภาพแวดล้อมการควบคุมภายในด้านการใช้งานระบบสารสนเทศทางการเงินและบัญชีของหน่วยงานภาครัฐ เพื่อระบุข้อบกพร่องในการใช้งานระบบ เพื่อนำมาปรับปรุงระบบและกระบวนการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศทางการเงินและบัญชีภาครัฐให้มีประสิทธิภาพ และข้อมูลมีความถูกต้อง, ครบถ้วน และเป็นปัจจุบัน

5.3 MEA03 เฝ้าติดตาม วัดผลและประเมินการปฏิบัติตามข้อกำหนดของหน่วยงานภายนอก

เป็นการประเมินกระบวนงานทางเทคโนโลยี และกระบวนงานของหน่วยงานที่สนับสนุนงานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับระบบสารสนเทศทางการเงินและบัญชีภาครัฐให้เป็นไปตามข้อปฏิบัติการรักษาความปลอดภัย และแผนแม่บทด้านความปลอดภัยที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้กำหนดไว้ โดยหน่วยงานที่เป็นเจ้าของระบบสารสนเทศควรให้ความสนใจและหมั่นคอยตรวจสอบระบบไม่ให้ถูกโจรกรรมข้อมูลทางการเงินของประเทศ

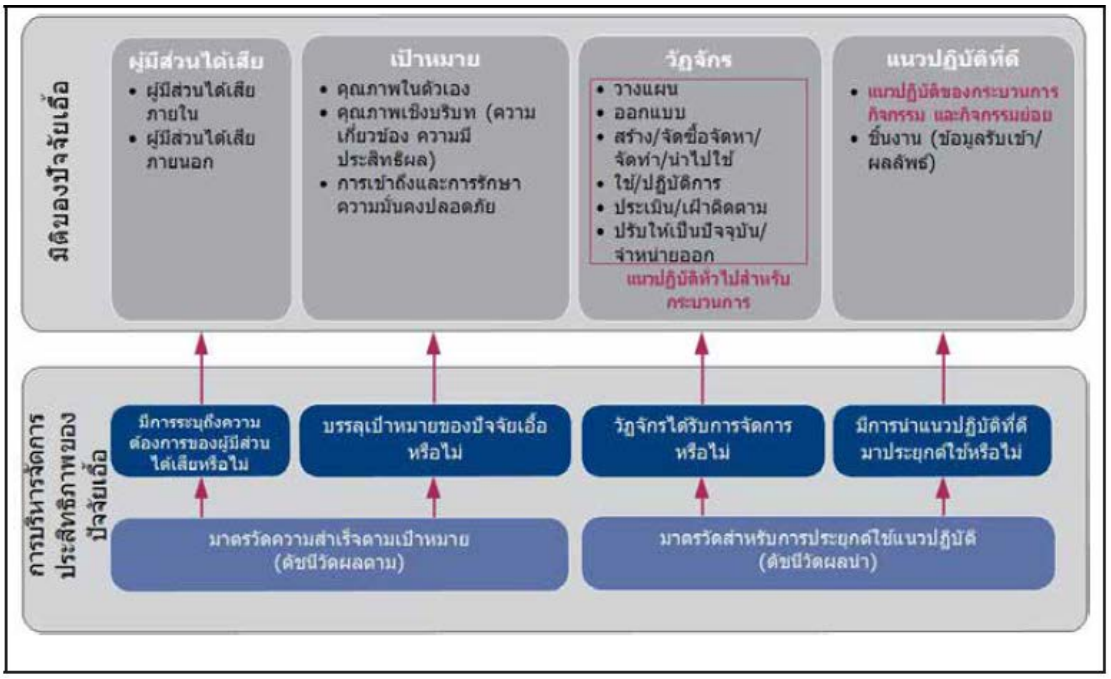
ความสัมพันธ์ระหว่างการกำกับดูแลกับการบริหารจัดการเชิงเทคโนโลยีสารสนเทศ

ความสัมพันธ์ระหว่างการกำกับดูแลกับการบริหารจัดการเชิงเทคโนโลยีสารสนเทศ โดยอ้างอิงปัจจัยสนับสนุนเพื่อให้ระบบการควบคุมภายในเชิงเทคโนโลยีสารสนเทศ มีประสิทธิภาพมากขึ้น

ปัจจัยสนับสนุนสามารถแบ่งได้เป็น 7 ประเภท คือ

1. หลักการ นโยบาย และกรอบการดำเนินงาน เป็นแนวทางที่ผู้บริหารใช้ในการตัดสินใจด้านการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศภายในองค์กร ซึ่งในการกำหนดหลักการ นโยบายที่ดีนั้น ผู้บริหารควรนึกถึงประสิทธิภาพในการใช้หลักการ นโยบายให้สอดคล้องกับสภาพการทำงานขององค์กร และสามารถบรรลุวัตถุประสงค์ที่องค์กรได้กำหนดไว้ นอกจากนั้น ผู้มีส่วนได้ส่วนเสียสามารถเข้าถึงหลักการ และนโยบาย

2. กระบวนการ เป็น แนวปฏิบัติงานของเจ้าหน้าที่ในองค์กร เพื่อให้บรรลุวัตถุประสงค์ในการควบคุมภายในด้านเทคโนโลยีสารสนเทศขององค์กร ภายใต้หน้าที่และความรับผิดชอบที่ได้รับมอบหมายตามนโยบายที่ผู้บริหารระดับสูงได้กำหนดไว้เป็นแนวทางในการปฏิบัติงาน ดังภาพต่อไปนี้



ภาพที่ 2.3 แผนผังองค์ประกอบของปัจจัยเอื้อ : กระบวนการ (ISCA, 2012)

ในแผนผังขององค์ประกอบของปัจจัยเอื้อด้านกระบวนการ มีดังนี้

2.1 ผู้มีส่วนได้ส่วนเสีย ตามกรอบการดำเนินงานของ COBIT 5 สามารถแบ่งกลุ่มผู้มีส่วนได้ส่วนเสียเป็น 2 ประเภท คือ

2.1.1 ผู้มีส่วนได้ส่วนเสียภายใน คือ บุคคลภายในองค์กรที่มีทำให้เกิดกระบวนการทำงานด้าน ได้แก่ ผู้บริหารระดับสูง ผู้ปฏิบัติในองค์กร เป็นต้น

2.1.2 ผู้มีส่วนได้ส่วนเสียภายนอก คือ บุคคลภายนอกที่ได้รับผลกระทบจากการดำเนินงานตามกระบวนการขององค์กร ได้แก่ ผู้รับบริการ, หน่วยงานที่ทำหน้าที่ตรวจสอบ เป็นต้น

2.2 เป้าหมาย คือ ผลลัพธ์ที่องค์กรคาดหวังจากการปฏิบัติงานตามกระบวนการที่ผู้บริหารได้กำหนดไว้ในนโยบายขององค์กร และกระบวนการควรสนับสนุนทั้งเป้าหมายขององค์กรและเป้าหมายทางเทคโนโลยีสารสนเทศไปด้วยกัน โดยเป้าหมายของกระบวนการแบ่งเป็น 3 ประเภท คือ

2.2.1 เป้าหมายในตนเอง (Intrinsic goal) คือ กระบวนการมีความสอดคล้องกับแนวทางปฏิบัติตามนโยบาย และกฎระเบียบที่องค์กรกำหนดไว้

2.2.2 เป้าหมายเชิงบริบท (Contextual goal) คือ กระบวนการขององค์กรมีการปรับเปลี่ยนตามสถานการณ์ที่เกิดโดยเฉพาะขององค์กร, ผู้มีส่วนได้ส่วนเสียสามารถเข้าใจกระบวนการได้ง่าย และสามารถนำไปประยุกต์ใช้กับงานที่ทำอยู่ได้

2.2.3 เป้าหมายการเข้าถึงและการรักษาความปลอดภัย กระบวนการทำงานขององค์กรควรเป็นความลับ และสามารถเข้าถึงได้เฉพาะผู้ปฏิบัติงานเท่านั้น

เป้าหมายทั้ง 3 ประเภทจะต้องมีตัวชี้วัดในวัดผลการบรรลุวัตถุประสงค์ขององค์กรที่กำหนดไว้ โดยใช้ตัวชี้วัดแบบ SMART แบ่งได้ดังนี้

