บทที่ 2

แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

การศึกษางานวิจัยฉบับนี้ ต้องอาศัยแนวคิดและทฤษฎีประกอบในการศึกษาและวิเคราะห์ข้อมูล เพื่อเป็นแนวทางในการสร้างกรอบความคิดในการทำงานวิจัย ให้งานวิจัยมีความถูกต้อง น่าเชื่อถือ มีประสิทธิภาพ และเพื่อให้มีความเข้าใจที่ตรงกันในงานวิจัยฉบับนี้ จึงขออธิบายแนวคิดและทฤษฎีที่เกี่ยวข้องดังต่อไปนี้

2.1 ระบบสารสนเทศ

2.1.1 ความหมายของระบบสารสนเทศ (Information System)

ระบบสารสนเทศ[1] หมายถึง ระบบที่มีการใช้คอมพิวเตอร์เข้ามาช่วยจัดการข้อมูลข่าวสารเพื่อให้ได้มาซึ่งสารสนเทศ เพื่อนำไปประกอบการตัดสินใจในเวลาอันรวดเร็วและถูกต้องที่สุด ดังนั้น ระบบสารสนเทศในที่นี้จึงประกอบไปด้วย ฮาร์ดแวร์ ซอฟต์แวร์ ผู้ใช้ กระบวนการ และตัวข้อมูลหรือสารสนเทศ โดยมีวัตถุประสงค์ที่ชัดเจนสามารถตรวจสอบและประเมินผลระบบได้

ระบบสารสนเทศ[2] หมายถึง องค์ประกอบต่างๆ ที่มีความเกี่ยวข้องและทำงานประสานกันในการเก็บรวบรวม บันทึก ประมวลผล จัดเก็บ และแจกจ่ายสารสนเทศ เพื่อการสนับสนุนการตัดสินใจและหน้าที่ทางการบริหาร ซึ่งได้แก่ การวางแผน การจัดองค์กร การประสานงาน การควบคุม และการสื่อสารภายในองค์กร

ระบบสารสนเทศ[3] หมายถึง ระบบที่ประกอบด้วย ผู้ใช้ระบบ ผู้พัฒนาระบบ พนักงานที่เกี่ยวข้อง ผู้เชี่ยวชาญในสาขา ระบบคอมพิวเตอร์ทั้งฮาร์ดแวร์และซอฟต์แวร์ ตัวแบบการวิเคราะห์ ระบบเครือข่าย และฐานข้อมูลที่ทำงานร่วมกัน เพื่อกำหนด รวบรวม และจัดเก็บข้อมูล

---

[1] วิเศษศักดิ์ โคตรอาษา, เทคโนโลยีสารสนเทศเพื่อการเรียนรู้, (กรุงเทพฯ: เธิร์ดเวฟเอ็ดดูเคชั่น, 2542), 9.

[2] เอก บุญเจือ, ระบบสารสนเทศทางการตลาด, (กรุงเทพฯ: โปรวิชั่น, 2545), 12.

[3] สุชาดา กีระนันทร์, คอมพิวเตอร์และระบบสารสนเทศ, (กรุงเทพฯ: ซีเอ็ดยูเคชั่น, 2545), 24.

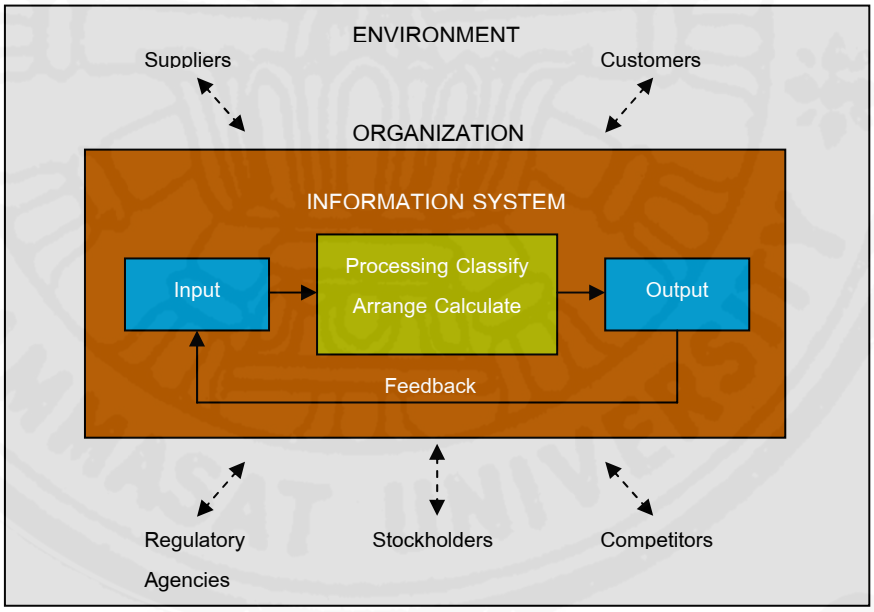
ทำการประมวลผลข้อมูล เพื่อสร้างสารสนเทศ และส่งผลลัพธ์ หรือสารสนเทศให้ผู้ใช้ เพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม การวิเคราะห์และติดตามผลการดำเนินงานขององค์กร เพื่อประโยชน์ในการบริหารองค์กรนั้น

2.1.2 กระบวนการทำงานของระบบสารสนเทศ[4]

กระบวนการทำงานของระบบสารสนเทศประกอบด้วยกิจกรรม 3 อย่างดังแสดงในภาพที่ 2.1 คือ (1) การนำข้อมูลเข้าสู่ระบบ (2) การประมวลผล และ (3) การนำเสนอผลลัพธ์

ภาพที่ 2.1

โครงสร้างของระบบสารสนเทศ



การนำข้อมูลเข้าสู่ระบบ (Input) คือ การจัดการรวบรวมข้อมูลจากส่วนต่างๆ ขององค์กร หรือจากสิ่งแวดล้อมภายนอกองค์กร

---

[4] Laudon, K. C. and Laudon, J. P, ระบบสารสนเทศเพื่อการจัดการ, แปลโดย สัลยุทธ์ สว่างวรรณ, (กรุงเทพฯ: เพียร์สัน เอ็ดดูเคชั่น อินโดไชน่า, 2545), 7.

การประมวลผล (Processing) คือ การทำหน้าที่ปรับเปลี่ยนข้อมูลที่นำเข้ามาให้อยู่ในรูปแบบที่มีความหมายต่อองค์กร ซึ่งสามารถนำไปใช้งานได้

การนำเสนอผลลัพธ์ (Output) คือ การจัดการนำข่าวสารหรือข้อมูลที่ผ่านการประมวลผลแล้ว ไปเสนอให้แก่ผู้ใช้ตามความเหมาะสม หรือนำไปส่งต่อให้กับส่วนอื่นซึ่งต้องนำข่าวสารนี้ไปใช้งานต่อไป

ระบบสารสนเทศบางระบบต้องการ **การตอบสนอง** (Feedback) ซึ่งก็คือส่วนหนึ่งของข้อมูลที่ผ่านการประมวลผลแล้ว แต่ถูกส่งกลับเข้าไปยังส่วนการนำเข้าข้อมูลอีกครั้งหนึ่ง เพื่อการตรวจสอบคุณภาพ หรือการปรับแต่งระบบให้มีความสอดคล้องกับสภาวะที่ต้องการ

2.2 ความเสี่ยง และการประเมินความเสี่ยง

2.2.1 ความหมายของความเสี่ยง

ความเสี่ยง[5] คือ โอกาสที่เหตุการณ์บางอย่างอาจเกิดขึ้นและมีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร ระดับของความเสี่ยงสามารถวัดได้จากผลที่ตามมา (Consequence) และโอกาสที่เหตุการณ์ของความเสี่ยงจะเกิดขึ้น (Likelihood)

2.2.2 ความเสี่ยงของการใช้ระบบสารสนเทศ[6]

การนำระบบสารสนเทศมาใช้ในองค์กรมีผลกระทบในด้านต่างๆ เช่น การรักษาความปลอดภัยของข้อมูลมีความสลับซับซ้อนมากขึ้น เพิ่มระดับของการพึ่งพาต่อระบบสารสนเทศ การควบคุมภายในมีความสลับซับซ้อนมากขึ้น และข้อผิดพลาดต่างๆ อาจส่งผลกระทบที่รุนแรง และรวดเร็วขึ้น

ดังนั้น องค์กรที่นำระบบสารสนเทศมาใช้ควรจะจัดให้มีกลไกในการควบคุม เพื่อที่จะรับมือกับผลกระทบที่กล่าวมาแล้ว แต่ก่อนที่จะลงมือสร้างกลไกการควบคุม ควรจะต้องรู้ให้ได้

---

[5] ตลาดหลักทรัพย์แห่งประเทศไทย และสมาคมผู้ตรวจสอบภายในแห่งประเทศไทย, แนวทางการตรวจสอบภายใน, (ปทุมธานี: ดูมายเบส, 2548), 63.

[6] วันชัย พิทักษ์กรณ์, "ความเสี่ยง และการประเมินความเสี่ยงของเทคโนโลยีสารสนเทศ," eLeader ฉบับที่ 168 (กุมภาพันธ์ 2546): 72-74.