เป้าหมายจะต้องระบุเฉพาะเจาะจง(Specific), สามารถวัดผลการดำเนินงานได้(Measurable), นำไปใช้งานได้จริง (Actionable), มีความเกี่ยวข้อง(Relevant)และทันเวลา(Timely) และตัวชี้วัดเหล่านี้จะช่วยในการบริหารปัจจัยเอื้อของกระบวนการให้มีประสิทธิภาพและประสิทธิผลซึ่งส่งผลต่อการนำแนวทางปฏิบัติมาประยุกต์ใช้ในกระบวนการ

2.3 วัฏจักร กระบวนการในแต่ละงานจะต้องมีวัฏจักรในการดำเนินงานแบ่งได้ ดังนี้

2.3.1 การวางแผน

2.3.2 การออกแบบ

2.3.3 การสร้าง/การจัดซื้อจัดหา

2.3.4 ใช้หรือการปฏิบัติงาน

2.3.5 การประเมินติดตาม

2.3.6 ปรับเป็นปัจจุบัน

กระบวนการควรมีการดำเนินการ ได้แก่ การกำหนดกระบวนการขององค์กรให้มีความเหมาะสมกับสภาพการทำงาน

2.4 แนวปฏิบัติที่ดีของกระบวนการ

องค์กรสามารถใช้กรอบการดำเนินงาน COBIT 5 ในเรื่องของกระบวนการกำกับดูแลและการบริหารจัดการเชิงเทคโนโลยีสารสนเทศ รวมทั้งโครงสร้างอ้างอิงของกระบวนการมาประยุกต์ใช้ให้เข้ากับองค์กร โดยมีแนวปฏิบัติซึ่งสามารถแบ่งเป็น

2.4.1 แนวปฏิบัติภาพรวมของการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร มีดังนี้

2.4.1.1 กระบวนการที่ดีควรมีคำแถลงการณ์การปฏิบัติการ (Statements of Actions) เพื่อใช้ในการควบคุมระดับความเสี่ยงให้อยู่ในระดับที่องค์กรสามารถยอมรับได้ และการใช้ทรัพยากรให้เกิดประโยชน์สูงสุดในการดำเนินงานในองค์กร

2.4.1.2 กระบวนการที่ดีควรมีความสอดคล้องกับแนวปฏิบัติที่ได้รับการยอมรับโดยทั่วไป

2.4.1.3 กระบวนการจะต้องมีลักษณะทั่วไป เหมาะสำหรับการนำไปประยุกต์ใช้ในแต่ละองค์กร

2.4.1.4 จะต้องครอบคลุมบุคคลที่มีหน้าที่ทั้งในภาคธุรกิจและด้านเทคโนโลยีสารสนเทศ

2.4.2 หน่วยงานที่ทำหน้าที่กำกับดูแลและผู้บริหารระดับสูงขององค์กรจะต้องทำการตัดสินใจในด้านการกำกับดูแลและการบริหารจัดการ ดังนี้

2.4.2.1 สามารถเลือกและตัดสินใจในการนำกระบวนการมาประยุกต์ใช้งาน

2.4.2.2 แนวปฏิบัติสามารถเพิ่มเติมและ/หรือนำไปปรับใช้ให้เหมาะสมตามความจำเป็น

2.4.2.3 กำหนดและเลือกแนวทางการปฏิบัติงานที่ไม่มีส่วนเกี่ยวข้องด้านเทคโนโลยีสารสนเทศ เพื่อนำมาปรับใช้ให้เข้ากับกระบวนงานธุรกิจ

2.4.2.4 ยอมรับความเสี่ยงจากการไม่มีนำกระบวนการมาประยุกต์ใช้

กระบวนการจะต้องมีตัวชี้วัดผลสำเร็จในแต่ละส่วนงาน เพื่อวัดประสิทธิภาพในการทำงานขององค์กร โดยมีการติดตามผลการดำเนินงานได้ตามเกณฑ์ ดังนี้

1. การระบุความต้องการของผู้มีส่วนได้ส่วนเสีย หมายถึง กระบวนการในองค์กรมีการระบุความต้องการของผู้มีส่วนได้ส่วนเสียหรือไม่

2. การบรรลุเป้าหมายและวัตถุประสงค์ขององค์กร หมายถึง กระบวนการขององค์กรบรรลุตามเป้าหมายและวัตถุประสงค์

3. การจัดการวัฏจักรของปัจจัยเอื้อ กระบวนการมีการบริหารจัดการวงจรการดำเนินงานของปัจจัยเอื้อหรือไม่

4. การนำแนวปฏิบัติมาประยุกต์ใช้งานองค์กรมีการนำแนวปฏิบัติตามกรอบการดำเนินงานมาประยุกต์ใช้งานหรือไม่

ปัจจัยเอื้อด้านกระบวนการนั้นเป็นปัจจัยหลักในการทำให้เกิดกิจกรรมในการดำเนินงานภายในองค์กร โดยมีความสัมพันธ์คู่กับปัจจัยเอื้ออื่น ๆ ดังนี้

1. ความสัมพันธ์กับปัจจัยด้านสารสนเทศ สารสนเทศเป็นส่วนหนึ่งที่ทำให้เกิดกระบวนการในด้านปัจจัยนำเข้า ในขณะเดียวกัน กระบวนการมีส่วนทำให้เกิดผลลัพธ์ในรูปแบบสารสนเทศ

2. ความสัมพันธ์กับโครงสร้างจัดองค์กร การระบุหน้าที่และบทบาทความรับผิดชอบให้กับงานในกระบวนการที่กำหนดไว้

3. ความสัมพันธ์กับการบริการ การให้บริการ โครงสร้างพื้นฐาน และระบบงานจำเป็นต้องมีกระบวนการสำคัญที่ช่วยในการดำเนินงานสัมฤทธิ์ผล

4. ความสัมพันธ์กับหลักการ นโยบายและกรอบการดำเนินงาน เป็นตัวกำหนดลักษณะของกระบวนการให้เป็นไปตามความต้องการขององค์กร

5. ความสัมพันธ์กับวัฒนธรรม และพฤติกรรม โดยคำนึงถึงประสิทธิภาพของการนำกระบวนการไปปฏิบัติใช้ในองค์กร

3. โครงสร้างองค์กร เป็น การระบุอำนาจการตัดสินใจ และหน้าที่ความรับผิดชอบของทุกส่วนงานในองค์กร รวมทั้งการบริหารจัดการบุคลากรในองค์กร แนวปฏิบัติที่ดีในการจัดโครงสร้างองค์กรที่ทำให้บรรลุผลการดำเนินงาน มีดังนี้

3.1 การดำเนินงานที่เกี่ยวข้องกับโครงสร้างองค์กรที่นำไปปฏิบัติงานได้ อย่างเช่น ความถี่ในการประชุมในองค์กร, กฎระเบียบภายในองค์กร และการจัดทำเอกสาร เป็นต้น

3.2 โครงสร้างองค์กรที่ดีควรมีผู้มีส่วนได้ส่วนเสียภายในและภายนอก เพื่อให้เกิดความสมดุลในการบริหารองค์กร

3.3 การจัดโครงสร้างองค์กร ควรมีการกำหนดอำนาจการตัดสินใจตามลักษณะของการจัดโครงสร้างองค์กร

3.4 ควรมีขั้นตอนการแจ้งเรื่องตามลำดับของโครงสร้างองค์กร ซึ่งระบุถึงวิธีการดำเนินงานในกรณีมีปัญหาที่เกี่ยวข้องกับการตัดสินใจ

4. วัฒนธรรม, จริยธรรม และพฤติกรรม เป็น ลักษณะการทำงานของคนในองค์กร ซึ่งเป็นปัจจัยสนับสนุนหลักในด้านการควบคุมภายในและการกำกับดูแลกิจการที่ดีในองค์กร โดยสอดคล้องกับการจัดโครงสร้างองค์กร และสภาพแวดล้อมการทำงานของบุคลากรในองค์กร มีแนวปฏิบัติที่ดี ซึ่งก่อให้เกิดแบบพฤติกรรมที่ดีในองค์กร มีดังนี้

4.1 มีการสื่อสารเรื่องรูปแบบพฤติกรรมที่ควรทำ และการส่งเสริมคุณค่าภายในองค์กรให้บุคลากรในองค์กรได้ทราบโดยทั่วกัน