เสียก่อนว่าองค์กรจะต้องจัดการประเด็นใดบ้าง และในลำดับใด ซึ่งกล่าวอีกนัยหนึ่งก็คือ องค์กรต้องจัดให้มีการ “ประเมินความเสี่ยง”

ภาพที่ 2.2
ขั้นตอนของการประเมินความเสี่ยง

การทำความเข้าใจวัตถุประสงค์

ก่อนที่จะเริ่มประเมินความเสี่ยง สิ่งแรกที่องค์กรควรทำความเข้าใจก็คือ อะไรคือวัตถุประสงค์ของระบบสารสนเทศ ซึ่งแนวทางในการกำหนดวัตถุประสงค์ ประกอบด้วย 7 คุณสมบัติ ดังนี้

- ประสิทธิผลของระบบสารสนเทศ (Effectiveness)
- ประสิทธิภาพของระบบสารสนเทศ (Efficiency)
- ความถูกต้องและความครบถ้วนของข้อมูลและระบบสารสนเทศ (Integrity)
- ความปลอดภัยของข้อมูลและระบบสารสนเทศ (Confidentiality)
- ความต่อเนื่องของการทำงานของระบบสารสนเทศ (Availability)
- การปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้อง (Compliance)
- ความน่าเชื่อถือของระบบสารสนเทศ (Reliability)

การระบุความเสี่ยง

เมื่อองค์กรรู้วัตถุประสงค์ของการใช้ระบบสารสนเทศแล้ว ลำดับถัดมาคือ การระบุความเสี่ยง ซึ่งก็คือสิ่งใดๆ ก็ตามที่เมื่อเกิดขึ้นแล้ว มีผลกระทบต่อวัตถุประสงค์ ดังนี้

ความมีประสิทธิผลของระบบสารสนเทศ Effectiveness

ความเสี่ยงที่อาจเกิดขึ้นมาจากการที่ระบบสารสนเทศอาจไม่สามารถตอบสนองต่อความต้องการทางธุรกิจได้อย่างทันท่วงที จากการที่ไม่สามารถนำระบบสารสนเทศไปใช้ในทาง

ปฏิบัติได้ ไม่สามารถเพิ่มมูลค่าให้กับองค์กร และไม่สามารถนำเสนอบริการใหม่ๆ ให้กับผู้ใช้บริการได้ เช่น ความเสี่ยงในการวางแผน การจัดโครงสร้างงานสารสนเทศที่ไม่เหมาะสม ขาดความร่วมมือจากผู้ใช้งาน และความเสี่ยงในกระบวนการพัฒนาระบบงาน เป็นต้น

ความมีประสิทธิภาพของระบบสารสนเทศ Efficiency

ความเสี่ยงที่ในการให้บริการด้านสารสนเทศอาจไม่มีประสิทธิภาพ โดยเฉพาะอย่างยิ่งด้านการบริหารและการใช้ทรัพยากรด้านสารสนเทศ เช่น ความเสี่ยงด้านการขาดแคลนบุคลากร การใช้เทคโนโลยีที่ล้าสมัย เป็นต้น

ความถูกต้องและความครบถ้วนของข้อมูล Integrity

ความเสี่ยงที่ข้อมูลอาจไม่ถูกต้องและครบถ้วน ซึ่งอาจสืบเนื่องมาจากการนำข้อมูลที่ผิดพลาดเข้าสู่ระบบ หรือการประมวลผลที่ไม่ถูกต้อง ซึ่งอาจมีผลกระทบต่อการดำเนินธุรกิจเนื่องจากใช้ข้อมูลไม่ถูกต้อง เช่น ความเสี่ยงด้านการนำข้อมูลเข้าสู่ระบบ ความเสี่ยงจากการประมวลผลผิดพลาด ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงข้อมูล เป็นต้น

การรักษาความลับ Confidentiality

ความเสี่ยงเกี่ยวกับการรักษาความลับและความปลอดภัยของข้อมูล และระบบสารสนเทศ หรือความเสี่ยงที่ข้อมูลอาจถูกเปิดเผยหรือใช้โดยที่ไม่ได้รับอนุญาต เช่น ความเสี่ยงจากการเจาะระบบ โครงสร้างการรักษาความปลอดภัย บุคลากรขาดความเอาใจใส่

การมีระบบใช้อย่างต่อเนื่อง Availability

ความเสี่ยงที่ระบบสารสนเทศอาจหยุดชะงัก และไม่สามารถให้บริการกับธุรกิจได้อย่างต่อเนื่อง เช่น ความเสี่ยงเกี่ยวกับอุบัติภัย อุบัติเหตุ เทคโนโลยีที่ล้าสมัย การไม่มีแผนฉุกเฉินและระบบเครือข่าย เป็นต้น

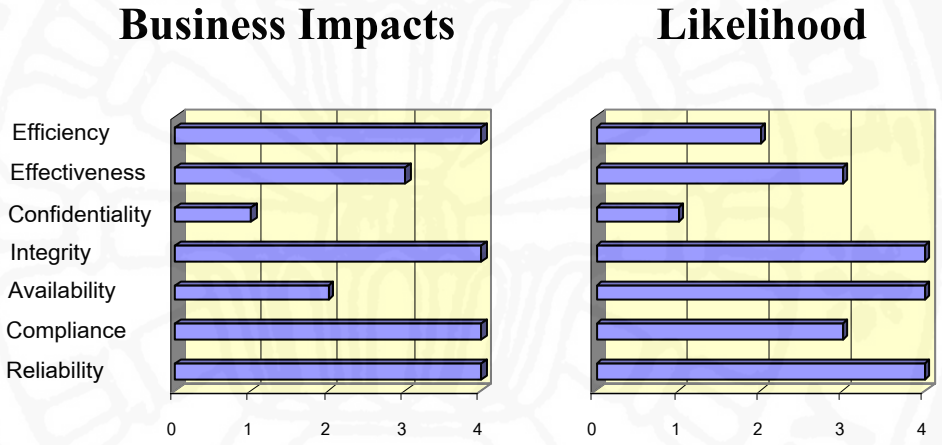
การปฏิบัติตามกฎเกณฑ์ Compliance

ความเสี่ยงที่ระบบสารสนเทศไม่สามารถช่วยให้องค์กรปฏิบัติตามกฎเกณฑ์ หรือกฎหมายที่เกี่ยวข้อง ได้อย่างมีประสิทธิภาพ

ความน่าเชื่อถือของระบบสารสนเทศ Reliability

ความเสี่ยงที่ระบบสารสนเทศขาดความน่าเชื่อถือ ซึ่งมีผลกระทบต่อความเชื่อมั่นต่อข้อมูลหรือรายงานต่างๆ จากระบบสารสนเทศ ทั้งรายงานเพื่อการบริหารงานภายใน และรายงานต่อบุคคลภายนอก เช่น ความผิดพลาดของโปรแกรม และข้อมูล ที่เกิดขึ้นบ่อยๆ เป็นต้น

ภาพที่ 2.3
การประเมินความสำคัญของแต่ละความเสี่ยง ทั้งด้านผลกระทบความเสี่ยง
และโอกาสที่จะเกิดขึ้น



การประเมินความสำคัญของความเสี่ยง

เมื่อองค์กรทราบความเสี่ยงทั้งหมดแล้ว ลำดับถัดมาก็คือการประเมินความสำคัญของแต่ละความเสี่ยง ซึ่งโดยทั่วไปจะทำการประเมิน 2 ด้านคือ ด้านโอกาสที่จะเกิด และด้านผลกระทบของความเสี่ยง ส่วนเกณฑ์ในการวัดนั้นอาจจะแตกต่างกันไป เช่น บางองค์กรใช้เกณฑ์ สูง กลาง และต่ำ บางองค์กรอาจใช้ตัวเลข 1 ถึง 5 เป็นต้น ส่วนวิธีการประเมินอาจใช้ผสมผสานกันระหว่างการประมาณการจากข้อมูลต่างๆ หรืออาจจะใช้วิธีที่ค่อนข้างเรียบง่ายคือ ประเมินตามความคิดเห็นของบุคคลที่เกี่ยวข้องกับความเสี่ยงนั้นๆ เช่น การจัดประชุมเชิงปฏิบัติการ เป็นต้น

จากวัตถุประสงค์ของการใช้ระบบสารสนเทศดังกล่าวข้างต้น โดยหลักการสากลของการควบคุมที่เป็นที่ยอมรับ สามารถสรุปได้ว่า ความเสี่ยงของการใช้ระบบสารสนเทศสามารถแบ่ง

ออกเป็น 2 ส่วนหลักๆ คือ (1) ความเสี่ยงด้านการควบคุมทั่วไป (General Control Risks) และ (2) ความเสี่ยงด้านการควบคุมเฉพาะระบบงาน (Application Control Risks)

2.2.3 ความเสี่ยงด้านการควบคุมทั่วไป (General Control Risk) ได้แก่

- ความเสี่ยงที่การจัดโครงสร้างงานสารสนเทศอาจไม่เอื้อต่อการจัดให้มีการควบคุมภายในที่ดี และไม่มีการแบ่งแยกงานสารสนเทศอย่างเหมาะสม
- การจัดทำระบบงานคอมพิวเตอร์ (Computer Application) อาจไม่สอดคล้องหรือไม่ตอบสนองต่อวัตถุประสงค์โดยรวมขององค์กรอย่างมีประสิทธิภาพ
- โปรแกรมคอมพิวเตอร์ที่ใช้งานอยู่ตามปกติอาจถูกเปลี่ยนแปลงโดยไม่เหมาะสมและไม่ถูกต้อง
- โปรแกรมคอมพิวเตอร์ และ/หรือ ข้อมูลที่จัดเก็บอยู่ในระบบคอมพิวเตอร์อาจถูกนำไปใช้งานหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
- ระบบคอมพิวเตอร์ที่ใช้ในการประมวลผลรายการทางธุรกิจ อาจเกิดเหตุขัดข้องแล้วส่งผลกระทบทำให้ธุรกิจหยุดชะงัก และ/หรือ ไม่อาจนำระบบกลับมาใช้ใหม่ได้ภายในเวลาอันสมควร

2.2.4 ความเสี่ยงด้านการควบคุมเฉพาะระบบงาน (Application Control Risks) ประกอบด้วย

- การแบ่งแยกหน้าที่ภายในระบบงานสารสนเทศอาจไม่เหมาะสม และไม่เอื้อให้มีการแบ่งแยกการทำงานภายในระบบงานอย่างเหมาะสม
- รายการต่างๆ อาจถูกนำเข้าสู่ระบบงานอย่างไม่ถูกต้อง ไม่ครบถ้วน ซ้ำซ้อน และไม่ตรงตามเงื่อนเวลา
- รายการที่เป็นรายการผิดปกติอาจไม่ได้ถูกแยกออก สอบทานและอนุมัติให้นำเข้าสู่การประมวลผลตามปกติอย่างเหมาะสม
- การรับส่งข้อมูลระหว่างระบบสารสนเทศอาจไม่ถูกต้อง ไม่ครบถ้วน ซ้ำซ้อน และไม่ตรงตามเงื่อนเวลา
- การประมวลผลรายการต่างๆ อาจไม่ถูกต้อง ไม่ครบถ้วน ซ้ำซ้อน และไม่ตรงตามเงื่อนไขเวลา