4.2 ผู้บริหารระดับสูงควรประพฤติตนให้เป็นแบบอย่างที่ดีแก่บุคลากร

4.3 องค์กรจะต้องกำหนดรูปแบบการให้ผลตอบแทน เพื่อแรงจูงใจให้บุคลากรให้สามารถปฏิบัติตนตามแบบพฤติกรรมที่ควรปฏิบัติ

4.4 องค์กรควรมีการกำหนดกฎระเบียบการประพฤติตนของบุคลากรในองค์กรให้สอดคล้องกับนโยบายที่องค์กรกำหนดไว้

5. สารสนเทศ เป็น สารสนเทศที่องค์กรได้นำมาใช้ในการควบคุมภายในและกำกับดูแลองค์กร ด้านกระบวนการทำงานด้านเทคโนโลยีสารสนเทศของคนในองค์กร และมีการกำหนดคุณภาพ และแนวปฏิบัติที่ดีเกี่ยวกับสารสนเทศ ได้ ดังนี้

5.1 คุณภาพของเป้าหมายด้านสารสนเทศ

5.1.1 คุณภาพในตัวเอง (Intrinsic Quality)

5.1.1.1 ความถูกต้อง

5.1.1.2 ความเที่ยงตรง ไม่มีการบิดเบือนข้อมูล

5.1.1.3 ความน่าเชื่อถือ ความถูกต้องของข้อมูลในสารสนเทศที่ได้รับมา

5.1.1.4 ชื่อเสียง แหล่งที่มาของข้อมูลสารสนเทศมีความน่าเชื่อถือ และเนื้อหาที่ได้มา

5.1.2 คุณภาพเชิงบริบทและการนำเสนอ หมายถึง การนำสารสนเทศมาประยุกต์ใช้ให้เหมาะสมกับสภาพการทำงานขององค์กร มีหลักการ ดังนี้

5.1.2.1 ความเกี่ยวเนื่อง สารสนเทศจะต้องมีการประยุกต์ใช้และเป็นประโยชน์ต่องานในองค์กร

5.1.2.2 ความครบถ้วน เนื้อหาข้อมูลสารสนเทศไม่มีการขาดช่วง และข้อมูลที่ได้มาเพียงพอต่องาน

5.1.2.3 ความเป็นปัจจุบัน สารสนเทศที่ได้รับมาควรมีความเป็นปัจจุบันให้ตรงตามภารกิจที่ได้รับ

5.1.2.4 ปริมาณงานสารสนเทศที่เหมาะสม ซึ่งสารสนเทศที่ดีจะต้องมีความเพียงพอต่องานที่ได้ทำ

5.1.2.5 การนำเสนอสารสนเทศควรสั้นกระชับ

5.1.2.6 การนำเสนอสารสนเทศควรมีความสอดคล้องกัน

5.1.2.7 ความสามารถในการตีความ มีการใช้ภาษาหรือคำอธิบายที่ชัดเจน

5.1.2.8 ความเข้าใจได้ ผู้ใช้งานสารสนเทศสามารถเข้าใจข้อมูลสารสนเทศได้

5.1.2.9 ความง่ายต่อการดำเนินงาน สารสนเทศสามารถนำไปประยุกต์ใช้งาน

5.1.3 คุณภาพด้านความมั่นคงปลอดภัยและเข้าถึง

5.1.3.1 ความพร้อมใช้และทันเวลา สารสนเทศที่จัดทำควรมีความพร้อมในการใช้งานและทันต่อเวลา

5.1.3.2 จำกัดการเข้าถึง สารสนเทศที่ดีควรมีการจำกัดการเข้าถึงเฉพาะบุคคลที่ได้รับการอนุญาตจากองค์กรเท่านั้น

6. บริการ โครงสร้างพื้นฐานและระบบงานเป็น รูปแบบระบบงาน, โครงสร้างของระบบงานและเทคโนโลยีที่ใช้ในการประมวลผลข้อมูลการทำงานของผู้ใช้งานระบบภายในองค์กร รวมทั้งทรัพยากรและกระบวนการทำงานมาช่วยให้บรรลุเป้าหมายและวัตถุประสงค์ขององค์กร ดังภาพต่อไปนี้ ซึ่งแสดงให้เห็นถึง

6.1 ผู้มีส่วนได้ส่วนเสีย ได้แก่ ผู้ให้บริการภายนอก, ผู้รับบริการ, ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เป็นต้น ขึ้นอยู่สถานการณ์บริการของหน่วยงาน

6.2 เป้าหมาย องค์กรควรให้ความสำคัญในการให้บริการ ระบบงาน และโครงสร้างพื้นฐานในการให้บริการให้เกิดประโยชน์ต่อองค์กรในด้านการเงิน รวมทั้งบรรลุเป้าหมายและวัตถุประสงค์การให้บริการ

6.3 วัฏจักร การให้บริการขององค์กรจะต้องมีครอบคลุม ระบบงานในอนาคต, ความสามารถในการให้บริการในอนาคต, รูปแบบเป้าหมายของโครงสร้างพื้นฐานการให้บริการและความสัมพันธ์ระหว่างส่วนประกอบด้านการให้บริการ

6.4 แนวปฏิบัติที่ดี หมายถึง แนวปฏิบัติด้านความสามารถในการให้บริการรวมถึง

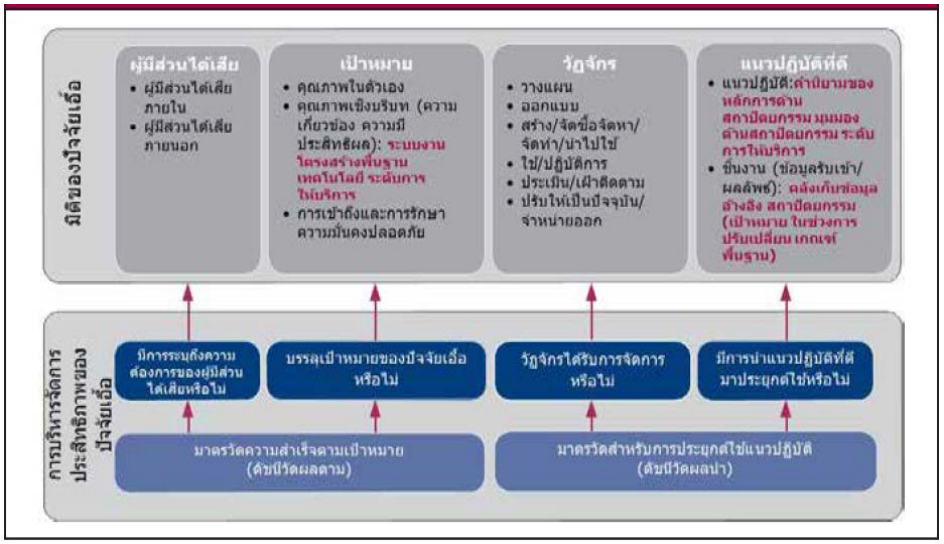
6.4.1 คำนิยามหลักการสถาปัตยกรรม หมายถึง แนวทางที่ใช้ในกำกับดูแลการนำเทคโนโลยีสารสนเทศไปใช้งาน และการใช้ทรัพยากรทางด้านเทคโนโลยีสารสนเทศภายในองค์กร

6.4.2 คำนิยามขององค์กรสำหรับโครงสร้างสถาปัตยกรรมที่เหมาะสม โดยให้ความสนใจเรื่องการตอบสนองความต้องการต่อผู้มีส่วนได้ส่วนเสียที่มีความหลากหลาย ได้แก่ รูปแบบ, รายการ และตัวชี้วัด โดยใช้โครงสร้างสถาปัตยกรรมเป็นพื้นฐาน, เป้าหมายและสถาปัตยกรรมที่อยู่ในช่วงระว่างการปรับเปลี่ยนระบบงาน อย่างเช่น การใช้แผนผังการเชื่อมโยงระบบการทำงานของ

ระบบการทำงานของระบบงาน (Application Interface Diagram) เป็นต้น

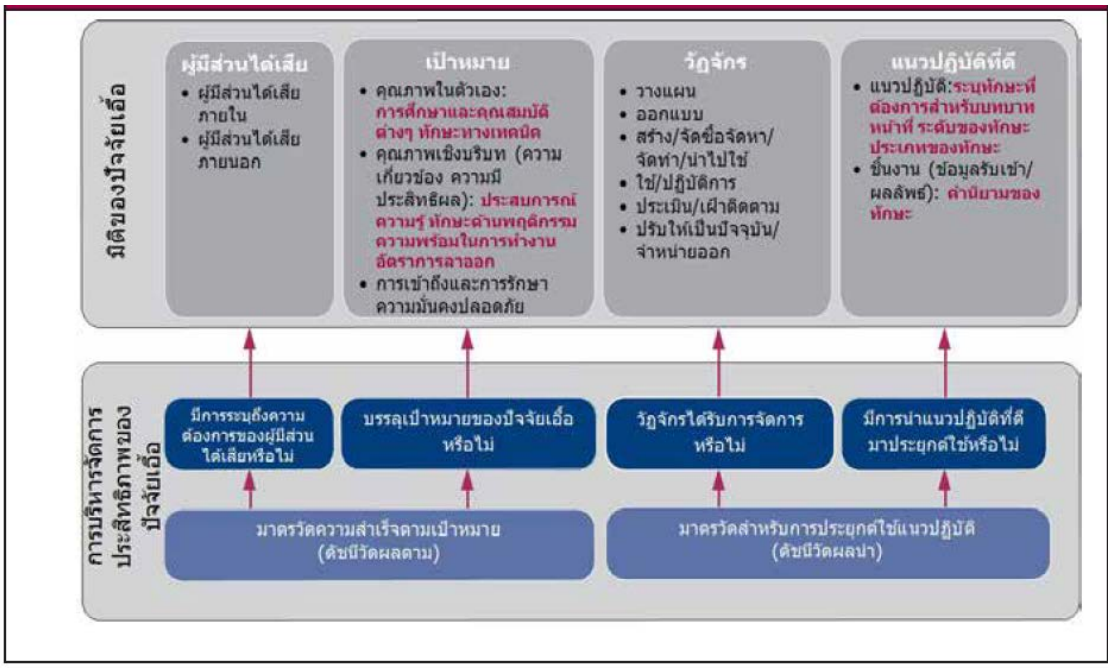
6.4.3 คลังเก็บสถาปัตยกรรม ซึ่งจัดเก็บผลการดำเนินงานของสถาปัตยกรรมแต่ละประเภท, หลักการและมาตรฐาน, แบบอ้างอิงของสถาปัตยกรรม และส่วนประกอบอื่น ๆ ของสถาปัตยกรรม อย่างเช่น ระบบงาน, โครงสร้างพื้นฐานทางเทคโนโลยี (อุปกรณ์ฮาร์ดแวร์คอมพิวเตอร์, โปรแกรมการใช้งาน, โครงสร้างระบบเครือข่าย) และโครงสร้างพื้นฐานกายภาพ (ISACA, 2012) เป็นต้น

ระดับการให้บริการที่องค์กรกำหนด และผู้ปฏิบัติงานด้านการให้บริการต้องปฏิบัติตามที่องค์กรได้มีการกำหนดไว้



ภาพที่ 2.4 แผนผังองค์ประกอบปัจจัยเอื้อด้านการบริการ โครงสร้างพื้นฐาน และระบบงาน (ISACA, 2012)

7. บุคคล, ทักษะ และศักยภาพ หมายถึง ความรู้ความสามารถของผู้ใช้งานระบบ ขึ้นอยู่กับกิจกรรมการดำเนินงานภายในองค์กร ดังภาพต่อไปนี้



ภาพที่ 2.5 แผนผังองค์ประกอบของปัจจัยเอื้อด้านบุคคล ทักษะ และศักยภาพ (ISACA, 2012)

ในแผนผังขององค์ประกอบของปัจจัยเอื้อด้านบุคคล ทักษะ และศักยภาพ มีดังนี้

7.1 ผู้มีส่วนได้ส่วนเสีย: ภายในและภายนอก ได้แก่ เจ้าหน้าที่ฝ่ายพัฒนาอบรม, เจ้าหน้าที่ฝ่ายสรรหาบุคคล, เจ้าหน้าที่ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และผู้รับบริการขององค์กร

7.2 เป้าหมาย องค์กรได้กำหนดเป้าหมายบุคคลจะต้องให้ความสำคัญของระดับการศึกษา, ความรู้ความสามารถ, ประสบการณ์การทำงาน และอัตรากำลังขององค์กรซึ่งเป้าหมายเหล่านี้จำเป็นต้องมีกิจกรรมและกระบวนการช่วยให้บรรลุเป้าหมายอย่างมีประสิทธิภาพ

7.3 วัฏจักร องค์กรต้องทราบความรู้ความสามารถและทักษะในสายงานของบุคลากรในองค์กร มาใช้ในการวางแผนการพัฒนาความรู้ความสามารถ และทักษะของบุคลากรในองค์กร การวางแผนจัดหาบุคลากรให้เหมาะสมกับงานที่ได้รับ และประเมินผลการเรียนรู้อย่างสม่ำเสมอ ซึ่งช่วยในการพัฒนาความรู้ของบุคลากร นอกจากนั้น นำไปสู่กระบวนการให้ผลตอบแทน หรือการให้การยอมรับสำหรับการบริหารจัดการทรัพยากรบุคคล

7.4 แนวปฏิบัติที่ดี แนวปฏิบัติควรระบุความจำเป็นของทักษะงานที่จำเป็นตามหน้าที่และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียภายใน และภายนอก รวมทั้งอธิบายระดับของทักษะความรู้ความสามารถที่ความเกี่ยวข้องกับงานด้านเทคโนโลยีสารสนเทศ ดังตัวอย่างต่อไปนี้

กระบวนการในโดเมนต่างๆ	ตัวอย่างประเภทของทักษะ
ประเมิน สั่งการ และเฝ้าติดตาม (EDM)	• การกำกับดูแลไอทีระดับองค์กร
จัดวางแนว จัดทำแผน และจัดระบบ (APO)	• การจัดทำนโยบายด้านไอที • กลยุทธ์ด้านไอที • สถาปัตยกรรมองค์กร • นวัตกรรม • การบริหารการเงิน • การบริหารจัดการกลุ่ม (ของโครงการหรือเงินลงทุน)
จัดสร้าง จัดหา และนำไปใช้ (BAI)	• การวิเคราะห์ธุรกิจ • การบริหารโครงการ • การประเมินการใช้งาน (ใช้และเรียนรู้ได้ง่าย) • การให้คำนิยามและการบริหารจัดการความต้องการ • การจัดทำโปรแกรม • การยศาสตร์ของระบบ (System ergonomics) • การเลิกใช้งานซอฟต์แวร์ (Software decommissioning) • การบริหารจัดการขีดความสามรถ (Capacity management)
ส่งมอบ บริการ และสนับสนุน (DSS)	• การบริหารจัดการความพร้อมใช้ • การบริหารจัดการปัญหา • การบริหารจัดการหน่วยบริหาร (Service desk) และเหตุการณ์ผิดปกติ • การบริหารจัดการความมั่นคงปลอดภัย • ปฏิบัติการด้านไอที • การบริหารจัดการฐานข้อมูล
เฝ้าติดตาม วัดผล และประเมิน (MEA)	• การสอบทานการปฏิบัติตาม (กฎหมายหรือกฎระเบียบข้อบังคับ) • การเฝ้าติดตามประสิทธิภาพในการดำเนินงาน • การตรวจสอบการควบคุม

ภาพที่ 2.6 ตัวอย่างประเภททักษะงานที่จำเป็นตามกระบวนงานหลักใน COBIT 5 (ISACA, 2012)

ปัจจัยสนับสนุนทั้ง 7 ประเภทจะต้องทำงานร่วมกัน เพื่อให้เกิดประสิทธิภาพในการควบคุมภายในระบบเทคโนโลยีสารสนเทศ จะต้องมีนโยบาย และกรอบการดำเนินงานด้านเทคโนโลยีขององค์กรที่มีความชัดเจน และครอบคลุมการดำเนินงานด้านเทคโนโลยีสารสนเทศ ดังภาพที่ 2.6 และภาพที่ 2.7

ภาพที่ 2.7 องค์ประกอบของปัจจัยสนับสนุนภายใต้กรอบการดำเนินงาน COBIT5 (ISACA, 2012)

ดังนั้น ปัจจัยสนับสนุนจะต้องมีกิจกรรมการกำกับดูแลองค์กร และการบริหารจัดการด้านเทคโนโลยีสารสนเทศมาช่วยให้การควบคุมภายในด้านเทคโนโลยีสารสนเทศมีประสิทธิภาพและบรรลุเป้าหมายการดำเนินงานภายในองค์กร ดังตารางต่อไปนี้