- ผลลัพธ์ที่ได้จากการประมวลผลโดยระบบสารสนเทศ อาจถูกนำไปใช้โดยไม่ได้รับอนุญาต

2.3 การตรวจสอบระบบสารสนเทศ

การตรวจสอบระบบสารสนเทศที่ใช้คอมพิวเตอร์ประมวลผล มักนิยมเรียกกันทับศัพท์ว่า “IT Audit” ซึ่งเมื่อสักยี่สิบปีก่อนจะใช้คำว่า “Electronic Data Processing Audit” ที่เรียกย่อๆ ว่า “EDP Audit” หรือ “Computer Audit” และในปัจจุบันนิยมเรียกว่า “IS Audit” ที่ย่อมาจาก “Information System Audit”

การตรวจสอบระบบสารสนเทศในทุกวันนี้ ถือเป็นเรื่องสำคัญที่ทุกองค์กรต้องปฏิบัติ ทั้งการตรวจสอบภายใน (Internal Audit) โดยพนักงานตรวจสอบขององค์กรเองโดยเฉพาะ ตลอดจนการตรวจสอบจากภายนอก (External Audit) เช่น การตรวจสอบจากบริษัทแม่ในต่างประเทศ หรือการตรวจสอบจากหน่วยงานที่มีหน้าที่ในการควบคุม เช่น ก.ล.ต. มีหน้าที่ตรวจสอบบริษัทหลักทรัพย์ หรือธนาคารแห่งประเทศไทยมีหน้าที่ตรวจสอบธนาคารพาณิชย์ เป็นต้น

หลักการในการตรวจสอบระบบสารสนเทศที่ถูกต้องก็คือ ต้องมีการประเมินความเสี่ยง (Risk Assessment) ขององค์กรเสียก่อน ซึ่งมีขั้นตอนสำคัญที่ต้องปฏิบัติ เช่น การระบุปัจจัยที่มีผลทำให้เกิดความเสี่ยง และการระบุความเสี่ยงที่มีโอกาสเกิดขึ้น (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการบริหารจัดการกับความเสี่ยง (Risk Management)

การตรวจสอบระบบสารสนเทศต้องพิจารณาเรื่องของ Control หรือการควบคุม ว่าได้มีการจัดการอย่างถูกต้องหรือไม่ การตรวจสอบการควบคุมแบ่งออกเป็น 3 ประเภทใหญ่ๆ คือ

1. การควบคุมแบบป้องกันล่วงหน้า (Preventive Control)
2. การควบคุมแบบค้นหาประวัติเหตุการณ์ที่เกิดขึ้น (Detective Control)
3. การควบคุมแบบแก้ไขปัญหาจากเหตุการณ์ที่เกิดขึ้น (Corrective Control)

IT Auditor ควรจะพิจารณาการควบคุม (Control) ไปพร้อมๆ กันทั้ง 3 มุมมอง ได้แก่

1. มุมมองทางด้านการบริหารจัดการ (Administrative Control)
2. มุมมองทางด้านเทคนิค (Technical Control)
3. มุมมองทางด้านกายภาพ (Physical Control)

IT Auditor ต้องมีความรู้ ความเข้าใจในขั้นตอนกระบวนการตรวจสอบระบบสารสนเทศ (IT Audit Process) ตลอดจนมีความรู้ด้านเทคนิคเชิงลึก (IT Audit Technical Know-how) ในระบบที่ต้องเข้าไปตรวจสอบ เราสามารถแบ่งประเภทของงานตรวจสอบระบบสารสนเทศออกเป็น 7 ประเภทใหญ่ๆ ดังนี้

การตรวจสอบในมุมมองทางด้านเทคนิค (Technical Control)

1. การตรวจสอบระบบปฏิบัติการ (NOS Audit) เช่น การตรวจสอบระบบ Server ที่ใช้ MS Windows เช่น Windows NT, Window 2000 Server ตลอดจน Workstation ที่ใช้ Windows XP เป็นต้น การตรวจสอบควรจะครอบคลุมถึงระบบปฏิบัติการอื่นด้วย เช่น การตรวจสอบระบบปฏิบัติการ Unix เช่น Sun Solaris, HP / UX, IBM AIX และระบบปฏิบัติการ Linux ที่ได้รับความนิยมเพิ่มขึ้นเรื่อยๆ

2. การตรวจสอบอุปกรณ์เครือข่าย (Network Devices Audit) เช่น การตรวจสอบ Router, การตรวจสอบ Switching และการตรวจสอบ Remote Access Server ตลอดจนการตรวจสอบโครงสร้างของเครือข่าย (Network Infrastructure Audit) และประสิทธิภาพของเครือข่าย (Network Performance Audit) โดยใช้โปรแกรมตรวจสอบประเภท Packet Sniffer หรือ RMON Probe เป็นต้น

3. การตรวจสอบอุปกรณ์รักษาความปลอดภัย (Security Devices Audit) เช่น การตรวจสอบ Firewall, การตรวจสอบ Intrusion Detection System (IDS), การตรวจสอบ Intrusion Prevention System (IPS), การตรวจสอบโปรแกรม Enterprise Anti-Virus, การตรวจสอบ VPN Server เป็นต้น การตรวจสอบอุปกรณ์รักษาความปลอดภัยนั้นเป็นสิ่งที่มีความจำเป็นอย่างสูง เพราะถ้าอุปกรณ์รักษาความปลอดภัยมีปัญหาเสียเอง หรือโดน Hacker เจาะเข้ามา compromised ก็จะทำให้เกิดปัญหากับความปลอดภัยของระบบโดยรวม

4. การตรวจสอบโปรแกรมฐานข้อมูล (RDBMS Audit) เช่น การตรวจสอบ Oracle, IBM DB2, Microsoft SQL Server, Informix, SYBASE หรือ MySQL RDBMS การตรวจสอบโปรแกรมฐานข้อมูลควรกระทำควบคู่ไปกับการตรวจสอบระบบปฏิบัติการที่โปรแกรมฐานข้อมูลทำงาน

อยู่ เช่น Oracle ทำงานบน Unix เป็นต้น เพื่อที่จะเจาะลึกลงไปในด้านความปลอดภัยของตัวโปรแกรมฐานข้อมูลเองว่ามีช่องโหว่หรือไม่

5. การตรวจสอบโปรแกรมประยุกต์และโปรแกรมที่ให้บริการในลักษณะ Server (Application Specific Audit) เช่น การตรวจสอบ Web Server IIS บน Microsoft Windows Platform และการตรวจสอบ Web Server Apache บน Unix / Linux Platform ซึ่งทั้ง 2 เป็นโปรแกรม Web Server ยอดนิยมอยู่ในขณะนี้ นอกจากการตรวจสอบ Web Server แล้ว IT Auditor ควรตรวจสอบ Mail Server, FTP Server, LDAP Server, RADIUS Server ตลอดจน DNS Server ซึ่งถือเป็นหัวใจหลักของระบบ หาก DNS Server มีปัญหาจะทำให้ระบบไม่สามารถอ้างอิง Hostname ได้ ซึ่งจะก่อให้เกิดปัญหาใหญ่กับระบบโดยรวม

<u>การตรวจสอบในมุมมองทางด้านการบริหารจัดการ</u> (Administrative Control)

6. การตรวจสอบกระบวนการบริหารจัดการควบคุมด้านสารสนเทศ (Administrative Control) ได้แก่ การตรวจสอบ Policy, Standard, Guideline และ Procedure ที่องค์กรมีอยู่ว่าครอบคลุม และมีการปฏิบัติตามหรือไม่ ในขั้นตอนนี้รวมถึงการตรวจสอบว่าองค์กรมีการจัดฝึกอบรมด้านการรักษาความปลอดภัย (Security Awareness Training) หรือไม่ ซึ่งตามปกติควรจะมีเป็นประจำทุกปี

   การตรวจสอบการบริหารจัดการนั้นต้องพิจารณาจากโครงสร้างหน่วยงาน, การแบ่งแยกหน้าที่ต่างๆ ในหน่วยงาน, การจัดทำแผนสำรองฉุกเฉิน และแผนรับเหตุการณ์ (Business Continuity Planning, Disaster Recovery Planning and Incident Response Procedure) ตลอดจนการควบคุมการเปลี่ยนแปลงระบบงาน (Change Control Management)

<u>การตรวจสอบในมุมมองทางด้านกายภาพ</u> (Physical Control)

7. การตรวจสอบด้านกายภาพ (Physical Control) ได้แก่ การตรวจสอบระบบควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์, การตรวจสอบ Hardware ระบบ Backup / Restore และระบบไฟ

สำรอง เช่น มี UPS เพียงพอหรือไม่ การตรวจสอบอุปกรณ์เฝ้าระวัง เช่น กล้องวงจรปิด (CCTV) เป็นต้น[7]

วิธีการในการตรวจสอบระบบสารสนเทศ จะมุ่งเน้นการตรวจสอบการควบคุมภายในของระบบเทคโนโลยีสารสนเทศในเรื่องต่างๆ ที่เกี่ยวข้อง เพื่อลดความเสี่ยงที่สามารถเกิดขึ้นได้ ซึ่งการควบคุมภายในระบบเทคโนโลยีสารสนเทศโดยทั่วไปนั้น จะแบ่งออกเป็น 2 ส่วน คือ

1. การควบคุมทั่วไป (General Controls) เป็นการควบคุมภายในที่เกี่ยวข้องโดยตรงกับสภาพแวดล้อมและการปฏิบัติงานของศูนย์คอมพิวเตอร์ การควบคุมการออกแบบ การรักษาความปลอดภัย การใช้โปรแกรมคอมพิวเตอร์ และความปลอดภัยของข้อมูลทั่งทั้งโครงสร้างระบบสารสนเทศขององค์กร ในภาพรวมแล้ว การควบคุมทั่วไปจะครอบคลุมไปถึงฮาร์ดแวร์ ซอฟต์แวร์ ขั้นตอนการปฏิบัติงาน เอกสารและทุกเรื่องที่เกี่ยวข้องกับคอมพิวเตอร์