ตารางที่ 2.2 ความสัมพันธ์ระหว่างการกำกับดูแลและการบริหารจัดการด้านเทคโนโลยีสารสนเทศโดยใช้โครงสร้างปัจจัยสนับสนุน (ISACA, 2012)

ปัจจัยสนับสนุน	**ความสัมพันธ์ระหว่างการกำกับดูแลกับการบริหารจัดการ**
กระบวนงาน	กระบวนงานการกำกับดูแลองค์กร และการบริหารจัดการมีความแตกต่างในด้านแนวปฏิบัติและกิจกรรมในการดำเนินงาน ซึ่งการกำกับดูแลองค์กรจะกำหนดทิศทางในการดำเนินงาน แต่การบริหารจัดการจะนำกรอบการดำเนินงานมาใช้ในการตัดสินใจ ทั้งสองกระบวนงานจำเป็นต้องใช้ตารางระบุหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานภายในองค์กร
สารสนเทศ	กระบวนงานการกำกับดูแลองค์กร และการบริหารจัดการใช้สารสนเทศในการรับ-ส่งข้อมูลและผลการดำเนินงานในด้านการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

ตารางที่ 2.2 (ต่อ)

ปัจจัยสนับสนุน	ความสัมพันธ์ระหว่างการกำกับดูแลกับการบริหารจัดการ
โครงสร้างองค์กร	โครงสร้างองค์กรมีการกำหนดหน้าที่การกำกับดูแลและการบริหารจัดการด้านเทคโนโลยีสารสนเทศ ที่แตกต่างกัน ขึ้นอยู่กับมีการองค์ประกอบที่ใช้ในการตัดสินใจ และการนำผลการตัดสินใจมาใช้ในการปฏิบัติงาน
หลักการ นโยบาย และกรอบการดำเนินงาน	เป็นส่วนหนึ่งที่ช่วยในการตัดสินใจของผู้บริหารในด้านการกำกับดูแลและการบริหารจัดการด้านเทคโนโลยีสารสนเทศขององค์กร
วัฒนธรรม จริยธรรม และพฤติกรรม	ลักษณะการทำงานของคนภายในองค์กรเป็นส่วนหนึ่งที่ช่วยในการกำหนดลักษณะงานด้านการกำกับดูแล และการบริหารจัดการเทคโนโลยีสารสนเทศขององค์กร ให้มีความชัดเจน และรัดกุมในด้านการควบคุมภายในให้มีประสิทธิภาพ
บุคลากร ทักษะและความสามารถ	ทักษะและความรู้ความสามารถของบุคลากรในงานแต่ละด้านที่ได้รับมอบหมาย ซึ่งบุคลากรจะต้องมีความเข้าใจในงานที่ได้รับ ในด้านการกำกับดูแล และการบริหารจัดการสารสนเทศในองค์กร
บริการ โครงสร้างพื้นฐานและระบบงาน	การบริการจำเป็นต้องใช้โครงสร้างพื้นฐานและระบบงาน โดยใช้เทคโนโลยีสารสนเทศให้เหมาะสมกับกระบวนงานด้านการกำกับดูแล, กระบวนงานด้านการบริหารจัดการ และสภาพการทำงานของคนในองค์กร

2.3 งานวิจัยที่เกี่ยวข้อง

เนื่องจากงานวิจัยนี้เป็นศึกษาองค์ประกอบขององค์ประกอบการบริหารจัดการเทคโนโลยีสารสนเทศตามกรอบงาน COBIT 5 ซึ่งเรื่องที่ผู้วิจัยกำลังศึกษาอยู่นั้น ยังไม่โดยแบ่งเป็น 3 หัวข้อ คือ (1) การประยุกต์หลักการควบคุมทั่วไปของระบบสารสนเทศทางการบัญชีตามสภาพแวดล้อมของธุรกิจ (2) ความสัมพันธ์หลักการควบคุมภายในกับการควบคุมเชิงเทคโนโลยีสารสนเทศ และ(3) หลักการควบคุมภายในเชิงเทคโนโลยีสารสนเทศ(IT Governance) สามารถสรุปประเด็นได้ดังต่อไปนี้

2.3.1 การประยุกต์หลักการควบคุมทั่วไปของระบบสารสนเทศทางการบัญชีตามสภาพแวดล้อมของธุรกิจแต่ละประเภท

งานวิจัยของนันทิดา โยธานวล และ ดร.ศักดิ์ชาย จันทร์เรืองได้ศึกษาเรื่องการควบคุมภายในทั่วไปของระบบสารสนเทศทางการบัญชี โดยใช้บริษัท อี.เทค จำกัด เป็นกรณีศึกษา โดยใช้วิธีการสอบถามพนักงานและการสังเกตการณ์ปฏิบัติงานของพนักงาน บริษัท อี.เทค จำกัด และใช้หลักการควบคุมทั่วไประบบสารสนเทศทางการบัญชี ปรากฏว่า การควบคุมภายในด้านสารสนเทศของบริษัทอยู่ในระดับดี เนื่องจาก บริษัทมีการปฏิบัติงานตามแนวทางด้านการควบคุมทั่วไปของระบบสารสนเทศ จึงส่งผลให้มีระบบการทำงานทางสารสนเทศมีประสิทธิภาพ ข้อมูลที่ออกมามีความถูกต้องครบถ้วน โปร่งใส และสามารถตรวจสอบได้ (นันทิดา โยธานวล และ ศักดิ์ชาย จันทร์เรือง, 2558) ในขณะเดียวกัน การนำระบบสารสนเทศทางการบัญชีมาใช้งานได้ทุกประเภทของธุรกิจ ไม่ว่าจะเป็นธุรกิจขนาดกลางและขนาดย่อม ย่อมมีเหตุการณ์หรือปัจจัยต่าง ๆ ที่ส่งผลต่อการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ซึ่งการวิจัยนี้ได้ทำการสอบถามความคิดเห็นเจ้าหน้าที่ทำบัญชีในธุรกิจขนาดกลางและขนาดย่อม ในเรื่องปัจจัยผลกระทบในเรื่องการนำระบบสารสนเทศทางการบัญชีมาใช้ในกิจการประกอบไปด้วยปัจจัยด้านอุปกรณ์คอมพิวเตอร์ โปรแกรมซอฟต์แวร์ และข้อมูลรายงานทางการเงินของระบบสารสนเทศทางการบัญชี ซึ่งปัจจัยด้านข้อมูลรายงานทางการเงินในระบบ เป็นสิ่งสำคัญมากที่สุดที่ใช้ในการตัดสินใจ รองลงมาเป็นส่วนประกอบของโปรแกรมซอฟต์แวร์ และอุปกรณ์คอมพิวเตอร์ (Phan Đüc Düng and Pham Anh Tuãn, 2015)

ในขณะเดียวกัน Dan Eigeles ได้ทำการศึกษาเรื่องการควบคุมภายในของระบบสารสนเทศทางการบัญชีในสภาพแวดล้อมของระบบเครือข่าย โดยใช้โครงสร้างการทำงานระหว่างระบบการควบคุมภายในกับระบบบัญชีให้สอดคล้องกับหลักการยืนยันตัวตนและระบุตัวตนของ I3A (Intelligent Authentication, Authorization and Administration) ซึ่งผลการศึกษาชี้ให้เห็นว่า ประสิทธิภาพของการตรวจสอบสิทธิ,กำหนดสิทธิเข้าใช้งาน และการบริหารจัดการแบบอัจฉริยะในด้านการยอมรับกรอบการดำเนินงานที่มีความยืดหยุ่นและครอบคลุมสำหรับปัญหา, นำแนวทางปฏิบัติที่เป็นไปได้ของการสื่อสารที่มีความปลอดภัยมาใช้ในระบบรักษาความปลอดภัยการใช้งานระบบ และหลักการ I3A สามารถจัดหาโครงสร้างแบบเปิดซึ่งมีการให้อำนาจในด้านการสื่อสารที่มีความปลอดภัยและการบริหารจัดการกระบวนการของสภาพแวดล้อมของการใช้งานซอฟต์แวร์ระบบ Firmware สำหรับอุปกรณ์อิเล็กทรอนิกส์แบบพกพา อย่างเช่น แท็บเล็ตและโทรศัพท์มือถือ เป็นต้น และอุปกรณ์คอมพิวเตอร์ ซึ่งทุกคนสามารถได้รับประโยชน์ โดยไม่จำเป็นต้องมีความรู้ทักษะพิเศษหรือความพยายามในการลงทุนภายนอก (Dan Eigeles, 2006)