2. การควบคุมระบบงาน (Application Controls) เป็นการควบคุมเฉพาะของแต่ละระบบงาน เช่น ระบบรายได้ ระบบสินค้าคงคลัง หรือระบบการจ่ายเงินเดือน เป็นต้น โดยครอบคลุมเกี่ยวกับความสมบูรณ์ ครบถ้วน ถูกต้องของการนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์ การประมวลผล และผลลัพธ์ที่ได้จากระบบคอมพิวเตอร์[8]

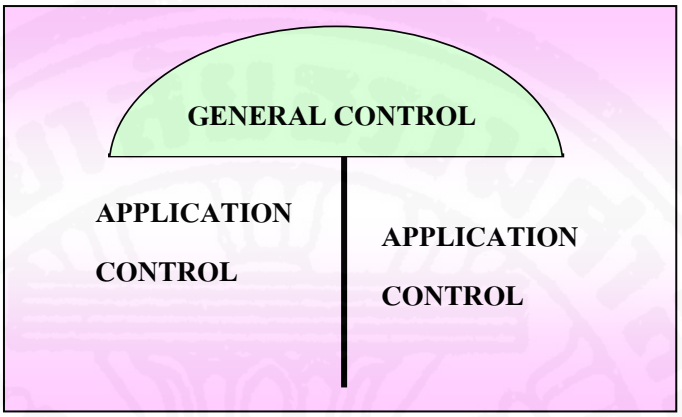
จะเห็นว่าการควบคุมทั่วไปจะมีลักษณะเหมือนร่มที่ครอบคลุมระบบงานเฉพาะต่างๆ ทั้งหมดดังภาพที่ 2.4 ดังนั้นถ้าการควบคุมภายในของการควบคุมทั่วไปมีไม่เพียงพอ ก็จะส่งผลกระทบต่อความน่าเชื่อถือในความครบถ้วน ถูกต้องของข้อมูลที่ได้จากระบบงานเฉพาะทุกระบบงาน ในขณะที่ถ้าการควบคุมภายในของระบบงานเฉพาะระบบใดระบบหนึ่งมีไม่เพียงพอ ก็จะกระทบความถูกต้องของข้อมูลระบบงานเฉพาะนั้นเพียงระบบเดียว

---

[7] ปริญญา หอมเอนก, “เรียนรู้หลักการตรวจสอบระบบสารสนเทศ (IT Audit) อย่างมีประสิทธิภาพในทางปฏิบัติ วิเคราะห์ปัญหาการตรวจสอบระบบสารสนเทศ และการแก้ปัญหาในเชิงบูรณาการ,” eWeek Thailand ปักษ์แรก (เมษายน 2547): 83-84.

[8] เจริญ เจษฎาวัลย์, ระบบควบคุมภายใน : หลักการและวิธีปฏิบัติ, (กรุงเทพฯ: พอดี, 2543), 39.

ภาพที่ 2.4
ความสัมพันธ์ระหว่างการควบคุมทั่วไป และการควบคุมระบบงาน



แต่ไม่ว่าจะจัดแบ่งอย่างไรก็ตาม ความรับผิดชอบในการตรวจสอบเทคโนโลยีสารสนเทศ (IT Auditing) ของผู้ตรวจสอบภายในควรจะครอบคลุมถึงเรื่องดังต่อไปนี้คือ

1) ระบบงาน (Application Systems)
2) การพัฒนาระบบงาน (System Development)
3) โครงสร้างองค์กร สถานที่ อุปกรณ์และสิ่งอำนวยความสะดวกต่างๆ (Installation and Facilities)

2.3.1 <u>การควบคุมทั่วไป (General Controls)</u>

การควบคุมทั่วไปเป็นการควบคุมที่กำหนดขึ้นเพื่อใช้ในหน่วยงานต่างๆ ขององค์กรที่เกี่ยวข้องกับการประมวลผลด้วย IT ให้มั่นใจว่าการประมวลผลข้อมูลด้วย IT จะเป็นไปอย่างเหมาะสม และการลงทุนในด้าน IT เหมาะสมและคุ้มค่า ซึ่งครอบคลุมในเรื่องทั่วไปเกี่ยวกับระบบสารสนเทศองค์กร ดังนี้

- การควบคุมกระบวนการพัฒนาระบบงาน
- การควบคุมซอฟต์แวร์
- การควบคุมทางกายภาพ
- การควบคุมการปฏิบัติงานเครื่องคอมพิวเตอร์

- การควบคุมความปลอดภัยข้อมูล
- ระเบียบวินัยผู้บริหาร มาตรฐาน และขั้นตอนการปฏิบัติงาน

การควบคุมกระบวนการพัฒนาระบบงาน (Implementation Controls) ตรวจสอบกระบวนการพัฒนาระบบงานในจุดต่างๆ เพื่อให้มั่นใจว่ากระบวนการพัฒนาฯ อยู่ในความควบคุมและการบริหารที่ดี การตรวจสอบการพัฒนาซอฟต์แวร์ควรที่จะมีการตรวจสอบทบทวนอย่างเป็นทางการในแต่ละขั้นตอนของการพัฒนาที่สำคัญ เพื่อเปิดโอกาสให้ผู้ใช้และผู้บริหารมีโอกาสยอมรับหรือปฏิเสธระบบงานเป็นระยะก่อนที่ระบบงานจะพัฒนาเสร็จเรียบร้อย การตรวจสอบระบบงานควรจะตรวจการเข้าไปมีส่วนร่วมของผู้ใช้ในแต่ละขั้นตอนของการพัฒนาฯ และนำทฤษฎีการวิเคราะห์ค่าใช้จ่ายต่อผลตอบแทนมาใช้ศึกษาความเป็นไปได้ของโครงการ การตรวจสอบจะต้องคำนึงถึงการประกันคุณภาพในระหว่างที่ทำการพัฒนา การเปลี่ยนแปลงระบบงาน และการทดสอบระบบงาน รวมทั้งเอกสารประกอบระบบงานนั้น

การควบคุมซอฟต์แวร์ (Software Controls) มีความจำเป็นสำหรับซอฟต์แวร์ประเภทต่างๆ ที่นำมาใช้ประกอบระบบงาน การควบคุมซอฟต์แวร์ตรวจสอบการใช้ซอฟต์แวร์ระบบและป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้งาน เนื่องจากซอฟต์แวร์ระบบมีความสำคัญต่อการควบคุมการทำงานของซอฟต์แวร์อื่นๆ และเป็นตัวที่เข้าไปแก้ไขเปลี่ยนแปลงข้อมูลโดยตรง

การควบคุมทางกายภาพ (Physical Hardware Controls) เป็นการป้องกันทางกายภาพเพื่อไม่ให้ใช้เครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ และตรวจสอบความผิดปกติของอุปกรณ์ทุกชนิด การป้องกันนี้รวมไปถึงการป้องกันอัคคีภัย การป้องกันไม่ให้อุณหภูมิและความชื้นในห้องเก็บอุปกรณ์สูงหรือต่ำเกินไป การป้องกันข้อมูลเสียหายด้วยการทำสำเนาข้อมูล การรักษาให้ฮาร์ดดิกส์สามารถให้บริการได้ตลอดเวลาที่ต้องการ เป็นต้น

การควบคุมการปฏิบัติงานเครื่องคอมพิวเตอร์ (Computer Operations Controls) ประยุกต์ใช้กับงานของฝ่ายคอมพิวเตอร์ เพื่อให้ขั้นตอนการปฏิบัติเกี่ยวกับอุปกรณ์บันทึกข้อมูลและการประมวลผลข้อมูลเป็นไปตามขั้นตอนที่กำหนด ได้แก่ การจัดสภาพแวดล้อมให้เหมาะสมกับการทำงานของเครื่องคอมพิวเตอร์ การใช้ซอฟต์แวร์ การทำสำเนาข้อมูล และการฟื้นสภาพข้อมูลในกรณีที่โปรแกรมไม่ทำงานตามปกติ เป็นต้น

การควบคุมความปลอดภัยข้อมูล (Data Security Controls) เป็นการปกป้องข้อมูลที่มีค่ายิ่งขององค์กรที่เก็บอยู่ในดิกส์หรือเทปหรืออุปกรณ์ใดก็แล้วแต่ ให้พ้นจากการใช้งาน การเปลี่ยนแปลง และการทำลายโดยบุคคลที่ไม่ได้รับอนุญาต การปกป้องนี้ต้องทำทั้งในขณะที่แฟ้มข้อมูลกำลังถูกใช้งานและเก็บรักษาไว้

ในสภาพการทำงานที่ข้อมูลมีการป้อนเข้ามาจากเครื่องเทอร์มินอล ข้อมูลที่แปลกปลอมเข้ามาจะต้องถูกกำจัดออกจากระบบ ซึ่งมีการแบ่งระดับการรักษาความปลอดภัยไว้หลายระดับ คือ

- เครื่องเทอร์มินอลอาจได้รับการป้องกันทางกายภาพ โดยอนุญาตให้บุคคลบางประเภทใช้งานได้
- ซอฟต์แวร์ระบบอาจใช้ระบบป้องกันด้วย User Name และ Password ซึ่งมอบหมายให้เฉพาะบางคนเท่านั้น
- อาจมีการจัดการรักษาความปลอดภัยเพิ่มเติมในส่วนอื่นที่มีความจำเป็น เช่น การป้อนข้อมูลอาจจัดให้เก็บไว้ในแฟ้มข้อมูลบางแฟ้มเท่านั้น การกำหนดผู้ใช้สำหรับโปรแกรมประยุกต์ การกำหนดชนิดการใช้งาน เป็นต้น

ระเบียบวินัยผู้บริหาร มาตรฐาน และขั้นตอนการปฏิบัติงาน (Administrative Disciplines, Standards, and Procedures) หมายถึง การกำหนดมาตรฐาน กฎเกณฑ์ ขั้นตอนการปฏิบัติงาน และวินัยในการรักษาความปลอดภัย เพื่อให้มั่นใจได้ว่าการรักษาความปลอดภัยทั่วไป และการรักษาความปลอดภัยโปรแกรมประยุกต์ได้รับการจัดตั้งและนำไปปฏิบัติอย่างจริงจัง การควบคุมสำหรับผู้บริหารแบ่งออกเป็น 3 ส่วน คือ การแบ่งแยกหน้าที่ นโยบายและขั้นตอนการปฏิบัติ และการควบคุมการปฏิบัติ

การแบ่งแยกหน้าที่ (Segregation of Functions) หมายถึง การออกแบบหน้าที่แต่ละหน้าที่ให้มีความชัดเจน เพื่อลดความเสี่ยงในการเกิดข้อผิดพลาด และการใช้ทรัพยากรองค์กรผิดวัตถุประสงค์ บุคคลผู้มีหน้าที่รับผิดชอบระบบปฏิบัติการไม่ควรเป็นบุคคลที่สามารถเปลี่ยนแปลงทรัพยากรขององค์กรได้

นโยบายและขั้นตอนการปฏิบัติงาน (Written Policies and Procedures) เป็นการกำหนดมาตรฐานสำหรับควบคุมการทำงานในระบบสารสนเทศ ขั้นตอนการปฏิบัติงานจะต้องได้รับการกำหนดอย่างเป็นทางการในรูปเอกสาร และได้รับการรับรองโดยผู้บริหารที่มีอำนาจ

การควบคุมการปฏิบัติ (Supervision) เกี่ยวข้องกับขั้นตอนการปฏิบัติในการควบคุม เพื่อให้ระบบสารสนเทศสามารถทำงานได้เป็นปกติ ถ้าปราศจากการควบคุมแล้ว ขั้นตอนการปฏิบัติที่ดีที่สุดก็อาจถูกละเลยได้

2.3.2 การควบคุมระบบงาน (Application Controls)

การควบคุมระบบงานเป็นมาตรการในการควบคุมที่สร้างขึ้นมาเฉพาะสำหรับแต่ละระบบงาน โดยมีทั้งที่เป็นระบบอัตโนมัติและขั้นตอนการปฏิบัติสำหรับผู้ที่เกี่ยวข้อง ทั้งนี้เพื่อให้แน่ใจว่าข้อมูลได้รับการประมวลผลอย่างสมบูรณ์และเที่ยงตรงสำหรับระบบงานนั้นๆ ซึ่งพอจะสรุปมาตรการการควบคุมระบบงานได้เป็น 3 ส่วน คือ การควบคุมข้อมูลนำเข้า การควบคุมการประมวลผล และการควบคุมผลลัพธ์

การควบคุมข้อมูลนำเข้า (Input Controls) ทำการตรวจสอบความถูกต้องและความสมบูรณ์ของข้อมูลก่อนที่จะนำเข้าสู่ระบบงาน แบ่งออกได้เป็น การอนุญาตข้อมูลนำเข้า การเปลี่ยนแปลงข้อมูล การแก้ไขข้อมูล และการจัดการข้อผิดพลาด

ข้อมูลนำเข้าจะต้องได้รับการอนุญาต (Input Authorization) อย่างเป็นทางการ จัดการบันทึก และตรวจสอบในขณะที่ข้อมูลดิบถูกป้อนเข้าสู่ระบบคอมพิวเตอร์ เช่น ขั้นตอนการปฏิบัติอย่างเป็นทางการจะกำหนดหน่วยงานที่ได้รับอนุญาตให้ป้อนข้อมูลรายการธุรกรรมเข้าสู่ระบบ หน่วยงานอื่นจะไม่มีสิทธิในการป้อนข้อมูลนี้

ข้อมูลนำเข้าจะต้องได้รับการเปลี่ยนแปลง (Data Conversion) ให้เหมาะสมกับโครงสร้างรายการธุรกรรมโดยไม่มีข้อผิดพลาด วิธีลดข้อผิดพลาดอาจทำได้โดยการป้อนข้อมูลผ่านเครื่องเทอร์มินอลโดยตรง หรือการใช้ระบบป้อนข้อมูลอัตโนมัติ

การควบคุมจำนวนรวม (Control Totals) สามารถจัดทำได้ก่อนที่จะนำรายการธุรกรรมไปประมวลผล จำนวนรวมในที่นี้อาจเป็นจำนวนรวมของรายการธุรกรรม หรือจำนวนรวมของข้อมูลในแต่ละเขตข้อมูลของรายการธุรกรรม เช่น จำนวนรวมของยอดขาย โปรแกรมคอมพิวเตอร์ที่ทำการประมวลผลรายการธุรกรรมจะรวมตัวเลขที่กำหนด และนำมาเปรียบเทียบกับจำนวนรวมดังกล่าว

การควบคุมการประมวลผล (Processing Controls) ให้การรับประกันว่าข้อมูลนั้นมีความครบถ้วนและถูกต้องในระหว่างการประมวลผลข้อมูล แบ่งออกเป็น การควบคุมจำนวนครั้งการประมวลผล การประกบคู่ และการตรวจสอบโปรแกรม

การควบคุมจำนวนครั้งการประมวลผล (Run Control Totals) เปรียบเทียบจำนวนข้อมูลนำเข้า (ที่มีการนับจำนวนไว้ล่วงหน้า) กับจำนวนครั้งที่มีการปรับปรุงแฟ้มข้อมูล (ที่มีการบันทึกไว้ในระหว่างที่มีการประมวลผล) จำนวนรวม เช่น จำนวนรายการธุรกรรม หรือจำนวนรวมของข้อมูลที่สำคัญ จะได้รับการเปรียบเทียบและรายงานผลเพื่อการตรวจทานในภายหลัง

การประกบคู่ (Computer Matching) ทำการประกบคู่รายการข้อมูลนำเข้าที่ไม่สอดคล้องกับรายการข้อมูลในแฟ้มข้อมูลหลักที่นำมาใช้ประมวลผลเพื่อการตรวจสอบในภายหลัง ข้อมูลที่ไม่สอดคล้องกันมักจะเกิดขึ้นกับข้อมูลนำเข้า แต่ในบางครั้งก็ต้องนำมาใช้เพื่อรับประกันความถูกต้องในการปรับปรุงข้อมูล

การตรวจสอบข้อมูลและ/หรือโปรแกรม (Edit Checks) หมายถึง การใช้โปรแกรมในการตรวจสอบข้อมูลนำเข้า เพื่อค้นหาข้อผิดพลาดก่อนที่จะนำไปประมวลผล ข้อมูลที่ไม่ผ่านการตรวจสอบจะถูกปฏิเสธไม่ให้นำไปประมวลผล อย่างไรก็ตามระบบงานบางอย่างก็ต้องการการตรวจสอบในระหว่างทำการปรับปรุงข้อมูลด้วย

การควบคุมข้อมูลผลลัพธ์ (Output Controls) ทำให้เกิดความมั่นใจว่าผลที่ได้รับจากการประมวลผลนั้นมีความเที่ยงตรง สมบูรณ์ และมีการแจกจ่ายไปยังผู้เกี่ยวข้อง ได้แก่งานดังนี้

- ตรวจความสมดุลจำนวนรวมผลลัพธ์กับจำนวนรวมข้อมูลนำเข้าและจำนวนรวมการประมวลผล
- ทบทวนรายงานที่แสดงถึงสิ่งที่เกิดขึ้นในระหว่างการประมวลผล
- การจัดทำขั้นตอนการปฏิบัติงานและเอกสารอย่างเป็นทางการที่อธิบายถึงผู้ที่มีสิทธิในการนำข้อมูลผลลัพธ์ รายงานการตรวจสอบ และเอกสารที่สำคัญไปใช้

2.3.3 การทดสอบระบบงาน[9]

ระบบงานจะต้องได้รับการทดสอบในทุกๆ ด้านที่จะสามารถทำการทดสอบได้ เพื่อให้เกิดความแน่ใจได้ว่าระบบงานจะทำงานได้ถูกต้องและเป็นไปตามที่ต้องการ ซึ่งการทดสอบระบบงานแบ่งออกเป็น 3 ขั้นตอน คือ การทดสอบแต่ละส่วน การทดสอบทั้งระบบ และการทดสอบเพื่อการยอมรับ

การทดสอบแต่ละส่วน (Unit Testing) เป็นการทดสอบโปรแกรมทีละโปรแกรมแยกกันต่างหาก เพื่อให้แน่ใจได้ว่าถ้าโปรแกรมแต่ละโปรแกรมทำงานได้อย่างถูกต้องแล้วก็จะทำให้ระบบงานทั้งระบบทำงานได้อย่างถูกต้องด้วย อย่างไรก็ตามวัตถุประสงค์ของการทดสอบในลักษณะนี้มักจะไม่สามารถทำได้อย่างสมบูรณ์ ดังนั้น การทดสอบจึงควรจะมุ่งเน้นการค้นหาจุดผิดพลาดในโปรแกรม และพยายามค้นหาวิธีการที่จะทำให้โปรแกรมนั้นสามารถตอบสนองกับสิ่งแวดล้อมได้ในทุกรูปแบบ

การทดสอบระบบทั้งระบบ (System Testing) เป็นการทดสอบการทำงานของระบบในภาพรวม ซึ่งจะทดสอบการทำงานร่วมกันระหว่างโปรแกรมส่วนต่างๆ ของระบบงาน (ที่ได้รับการทดสอบแบบแยกส่วนมาก่อนหน้านี้แล้ว) นอกจากนั้นยังทำการประเมินค่าระยะเวลาที่ใช้ในการทำงาน ความสามารถในการตอบสนองเมื่อมีผู้ใช้งานเป็นจำนวนมากพร้อมกัน การฟื้นคืนสภาพเมื่อระบบเกิดความล้มเหลว ความสามารถในการใช้งานระบบหลังความล้มเหลว และเอกสารประกอบที่อธิบายการทำงานทุกส่วนของระบบงาน

การทดสอบเพื่อการยอมรับระบบ (Acceptance Testing) เป็นการทดสอบในขั้นตอนสุดท้ายเพื่อให้เกิดความมั่นใจว่าระบบงานพร้อมที่จะนำไปติดตั้งใช้งานได้ ผลจากการทดสอบระบบงานทั้งระบบจะถูกนำมาพิจารณาโดยพนักงานผู้ใช้ระบบงาน และผู้บริหาร เมื่อทุกฝ่ายมีความพอใจต่อผลที่เกิดขึ้นจากการทดสอบ รวมทั้งระบบงานสามารถทำงานได้ตาม

---

[9] กิตติ ภักดีวัฒนะกุล และ พนิดา พานิชกุล, คัมภีร์การวิเคราะห์และออกแบบระบบ, พิมพ์ครั้งที่ 2. (กรุงเทพฯ: เคทีพี คอมพ์ แอนด์ คอนซัลท์, 2546), 432-434.