ซึ่งการควบคุมภายในและการนำระบบสารสนเทศมาช่วยในการทำงานด้านการเงินและบัญชี ได้ส่งผลกระทบถึงประสิทธิภาพในการปฏิบัติงานด้านการเงินและบัญชีของหน่วยงานภาครัฐ ซึ่งงานวิจัยของ ภิรมย์พร เยาดำ ได้ทำการศึกษาประสิทธิของระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ (GFMIS) โดยใช้หน่วยงานในจังหวัดระนองเป็นกรณีศึกษา โดยผลการศึกษาปรากฏว่า ระบบ GFMIS มีประสิทธิภาพโดยรวมอยู่ในระดับที่ดี ในด้านความโปร่งใสในการทำงาน และด้านความถูกต้อง แม่นยำของข้อมูลในระบบ ซึ่งระบบ GFMIS เป็นระบบที่ช่วยเพิ่มประสิทธิภาพในการทำงานด้านการเงินการคลังของหน่วยงานภาครัฐให้ประสิทธิภาพทุกด้าน ยังช่วยเพิ่มประสิทธิภาพด้านการเงินการคลังภาครัฐของหน่วยงานให้ดียิ่งขึ้น (ภิรมย์พร เยาดำ, 2559)

2.3.2 ความสัมพันธ์หลักการควบคุมภายในกับการควบคุมเชิงเทคโนโลยีสารสนเทศ

การควบคุมภายในของระบบสารสนเทศทางการบัญชีในสภาพแวดล้อมของระบบเครือข่าย โดยใช้โครงสร้างการทำงานระหว่างระบบการควบคุมภายในกับระบบบัญชีให้สอดคล้องกับหลักการควบคุมภายในแบบกรอบการทำงาน COSO ซึ่งหลักการควบคุมภายในของหน่วยงาน

ทั้งภาครัฐและเอกชนจะประสบผลสำเร็จนั้นขึ้นอยู่วัตถุประสงค์ในการดำเนินงานด้านการเงินการบัญชี สภาพแวดล้อมของหน่วยงาน ความพร้อมของอุปกรณ์ในการใช้งานระบบสารสนเทศทางการบัญชี รวมทั้งโครงสร้างหน่วยงานที่เป็นไปตามมาตรฐานที่กำหนดและ นโยบายการพัฒนาบุคคลให้มีความรู้ความสามารถพื้นฐานในการใช้งานระบบสารสนเทศทางการบัญชี เพื่อให้การบริหารจัดการและพัฒนาระบบควบคุมภายในระบบสารสนเทศทางบัญชีภายในหน่วยงานมีประสิทธิภาพมากขึ้น และลดความเสี่ยงที่อาจจะเกิดขึ้นทันท่วงที (ธารินี เณรวงศ์, 2558; GAO Fanxiu, 2016)

ในขณะนั้น Michele Rubino Filippo Vitolla และ Antonello Garzoni ได้ทำการศึกษาเรื่องความสัมพันธ์ระหว่างการควบคุมเชิงเทคโนโลยีสารสนเทศ กับสภาพแวดล้อมในการควบคุม โดยใช้หลักการวิเคราะห์การควบคุมบนพื้นฐาน 3 อย่าง คือ Organizational Controls, Process Controls และ Soft variables Controls หลักการการควบคุมภายในจะประสบผลสำเร็จได้ขึ้นอยู่กับการบริหารจัดการและพนักงานในองค์กร การนำหลักการควบคุมเชิงเทคโนโลยีสารสนเทศมาใช้ในการวิเคราะห์โครงสร้างการควบคุมสภาพแวดล้อมอยู่บนพื้นฐานของหลักการการควบคุมทั่วไป และการควบคุมเฉพาะระบบปฏิบัติการ นอกจากนั้น ผู้จัดการ และผู้สอบบัญชีสามารถศึกษาความรู้ในเรื่องการควบคุมเชิงเทคโนโลยีสารสนเทศ และเข้าใจกระบวนการทำงานขององค์กร รวมทั้งสามารถระบุความเสี่ยงที่เกิดขึ้นได้ในระบบการควบคุมภายใน (How IT controls improve the control environment) และได้ทำการศึกษาผลกระทบของกรอบการดำเนินงานด้านธรรมาภิบาลเทคโนโลยีสารสนเทศ (IT Governance) ที่ส่งผลต่อสภาพแวดล้อมของการควบคุมภายในองค์กร โดยอ้างอิงโครงสร้างและกระบวนการทำงานของกรอบการดำเนินงานการควบคุมภายในด้านเทคโนโลยีสารสนเทศ(COBIT) ตามหลักการ 5 ประการ ได้แก่ Evaluate, direct and monitor (EDM); Align, plan and organize (APO); Build, acquire and implement (BAI); Deliver, service and support (DSS); และMonitor, evaluate and assess (MEA) ซึ่งหลักการดังกล่าวสามารถนำไปปรับปรุงกระบวนการทำงานด้านสภาพแวดล้อมการควบคุมในภาพรวม รวมทั้งช่วยให้ผู้บริหารและผู้สอบบัญชีสามารถบริหารความเสี่ยงภายในด้านระบบเทคโนโลยีสารสนเทศทางการบัญชีได้ และป้องกันความเสี่ยงจากการใช้งานระบบที่อาจจะเกิดขึ้นในอนาคต (Michele Rubino Filippo Vitolla and Antonello Garzoni, 2017)

2.3.3 หลักการกำกับดูแลที่ดีเชิงเทคโนโลยีสารสนเทศ (IT Governance)

การกำกับดูแลที่ดีเชิงเทคโนโลยีสารสนเทศเป็นส่วนหนึ่งในหลักการกำกับดูแลกิจการที่ดี (Good Governance) อย่างเช่น การศึกษาวิจัย ของ Dr.Talal H.Hayale และ Dr.Husam A.Abu Khadra ซึ่งเป็นการศึกษาเรื่องการสืบสวนอุปสรรคของการรักษาความปลอดภัยระบบสารสนเทศทางการบัญชี โดยใช้หน่วยงานธนาคารของประเทศจอร์แดนเป็นกรณีศึกษา ซึ่งผลการวิจัย แสดงให้เห็นว่า อุปสรรคที่ทำให้การรักษาความปลอดภัยระบบสารสนเทศทางการบัญชีที่ธนาคารของประเทศจอร์แดน ได้ประสบปัญหา 3 อันดับแรก คือ 1.พนักงานป้อนข้อมูลที่ไม่เหมาะสมด้วยความประมาทเลินเล่อ, 2.พนักงานลบข้อมูลโดยไม่ได้ตั้งใจ และ 3.พนักงานจงใจป้อนข้อมูลที่ไม่เหมาะสม และส่วนใหญ่จะเป็นปัญหาที่เกิดจากความประมาทเลินเล่อของพนักงานธนาคารเอง (Talal H.Hayale and Husam A. Abu Khadra, 2008)

นอกจากนั้น ยังมีกรอบการควบคุมภายในเชิงเทคโนโลยีสารสนเทศอื่นๆ ที่ช่วยให้การดำเนินงานด้านเทคโนโลยีได้อย่างรัดกุม และเป็นการควบคุมความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ ได้แก่ งานวิจัยของ Semir Ibrahimovic และ Ulrik Franke ได้ทำการศึกษาเรื่องความน่าจะเป็นเรื่องการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศในรูปแบบของกรอบการดำเนินงาน Basel II ซึ่งเป็นการกรอบการควบคุมภายในของธนาคารทั่วโลกที่นิยมใช้กัน โดยทำการวิเคราะห์ข้อมูลความเสี่ยงเหตุการณ์ต่างๆของธนาคารขนาดกลางของประเทศบอสเนียมาเป็นกรณีศึกษา โดยผลการศึกษาชี้ให้เห็นความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งกรอบการดำเนินงาน Basel II ไม่ได้รวมไว้ และนำกรอบการดำเนินงาน Basel II มาพัฒนาในด้านการควบคุมภายในเชิงเทคโนโลยีสารสนเทศของธนาคารให้มีคุณภาพและป้องกันเหตุการณ์ความเสี่ยงที่จะส่งผลกระทบต่อการดำเนินงานของธนาคาร (Semir Ibrahimovic and Ulrik Franke, 2017)