มาตรฐานที่ต้องการแล้ว จะถือว่าระบบงานได้รับการยอมรับอย่างเป็นทางการ และสามารถนำไปติดตั้งใช้งานได้

2.3.4 วิธีการที่ใช้ในการทดสอบระบบงาน

วิธีการที่ใช้ในการทดสอบประสิทธิภาพการทำงานของโปรแกรมระบบงาน สามารถจำแนกได้ ดังนี้

2.3.4.1 การทดสอบการทำงานสูงสุด (Peak Load Testing) เป็นการทดสอบประสิทธิภาพในการประมวลผลของโปรแกรมระบบงาน เมื่อมีการทำรายการมากที่สุด ณ ช่วงเวลาใดเวลาหนึ่ง เพื่อทดสอบว่าระบบจะสามารถรองรับการทำรายการมากที่สุดได้เพียงใด และนานเท่าไหร่เมื่อต้องประมวลผลจำนวนรายการที่มากที่สุดดังกล่าวในช่วงเวลาหนึ่ง

ตัวอย่างเช่น ระบบงานสามารถรองรับการทำรายการได้สูงสุด 1,000 รายการต่อวัน แต่ในการทดสอบสมมติให้มีการทำรายการ 1,200 รายการต่อวัน เป็นต้น การทดสอบลักษณะนี้จะทำให้ทราบได้ว่าระบบสามารถรองรับการทำรายการมากกว่าขีดสูงสุดที่กำหนดได้หรือไม่ และได้นานเพียงใด มีปัญหาอะไรเกิดขึ้นบ้าง

2.3.4.2 การทดสอบประสิทธิภาพของเวลา (Performance Testing) เป็นการทดสอบระบบ เพื่อพิจารณาถึงช่วงเวลาที่ใช้ในการประมวลผลรายการว่าใช้ระยะเวลานานเพียงใดในการทำรายการ ไม่ว่าจะเป็นการประมวลผลแบบกลุ่ม (Batch Processing) หรือการประมวลผลแบบออนไลน์ (Online Processing) รวมทั้งทดสอบช่วงเวลาที่ใช้ในการเข้าถึงข้อมูลแบบลำดับ (Sequential Access) และแบบสุ่ม (Random Access) ด้วย

2.3.4.3 การทดสอบการกู้ระบบ (Recovery Testing) เป็นการทดสอบความสามารถในการกู้ระบบรวมทั้งการกู้ข้อมูลให้สามารถกลับคืนสู่สภาวะปกติ กรณีเกิดเหตุการณ์ที่ทำให้ระบบงานไม่สามารถทำงานต่อไปได้

2.3.4.4 การทดสอบการเก็บข้อมูล (Storage Testing) เป็นการทดสอบความสามารถของระบบในการเก็บข้อมูล ว่าสามารถเก็บข้อมูลได้สูงสุดเป็นจำนวนเท่าใด เพื่อจะได้เตรียมการรองรับจำนวนข้อมูลที่อาจจะเพิ่มมากขึ้นในอนาคต

2.3.4.5 การทดสอบกระบวนการปฏิบัติงาน (Procedure Testing) เป็นการทดสอบการจัดทำเอกสารคู่มือการดำเนินงานของระบบ และคู่มือการปฏิบัติงานสำหรับผู้ใช้นั้น ว่าสามารถสร้างความเข้าใจให้กับผู้ใช้งานได้มากน้อยเพียงใด และเมื่อเกิดปัญหาในเบื้องต้นขึ้น ผู้ใช้งานสามารถอ่านคู่มือเพื่อแก้ไขปัญหานั้นได้หรือไม่

2.3.4.6 การทดสอบระบบงานรวม (System Integrated Testing) เป็นการทดสอบโปรแกรมระบบงานจากการเพิ่มโปรแกรมเข้าไปเรื่อยๆ จนกระทั่งครบทุกโปรแกรมของระบบงาน ว่าโปรแกรมระบบงานทุกโปรแกรมเมื่อทำงานร่วมกันแล้วจะให้ผลลัพธ์ที่ถูกต้องหรือไม่ และหลังจากนั้นจะทดสอบโดยใช้ระบบงานย่อยเพิ่มไปเรื่อยๆ จนกระทั่งครบทุกระบบงานย่อยของระบบงานรวม เพื่อทดสอบว่าระบบงานรวมสามารถทำงานให้ผลลัพธ์ที่มีประสิทธิภาพเป็นที่ยอมรับได้หรือไม่ และเพื่อทำให้มั่นใจได้ว่าระบบงานนั้นสามารถตอบสนองความต้องการของผู้ใช้งานได้ดีที่สุด

2.3.4.7 การทดสอบเพื่อยอมรับระบบงานโดยผู้ใช้งาน (User Acceptance Test) หลังจากที่ได้ทดสอบความสมบูรณ์และความถูกต้องของระบบงานรวมแล้ว ยังจะต้องทำการทดสอบเพื่อยอมรับระบบงานโดยผู้ใช้งานด้วย ซึ่งเป็นการทดสอบที่สำคัญเทียบเท่ากับการทดสอบระบบงานรวม เนื่องจากการพัฒนาระบบนั้นก็เพื่อตอบสนองความต้องการในการดำเนินงานของผู้ใช้ระบบงาน โดยวิธีการทดสอบเพื่อยอมรับระบบงานนั้นสามารถแบ่งออกเป็น 2 ประเภท คือ

1) Alpha Testing คือ การทดสอบความสมบูรณ์ของระบบงานโดยใช้ข้อมูลที่สมมติขึ้นเพื่อทำการทดสอบ และสมมติให้ระบบอยู่ในสถานการณ์ที่อาจจะเกิดขึ้นได้ มีการทดสอบ 4 ประการ ดังนี้

- Recovery Testing เป็นการทดสอบการกู้ระบบงาน เพื่อทดสอบว่าระบบมีประสิทธิภาพในการกู้ระบบและข้อมูลคืนสู่สภาวะปกติและดำเนินงานต่อไปได้ หากเกิดกรณีที่ระบบหยุดชะงักไม่สามารถทำงานได้

- Security Testing เป็นการทดสอบความปลอดภัยของระบบงานว่ามีเครื่องมือรักษาความปลอดภัยที่รัดกุม และมีประสิทธิภาพเพียงพอหรือไม่ จากสถานการณ์การลักลอบเข้าสู่ระบบหรือการลักลอบเรียกใช้ข้อมูล
- Stress Testing เป็นการทดสอบประสิทธิภาพการทำงานของระบบงานภายใต้สภาพความกดดัน เช่น จะเกิดอะไรขึ้นเมื่อผู้ใช้ป้อนข้อมูลไม่ครบทุก Field หรือจะเกิดอะไรขึ้นเมื่อมีการเข้าถึงข้อมูลในเวลาเดียวกันจากผู้ใช้หลายๆ คน เป็นต้น
- Performance Testing เป็นการทดสอบประสิทธิภาพการทำงานของระบบงานภายใต้สภาพแวดล้อมที่แตกต่างกันว่าระบบมี Response Time มากน้อยเพียงใด เช่น ระบบปฏิบัติการคอมพิวเตอร์ที่แตกต่างกัน หรือระบบเครือข่ายที่แตกต่างกัน เป็นต้น

2) Beta Testing คือ การทดสอบความสมบูรณ์ของระบบงานโดยใช้ข้อมูลจริงทำการทดสอบภายใต้สถานการณ์ที่เกิดขึ้นจริง การทดสอบประเภทนี้ถือว่าเป็นการซ้อมติดตั้งระบบเพื่อใช้งานจริง เนื่องจากเป็นการทดสอบระบบงานอย่างสมจริงไม่ว่าจะเป็นสถานการณ์ข้อมูล ขั้นตอนการดำเนินงาน เอกสารคู่มือ การฝึกอบรม การสนับสนุนการทำงาน รวมทั้งยังเป็นการแก้ปัญหาที่พบจากการทดสอบแบบ Alpha Testing ด้วย

2.3.5 <u>การติดตั้งระบบงานจริงบน Production System (Implementation)</u>

เมื่อทดสอบโปรแกรมระบบงานจนผู้ใช้ยอมรับแล้ว ระบบงานที่ได้รับการพัฒนาก็พร้อมที่จะนำมาใช้งานจริงด้วยการติดตั้ง (Installation) บน Production System ทั้งนี้ การติดตั้งระบบ คือ การเปลี่ยนการทำงานจากระบบงานเดิมไปเป็นระบบงานใหม่ แต่การเปลี่ยนแปลงไปสู่สิ่งใหม่ย่อมมีผลกระทบต่อผู้ใช้งานบางกลุ่ม ที่ยังคงมีความคุ้นเคยกับวิธีการดำเนินงานแบบเก่า รวมทั้งข้อจำกัดในเรื่องของความพร้อมในการเปลี่ยนแปลง ดังนั้นจึงควรเลือกแนวทางที่เหมาะสมในการติดตั้งระบบด้วย ซึ่งแบ่งออกเป็น 4 แนวทาง ดังนี้

2.3.5.1 <u>การติดตั้งแบบทันทีทันใด</u> (Direct Installation) เป็นวิธีการติดตั้งที่มีการใช้ระบบงานใหม่ทันที และยกเลิกการใช้ระบบงานเก่าทันทีเช่นเดียวกัน วิธีการแบบนี้องค์กรเสียค่าใช้จ่ายน้อยแต่มีความเสี่ยงสูง เนื่องจากข้อมูลในการใช้งานจริงที่นำเข้าสู่ระบบมีความเป็นไปได้ในการเกิดข้อผิดพลาดได้มากกว่าข้อมูลที่สมมติขึ้นเพื่อการทดสอบ และหากเกิดกรณีเช่นนี้จะ