โดยกรอบงานส่วนใหญ่ที่องค์กรนิยมใช้งานกันมากที่สุด คือกรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร ตามวัตถุประสงค์การควบคุมภายในด้านสารสนเทศและเทคโนโลยีที่เกี่ยวข้อง (Control Objectives for Information and related Technology : COBIT) เพื่อให้หลักการควบคุมภายในเทคโนโลยีสารสนเทศขององค์กรมีความสอดคล้องกับสภาพแวดล้อมและนโยบายด้านการควบคุมภายใน นอกจากนั้นมีการพัฒนาปรับปรุง และทบทวนกรอบงานการกำกับดูแลเทคโนโลยีสารสนเทศมาอย่างต่อเนื่องมาจนถึงปัจจุบัน

ให้เหมาะสมกับ การใช้งานขององค์กร อย่างเช่น งานวิจัยของ วรัญญาภรณ์ สิริพิพัฒนพร และสมชาย นำประเสริฐชัย ได้ทำการศึกษาประเด็นความเสี่ยงด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐ โดยใช้หลักการ CoBit 3 ที่ใช้ในกระบวนการธุรกิจ ซึ่งชี้ให้เห็นความเสี่ยงด้าน ICT ของหน่วยงานภาครัฐประสบอยู่ในด้านการขาดแคลนบุคคลากรที่มีความรู้ความสามารถด้านเทคโนโลยีสารสนเทศ ทักษะคอมพิวเตอร์ขั้นสูง และด้านการเงินการคลัง เนื่องจากเงินงบประมาณที่ได้รับมาไม่เพียงพอต่อการพัฒนาระบบ และความต้องการด้านเทคโนโลยีสารสนเทศของคนในหน่วยงาน และได้มีการแสดงตารางการควบคุมความเสี่ยงทางสารสนเทศของปัญหาที่หน่วยงานพบ เพื่อใช้เป็นหลักในการควบคุมความเสี่ยงด้าน ICT ของหน่วยงานให้มีประสิทธิภาพ (วรัญญาภรณ์ สิริพิพัฒนพร และสมชาย นำประเสริฐชัย, 2558)

นอกจากนั้น องค์กรมีการนำกิจกรรมของกระบวนการในกรอบการดำเนินงาน COBIT มาใช้ในการกำกับดูแลด้านเทคโนโลยีสารสนเทศขององค์กร โดยแสดงให้เห็นความสำคัญของกระบวนการภายใต้กรอบการดำเนินงาน COBIT แต่ละข้อที่มีส่วนช่วยด้านการดำเนินงานด้านเทคโนโลยีสารสนเทศหรือสามารถนำใช้งานในองค์กรได้ตามสภาพแวดล้อม ซึ่งงานวิจัยของ Ahmad Abu-Musa มีการศึกษาความสำคัญและการนำกระบวนการ COBIT นำมาประยุกต์ใช้กับบริษัทในประเทศซาอุดิอาระเบีย โดยการทำแบบสอบถามบุคลากรในองค์กรแต่ละประเภทของธุรกิจ ได้แก่ ธุรกิจผลิตสินค้า, ให้บริการ, ธุรกิจน้ำมันและพลังงาน, หน่วยงานภาครัฐ เป็นต้น ซึ่งผลการศึกษาชี้ให้เห็นถึงความสำคัญของการนำ COBIT มาใช้ในหลักการกำกับดูแลด้านเทคโนโลยีสารสนเทศของบุคลากรในองค์กร เพื่อให้องค์กรสามารถดำเนินงานได้อย่างต่อเนื่อง และบรรลุเป้าหมายวัตถุประสงค์ที่องค์กรได้กำหนดไว้ (Ahmad Abu-Musa, 2008)

ในขณะเดียวกัน องค์กรภาครัฐมีการนำกรอบงาน COBITมาประยุกต์ใช้ให้เข้ากับสภาพแวดล้อมในการทำงานด้านเทคโนโลยีสารสนเทศขององค์กร อย่างเช่น งานวิจัยของ Loai Al Omari, Paul Barnes และ Grant Pitman เป็นการศึกษาด้านเพิ่มประสิทธิภาพในการนำ COBIT 5มาใช้ในการกำกับดูแลเชิงเทคโนโลยีสารสนเทศ โดยใช้หน่วยงานภาครัฐ ในรัฐ Queensland ของประเทศออสเตรเลียเป็นตัวอย่างในการศึกษา และผลการศึกษาได้แสดงให้เห็นถึงความสำคัญของกระบวนการกำกับดูแลการใช้งานเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐ รวมทั้งความเป็นไปได้ในการเป็นส่วนหนึ่งของกรอบงานด้านการตรวจสอบการกำกับดูแลด้านเทคโนโลยีสารสนเทศที่มีความยั่งยืน ซึ่งในอนาคตกรอบการตรวจสอบ

ด้านเทคโนโลยีสารสนเทศมีการพัฒนาด้านตัวชี้วัดการตรวจสอบของชุดกระบวนการด้านการบริหารจัดการเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐในปัจจุบันและอนาคต (Loai Al Omari, Paul Barnes and Grant Pitman, 2012)

กรอบการดำเนินงาน COBIT เป็นเครื่องมือด้านการกำกับดูแลสามารถนำมาใช้งานด้านการควบคุมการใช้งานเทคโนโลยีสารสนเทศภายในองค์กรของผู้บริหารระดับสูง นอกจากนั้นยังเครื่องมือสำหรับผู้ตรวจสอบภายใน เพื่อใช้ในการให้คำแนะนำแก่ผู้บริหารระดับสูงในด้านเทคโนโลยีสารสนเทศ และนำไปสู่การพัฒนาระบบการตรวจสอบให้มีประสิทธิภาพมากขึ้นเหมือนกับการศึกษาด้านการตรวจสอบหลักการกำกับดูแลเทคโนโลยีสารสนเทศของ Mayang Anglingsari, Vivin Ayu Lestari และ Ismiarta Akunuranda โดยนำ PT.XY มาเป็นกรณีศึกษา ซึ่งมีการวัดระดับค่าการพัฒนาปรับปรุงระบบการควบคุมภายในและการกำกับดูแลด้านเทคโนโลยีสารสนเทศและวิเคราะห์ช่องว่างระหว่างระดับค่าการพัฒนาปรับปรุงและระบบที่ควรจะเป็น โดยผลการศึกษาได้ชี้ให้เห็นถึงช่องว่างของแต่ละกระบวนการบริหารจัดการเทคโนโลยีสารสนเทศของกรอบงาน COBIT 4.1 ที่องค์กรควรนำมาพัฒนาหรือปรับปรุงระบบการควบคุมภายในให้ดีขึ้น (Mayang Anglingsari, Vivin Ayu Lestari and Ismiarta Akunuranda, 2017)

ยังเป็นแนวทางสำหรับการบริหารความเสี่ยงด้านการใช้งานบนเครือข่ายอินเตอร์เน็ตของผู้บริหารระดับสูง และผู้ตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ โดยมีการศึกษากรอบงานของ COBIT 5 สำหรับการบริหารความเสี่ยงด้านการใช้งานที่เกี่ยวข้องกับสิ่งของที่มีการเชื่อมต่อกับอินเตอร์เน็ต (Internet of Things : IoT) ซึ่งให้ความสำคัญในด้านข้อมูลและโปรแกรม, ความปลอดภัยของอินเตอร์เน็ต การบริหารความเปลี่ยนแปลง ความร่วมมือของผู้ค้า โครงสร้างของระบบ และสภาพแวดล้อมทางกายภาพเป็นหลัก และผลการศึกษายังแสดงให้เห็นถึงกลยุทธ์ด้านการบริหารความเสี่ยงภายใต้กรอบงาน COBIT 5 ที่หน่วยงานนิยมใช้ สามารถนำมาปรับปรุงเกณฑ์คุณภาพการบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Faride Latifi and Houman Zarrabi, 2017)

นอกจากการนำหลักการ COBIT 5 มาใช้ในการวางแผน และการสร้างระบบสารสนเทศ ยังให้ความสำคัญในด้านการให้บริการระบบสารสนเทศแก่ผู้ใช้งาน โดยมีการศึกษาการพื้นฐานการตรวจสอบการกำกับดูแลที่ดีเชิงเทคโนโลยีสารสนเทศใช้แผนกการฝึกอบรมเป็นกรณีศึกษา โดยผลการศึกษาปรากฏว่า ธุรกิจมีการดำเนินการแต่ไม่ถึงระดับที่คาดหวังไว้ตามข้อปฏิบัติตามหลัก COBIT 5 ด้านส่งมอบ

ด้านส่งมอบ บริการและสนับสนุน (DSS) ซึ่งกระบวนการกำกับดูแลที่ดีเชิงเทคโนโลยี (IT Governance) ของแผนกการฝึกอบรมจะมีแบบแผนและมีการทำซ้ำ (Johanes Fernandes Andry, 2016)

ในปัจจุบัน หลักการและมาตรฐานการควบคุมและกำกับดูแลการใช้เทคโนโลยีสารสนเทศให้มีประสิทธิภาพในการทำงานภายในองค์กร ซึ่งหลักการเหล่านี้สามารถนำมาประยุกต์ด้วยกันได้ อย่างเช่น การนำกรอบงาน COBIT และหลักการ ISO 27001 มาใช้งานร่วมกันในด้านการควบคุมระบบความปลอดภัยของเทคโนโลยีสารสนเทศ มีการศึกษาข้อดีข้อเสียของการใช้งานมาตรฐาน ISO 27001, COBIT และการใช้งานกรอบงาน COBIT ควบคู่กับ ISO 27001 ซึ่งข้อดีของ ISO 27001 ในด้านความปลอดภัยของการใช้งานเทคโนโลยีสารสนเทศ ส่วนของกรอบงาน COBIT มีข้อดีในด้านแนวทางการปฏิบัติ แต่การนำกรอบงานทั้งสองมาใช้ควบคู่กันจะช่วยอำพรางข้อบกพร่องซึ่งกันและกันในด้านการควบคุมและกำกับดูแลการใช้งานเทคโนโลยีสารสนเทศ จึงจำเป็นต้องมีหลักการหรือแนวทางในการปฏิบัติมาใช้คู่กัน เพื่อเพิ่มประสิทธิภาพในการกำกับดูแลด้านเทคโนโลยีสารสนเทศขององค์กรให้สามารถทำงานได้อย่างต่อเนื่อง (Tolga MATARACIOGLU and Sevgi OZKAN, 2011) ยังมีบางหน่วยงานที่ยังนำหลัก COBIT 5 และมาตรฐานด้านความปลอดภัยอย่าง ISO/IEC 27001 มาช่วยในการแก้ไขปัญหาในการทำงานด้านเทคโนโลยีสารสนเทศ อย่างเช่นการศึกษาและวิเคราะห์ช่องว่างในการทำงานด้านเทคโนโลยีสารสนเทศ ซึ่งผลการศึกษาได้กล่าวถึงกระบวนงาน COBIT 5 ที่หน่วยงานที่เป็นกรณีศึกษาควรให้ความสำคัญกับกระบวนการ COBIT 5 และมาตรฐานด้านความปลอดภัย รวมทั้งศึกษาปัญหาด้านเทคโนโลยีสารสนเทศของบริษัทให้เป็นไปกรอบการดำเนินงานด้านเทคโนโลยีสารสนเทศ (ธัญญรัตน์ ปิยวัฒน์กานนท์ และชุติมา เบี้ยวไข่มุข, 2560)

นอกจากนั้นมีการเปรียบเทียบการนำงานวิจัยด้านมาตรฐานการควบคุมภายในที่ดีเชิงเทคโนโลยีสารสนเทศในรูปแบบของ COBIT 5 ซึ่งงานวิจัยของ Savanid Vatanasakdakul, Atichat Preittigun และ Wachara Chantatub ได้มีการนำงานวิจัยที่เกี่ยวกับการควบคุมที่ดีเชิงเทคโนโลยีสารสนเทศ (IT Governance) มาเปรียบเทียบและจับคู่ให้กับกระบวนการบริหารจัดการเทคโนโลยีสารสนเทศตามกรอบงาน COBIT 5 และผลการศึกษา ปรากฏว่า กรอบงาน COBIT 5 มีหัวข้อที่เหมือนกันและแตกต่างกัน ซึ่งหัวข้อที่

เหมือนกันด้านการควบคุมที่ดีเชิงเทคโนโลยีสารสนเทศจะเหมือนกับหัวข้อการกำกับดูแลของ COBIT 5 ในเรื่องการสร้างระบบการควบคุมดูแล, การส่งมอบคุณค่าทางธุรกิจ และการบริหารของความเสี่ยงและทรัพยากรในองค์กร (Savanid Vatanasakdakul, Atichat Preittigun and Wachara Chantatub, 2012)

ขอบเขตการวิจัย

กระบวนการบริหารจัดการเทคโนโลยีสารสนเทศตามกรอบงานโคบิต 5.0 (COBIT 5.0)
1. การกำกับดูแล (Evaluate, Direct, Monitor: EDM) 1.1 EDM01 มั่นใจในการกำหนดกรอบการดำเนินงานการกำกับดูแลและการบำรุงรักษา 1.2 EDM02 มั่นใจในการส่งมอบผลประโยชน์ 1.3 EDM03 มั่นใจในความเสี่ยงที่เหมาะสม 1.4 EDM04 มั่นใจในการใช้ทรัพยากรให้เกิดประโยชน์สูงสุด 1.5 EDM05 มั่นใจในความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย
2. การวางแผน (Align, Plan, Organize: APO) 2.1 APO01 บริหารจัดการกรอบการดำเนินงานด้านบริหารงานด้าน IT 2.2 APO02 บริหารจัดการกลยุทธ์ 2.3 APO03 บริหารจัดการสถาปัตยกรรมองค์กร 2.4 APO04 บริหารจัดการนวัตกรรม 2.5 APO05 บริหารจัดการกลุ่มของชุดโครงการ 2.6 APO06 บริหารจัดการงบประมาณและต้นทุน 2.7 APO07 บริหารจัดการทรัพยากรบุคคล 2.8 APO08 บริหารจัดการความสัมพันธ์ 2.9 APO09 บริหารจัดการข้อตกลงการให้บริการ 2.10 APO10 บริหารจัดการผู้ขายหรือผู้ให้บริการ 2.11 APO11 บริหารจัดการคุณภาพ 2.12 APO12 บริหารจัดการความเสี่ยง 2.13 APO13 บริหารจัดการความมั่นคงปลอดภัย
3. การสร้าง (Build, Acquire, Implement : BAI) 3.1 BAI01 บริหารจัดการโครงการและชุดโครงการ 3.2 BAI02 บริหารจัดการข้อกำหนดความต้องการ 3.3 BAI03 บริหารจัดการระบุและจัดสร้างกระบวนการแก้ปัญหาแบบเบ็ดเสร็จ 3.4 BAI04 บริหารจัดการความพร้อมใช้งานและขีดความสามารถ 3.5 BAI05 บริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล 3.6 BAI06 บริหารจัดการการเปลี่ยนแปลง 3.7 BAI07 บริหารจัดการการยอมรับการเปลี่ยนแปลงและการปรับเปลี่ยน

กระบวนการบริหารจัดการเทคโนโลยีสารสนเทศตามกรอบงานโคบิต 5.0 (COBIT 5.0)
3. การสร้าง (Build, Acquire, Implement : BAI) 3.8 BAI08 บริหารจัดการความรู้ 3.9 BAI09 บริหารจัดการทรัพย์สิน 3.10 BAI10 บริหารจัดการองค์ประกอบของระบบ
4. การส่งมอบ (Deliver, Service, Support : DSS) 4.1 DSS01 บริหารจัดการการปฏิบัติการ 4.2 DSS02 บริหารจัดการคำร้องขอบริการและเหตุการณ์ที่เกิดขึ้น 4.3 DSS03 บริหารจัดการปัญหา 4.4 DSS04 บริหารจัดการความต่อเนื่อง 4.5 DSS05 บริหารจัดการด้านความปลอดภัย 4.6 DSS06 บริหารจัดการการควบคุมกระบวนการทางธุรกิจ
5. การติดตาม (Monitor, Evaluate, Assess : MEA) 5.1 MEA01 เฝ้าติดตาม วัดผลและประเมินประสิทธิภาพและความสอดคล้องในการดำเนินงาน 5.2 MEA02 เฝ้าติดตาม วัดผลและประเมินระบบการควบคุมภายใน 5.3 MEA03 เฝ้าติดตาม วัดผลและประเมินการปฏิบัติตามข้อกำหนดของหน่วยงานภายนอก