ส่งผลกระทบต่อผู้ใช้ระบบจนทำให้ระบบหยุดชะงักได้ วิธีการแก้ปัญหาอย่างหนึ่งคือนำระบบเก่าเข้ามาใช้งานอีกครั้ง แต่จะเสียเวลามากในการปรับปรุงข้อมูลในระบบเก่าทั้งหมด แต่ข้อดีของการติดตั้งวิธีนี้คือ สามารถเลื่อนกำหนดการใช้งานระบบใหม่ออกไปได้หากองค์กรหรือผู้ใช้งานยังไม่มีความพร้อมสำหรับระบบใหม่

2.3.5.2 <u>การติดตั้งแบบขนาน</u> (Parallel Installation) เป็นวิธีการติดตั้งที่มีการใช้ระบบงานใหม่ไปพร้อมๆ กับการใช้ระบบงานเก่า จนกว่าผู้ใช้และผู้บริหารจะพอใจระบบใหม่และตัดสินใจที่จะหยุดใช้ระบบเก่า วิธีการแบบนี้องค์กรต้องเสียค่าใช้จ่ายค่อนข้างสูง เนื่องจากต้องคอยดูแล บำรุงรักษาระบบให้มีความสมบูรณ์ สามารถดำเนินงานอย่างมีประสิทธิภาพมากที่สุดทั้งสองระบบในเวลาเดียวกัน แต่ข้อดีของการติดตั้งวิธีนี้คือ ทำให้สามารถเปรียบเทียบผลการดำเนินงานระหว่างระบบใหม่กับระบบเก่าได้

2.3.5.3 <u>การติดตั้งแบบนำร่อง</u> (Single Location Installation / Pilot Installation) เป็นวิธีการติดตั้งที่มีการใช้ระบบงานใหม่เพียงหน่วยเดียวขององค์กรก่อนเพื่อเป็นการนำร่อง แล้วจึงค่อยปรับเปลี่ยนทั้งหมดเมื่อเห็นว่าระบบใหม่นั้นลงตัวแล้ว ข้อดีของวิธีการนี้คือ เสียค่าใช้จ่ายน้อยกว่าสองวิธีแรก และเมื่อเกิดข้อผิดพลาดหรือความเสียหายเนื่องจากระบบงานใหม่ ความเสียหายนั้นจะจำกัดอยู่เพียงแค่หน่วยงานที่จัดให้มีการติดตั้งระบบใหม่แบบนำร่องเท่านั้น ไม่ทำให้การดำเนินธุรกิจของทั้งองค์กรเสียหายไปด้วย ทั้งยังสามารถติดตามผลและดูแลระบบใหม่ได้อย่างเต็มที่ เพื่อปรับปรุงและแก้ไขให้เป็นระบบที่สมบูรณ์ก่อนนำไปใช้กับส่วนที่เหลือขององค์กร

2.3.5.4 <u>การติดตั้งแบบทยอยติดตั้งเป็นระยะ</u> (Phased Installation) เป็นวิธีการติดตั้งที่มีการใช้ระบบงานใหม่เพียงบางส่วนก่อนระยะหนึ่งควบคู่ไปกับระบบงานเก่า แล้วจึงค่อยๆ ทยอยใช้ระบบงานใหม่เพิ่มขึ้นทีละส่วน จนกระทั่งครบทุกส่วนของระบบงานใหม่อย่างเต็มรูปแบบในที่สุด มีลักษณะคล้ายกับการติดตั้งแบบนำร่อง แต่ต่างกันที่แบบทยอยติดตั้งไม่คำนึงถึงสถานที่ แต่คำนึงถึงระบบงานย่อยโดยการติดตั้งทีละระบบ ข้อดีของวิธีการนี้คือ สามารถจำกัดความเสี่ยงที่เกิดขึ้นได้ เนื่องจากการปรับเปลี่ยนเป็นช่วงระยะเวลา ความเสี่ยงหรือข้อผิดพลาดจึงเกิดขึ้นในช่วงที่มีการเปลี่ยนแปลงระบบงานใหม่เท่านั้น ข้อเสียคือ ความไม่สอดคล้องของการดำเนินงานในระบบงานย่อยของระบบใหม่และระบบเก่า อาจจะเกิดปัญหาในการติดต่อระหว่างฐานข้อมูลของระบบใหม่กับฐานข้อมูลของระบบเก่าได้

2.4 องค์กรที่นำมาเป็นกรณีศึกษา

องค์กรที่นำมาเป็นกรณีศึกษาในงานวิจัยครั้งนี้ ประกอบธุรกิจทางการเงินด้านบัตรเครดิต และการให้สินเชื่อบุคคลที่ไม่ใช่สถาบันการเงิน (Non-bank) อยู่ภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทย และสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) โดยมีรายละเอียด ดังนี้

2.4.1 วิสัยทัศน์ (Vision)

มุ่งมั่นที่จะเป็นผู้นำในธุรกิจบัตรเครดิต และสินเชื่อเพื่อผู้บริโภค

2.4.2 พันธกิจ (Mission)

นำเสนอผลิตภัณฑ์ และบริการด้านบัตรเครดิต และสินเชื่อเพื่อผู้บริโภคที่ครบวงจร พร้อมด้วยสิทธิประโยชน์ ความสะดวกสบาย ปลอดภัย ในราคายุติธรรม เพื่อความคุ้มค่า และความพึงพอใจสูงสุดของผู้บริโภค

2.4.3 ค่านิยมขององค์กร (Core Values)

เน้นการบริหารงานและการบริการด้วยคุณภาพระดับมาตรฐานสากล โปร่งใส มีเป้าหมายที่ชัดเจน เข้าถึงความต้องการของผู้บริโภคอย่างแท้จริง

2.4.4 บุคลิกองค์กร (Corporate Personality)

สร้างภาพลักษณ์สะท้อนบุคลิกใหม่ขององค์กร

- มีความทันสมัย ก้าวหน้าในระดับสากล (Modern)
- มีความกระตือรือร้นที่จะนำเสนอสิ่งใหม่ๆ (Dynamic)
- การทำงานอย่างมืออาชีพ (Professional)
- การทำงานด้วยความจริงใจ ซื่อสัตย์ ทำงานอย่างโปร่งใส (Simplicity)

- การทำงานอย่างเป็นมิตรด้วยความสนุกสนาน มีชีวิตชีวา พร้อมให้บริการ (Fun & Friendly)

2.4.5 ลักษณะการประกอบธุรกิจ

ธุรกิจหลักขององค์กรที่นำมาเป็นกรณีศึกษา สามารถแบ่งออกได้เป็น 5 กลุ่มธุรกิจหลัก คือ

1. **ธุรกิจบัตรเครดิต** (Credit Card Business)

ธุรกิจทางด้านบัตรเครดิตโดยทั่วๆ ไปแล้วประกอบด้วยธุรกิจย่อย 2 กลุ่ม คือ ธุรกิจที่เกี่ยวกับผู้ถือบัตรเครดิต และธุรกิจที่เกี่ยวกับร้านค้าที่รับชำระด้วยบัตรเครดิต

ธุรกิจที่เกี่ยวกับผู้ถือบัตรเครดิตนั้นจะเริ่มจากการออกบัตร อนุมัติวงเงินให้กับผู้ถือบัตร การกำกับดูแลการใช้จ่ายผ่านบัตร การรับชำระหนี้ และการติดตามหนี้ โดยที่ธนาคาร / บริษัทผู้ออกบัตร (Issuing Bank) จะได้รับรายได้เป็นค่าธรรมเนียมในการทำรายการต่างๆ และดอกเบี้ยรับ ธุรกิจด้านนี้เรียกว่า **ธุรกิจการออกบัตรเครดิต** (Issuing Business) โดยค่าธรรมเนียมที่ได้รับจะประกอบด้วยค่าธรรมเนียมที่ได้รับในฐานะธนาคาร / บริษัทผู้ออกบัตร เรียกว่า Interchange Fee ซึ่งคิดเป็นอัตราส่วนของการใช้จ่ายผ่านบัตรเครดิตทุกครั้งที่ผู้ถือบัตรนำบัตรขององค์กรไปชำระค่าสินค้าและบริการ นอกจากนี้ ยังมีการคิดอัตราดอกเบี้ยและค่าธรรมเนียมอื่นๆ เช่น ค่าธรรมเนียมในการใช้วงเงิน ค่าธรรมเนียมการใช้บริการเบิกเงินสดล่วงหน้า ฯลฯ

สำหรับธุรกิจที่เกี่ยวกับร้านค้าที่รับชำระด้วยบัตรเครดิตนั้น ภายหลังจากคัดเลือกและแต่งตั้งร้านค้าแล้ว ธนาคาร / บริษัทร้านค้า (Acquiring Bank) จะติดตั้งเครื่องรูดบัตรให้กับร้านค้า กำกับดูแลการอนุมัติการรับชำระค่าสินค้าหรือบริการจากผู้ถือบัตร รวมทั้งควบคุมการกระทำทุจริตของร้านค้า ซึ่งธุรกิจด้านนี้เรียกว่า **ธุรกิจร้านค้ารับบัตรเครดิต** (Acquiring Business) โดยรายได้ของธนาคาร / บริษัทร้านค้าจะมาจากค่าธรรมเนียม ซึ่งคิดตามสัดส่วนของมูลค่าการใช้บัตรผ่านเครื่องรูดบัตรเครดิตทั้งหมด โดยทั่วไปอัตราค่าธรรมเนียมที่คิดจากร้านค้านี้ เรียกว่า Discount Rate อย่างไรก็ตาม ค่าธรรมเนียมที่ได้รับนี้ ส่วนหนึ่งจะต้องแบ่งเพื่อชำระให้กับธนาคาร / บริษัทผู้ออกบัตร

2. **ธุรกิจสินเชื่อบุคคล** (Personal Loans Business)

เป็นการบริการให้สินเชื่ออเนกประสงค์ ตามวัตถุประสงค์การใช้เงินของลูกค้าบุคคลธรรมดาทั่วไป ช่วยให้ลูกค้ามีความคล่องตัวในการใช้จ่ายยามฉุกเฉิน โดยไม่ต้องมีหลักทรัพย์หรือบุคคลค้ำประกันใดๆ ด้วยอัตราดอกเบี้ยและค่าธรรมเนียมการใช้วงเงินต่ำ และคิดแบบลดต้นลดดอก

3. **ธุรกิจสินเชื่อเจ้าของกิจการ** (Self-Employed Loans Business)

เป็นสินเชื่อไม่มีหลักประกันสำหรับบุคคลที่เป็นเจ้าของกิจการ (KTC Million) ที่ต้องการเงินทุนหมุนเวียน เพื่อใช้ในการดำเนินงาน ไม่ว่าจะเป็นการซื้ออุปกรณ์ต่างๆ ซื้อเครื่องจักรใหม่ ซื้อวัตถุดิบ เพื่อเพิ่มกำลังการผลิต หรือนำไปใช้ในการตกแต่งอาคารสำนักงาน

4. **ธุรกิจบริการเกี่ยวเนื่องกับระบบการชำระเงิน** (Payment Products Business)

เป็นธุรกิจที่มีรูปแบบให้บริการในลักษณะของการเป็นตัวกลางการชำระเงินระหว่างผู้ซื้อและผู้ขายสินค้าหรือผู้ให้บริการ โดยใช้บัตรเป็นเครื่องมือชำระเงิน ซึ่งจะทำให้ลดความเสี่ยงและเพิ่มความสะดวกสบายในการชำระเงินแก่ทั้งสองฝ่าย

5. **ธุรกิจสินเชื่อผ่อนชำระสินค้า** (Asset Finance Business)

เป็นธุรกิจสินเชื่อเพื่อการผ่อนชำระสินค้าโดยตรง ซึ่งเป็นอีกช่องทางหนึ่งขององค์กรที่จะช่วยสร้างความหลากหลายในการให้บริการ

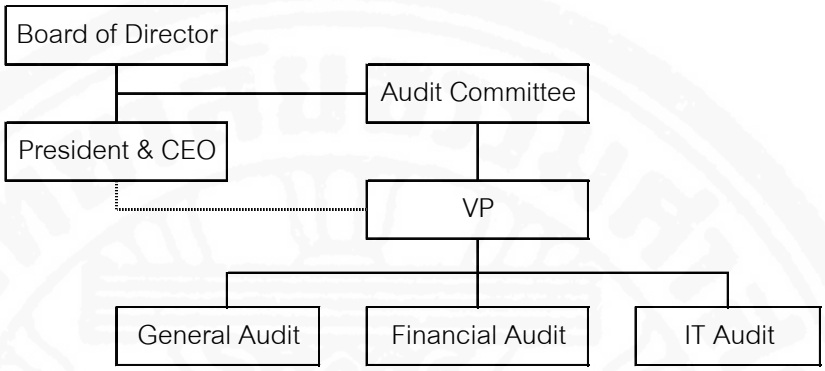
2.4.6 <u>โครงสร้างองค์กร</u>

งานวิจัยฉบับนี้ จะกล่าวถึงโครงสร้างขององค์กรที่นำมาเป็นกรณีศึกษา เฉพาะฝ่ายงานหลักที่มีส่วนเกี่ยวข้องกับกระบวนการตรวจสอบระบบสารสนเทศ ดังนี้

2.4.6.1 <u>ฝ่ายตรวจสอบภายใน</u> (Internal Audit Department) ประกอบด้วย 3 หน่วยงาน คือ (1) General Audit (2) Financial Audit และ (3) Information Technology Audit หรือ IT Audit

ภาพที่ 2.5

การจัดโครงสร้างองค์กรของฝ่ายตรวจสอบภายใน



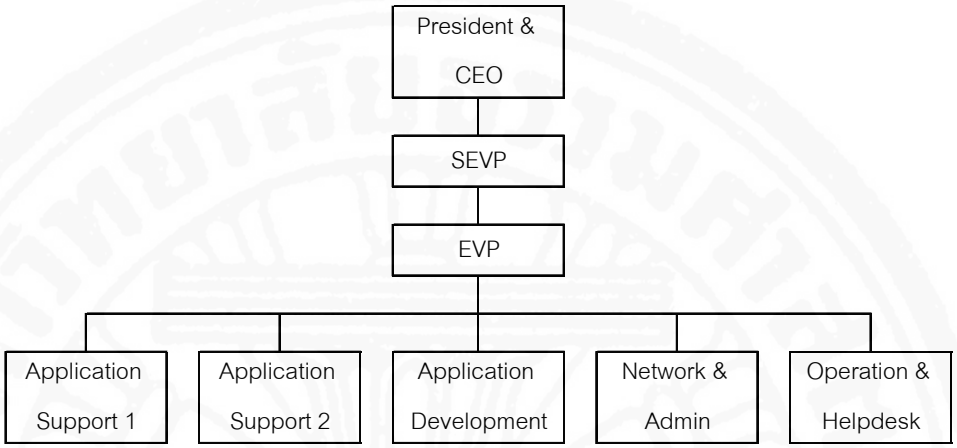
ฝ่ายตรวจสอบภายใน มีขอบเขตหน้าที่ความรับผิดชอบ ดังนี้

- หน่วยงาน General Audit และ Financial Audit ทำหน้าที่สอบทานความถูกต้องครบถ้วน และความเชื่อถือได้ของข้อมูลทางบัญชีและการเงิน ควบคุมดูแลการเก็บรักษาและการใช้ทรัพย์สิน ประเมินความเพียงพอและประสิทธิภาพของระบบการควบคุมภายในของระบบต่างๆ พร้อมทั้งวางแผนการตรวจสอบและจัดให้มีการปฏิบัติตามแผน
- หน่วยงาน Information Technology Audit หรือ IT Audit ทำหน้าที่ดูแลรับผิดชอบในการตรวจสอบและประเมินประสิทธิภาพของระบบการควบคุมภายใน หรือการบริหารความเสี่ยงที่เกิดขึ้นจากการใช้ระบบสารสนเทศ ควบคุมความเชื่อถือได้ของข้อมูลและเอกสารระบบงาน (Data Integrity and Documentation) รวมทั้งกระบวนการจัดการระบบสารสนเทศในส่วนของการบริหารโครงการ (IT Project Management) และความเหมาะสมของขั้นตอนในพัฒนาและทดสอบระบบงาน

2.4.6.2 <u>ฝ่ายเทคโนโลยีสารสนเทศ</u> (Information Technology Department) ประกอบด้วย 5 หน่วยงาน คือ (1) Application Support 1 (2) Application Support 2 (3) Application Development (4) Network & Admin และ (5) Operation & Helpdesk

ภาพที่ 2.6

การจัดโครงสร้างองค์กรของฝ่ายเทคโนโลยีสารสนเทศ



ฝ่ายเทคโนโลยีสารสนเทศ มีขอบเขตหน้าที่ความรับผิดชอบ ดังนี้

- บริหาร ดูแล ให้การสนับสนุนด้านระบบงาน / ระบบคอมพิวเตอร์ สนับสนุนการแก้ไขปรับปรุง และพัฒนาระบบงาน / ระบบคอมพิวเตอร์ที่เกี่ยวข้องแก่หน่วยงานต่างๆ
- ให้คำปรึกษา ความรู้ด้านระบบงาน และระบบงานคอมพิวเตอร์แก่หน่วยงานต่างๆ
- วิเคราะห์และประสานงานการแก้ไขปัญหาต่างๆ ที่เกิดขึ้นจากระบบงาน และ/หรือระบบคอมพิวเตอร์กับหน่วยงานทั้งภายในและภายนอกองค์กร

2.5 มาตรฐาน COBIT

มาตรฐาน “COBIT”[10] ย่อมาจาก “Control Objectives for Information and Related Technology” เริ่มพัฒนาโดยองค์กรระดับโลก คือ The Information Systems Audit and Control Association (ISACA) และ IT Governance Institute (ITGI) เป็นผู้ดูแลในปัจจุบัน

[10] http://www.acisonline.net/article_prinya_eweek_010748.htm and http://www.isaca-bangkok.org/association/isacabkk/Cobit.html.

(ISACA และ ITGI ตั้งอยู่ที่ประเทศสหรัฐอเมริกา) โดยมีวัตถุประสงค์เดิม เพื่อให้เป็นเครื่องมือ (Tools) หรือ กรอบแนวทาง (Guideline) สำหรับการตรวจสอบภายในเทคโนโลยีสารสนเทศ อย่างไรก็ดี ต่อมาผู้บริหารธุรกิจ ผู้บริหารระบบสารสนเทศได้นำมาตรฐาน COBIT ไปประยุกต์ใช้กับองค์กร เพื่อกำกับดูแลระบบสารสนเทศด้วย

มาตรฐาน COBIT เป็นมาตรฐานหนึ่งที่อธิบายถึงรายละเอียดของกระบวนการทางเทคโนโลยีสารสนเทศ (Information Technology Process) ได้แก่ รายละเอียดของการเตรียมความพร้อมแต่ละขั้นตอนว่าต้องทำอะไรบ้าง สิ่งไหนที่สำคัญ และมีทรัพยากรตัวใดบ้างที่ต้องพิจารณาเป็นพิเศษ รวมทั้งวัตถุประสงค์ของการควบคุมและแนวทางในการปฏิบัติ โดยมีหลักการดังนี้

วิสัยทัศน์

เป็นแบบอย่างของการบริหารจัดการเทคโนโลยีสารสนเทศ

พันธกิจ

ศึกษา, พัฒนา, เผยแพร่, มีความน่าเชื่อถือและทันเหตุการณ์ เพื่อให้เป็นวัตถุประสงค์ของการควบคุมที่เป็นที่ยอมรับสำหรับผู้บริหารและผู้ตรวจสอบในระดับสากล

หลักการสำคัญ

การจัดทำสารสนเทศต้องทำให้องค์กรบรรลุเป้าหมายได้ และการจัดการเทคโนโลยีสารสนเทศต้องมีกระบวนการที่แน่นอน

มาตรฐาน COBIT เป็นทั้งแนวคิดและแนวทางการปฏิบัติ (Framework) เพื่อการควบคุมภายในที่ดีด้านเทคโนโลยีสารสนเทศสำหรับองค์กรต่างๆ ที่จะใช้อ้างอิงถึงแนวทางการปฏิบัติที่ดี (Best Practice) ซึ่งสามารถนำไปปรับใช้ได้ในทุกองค์กรสำหรับกิจกรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยโครงสร้างของมาตรฐาน COBIT 3rd Edition ได้ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจ (Business Process) สามารถแบ่งได้เป็น 4 กระบวนการหลัก (Domain) ได้แก่

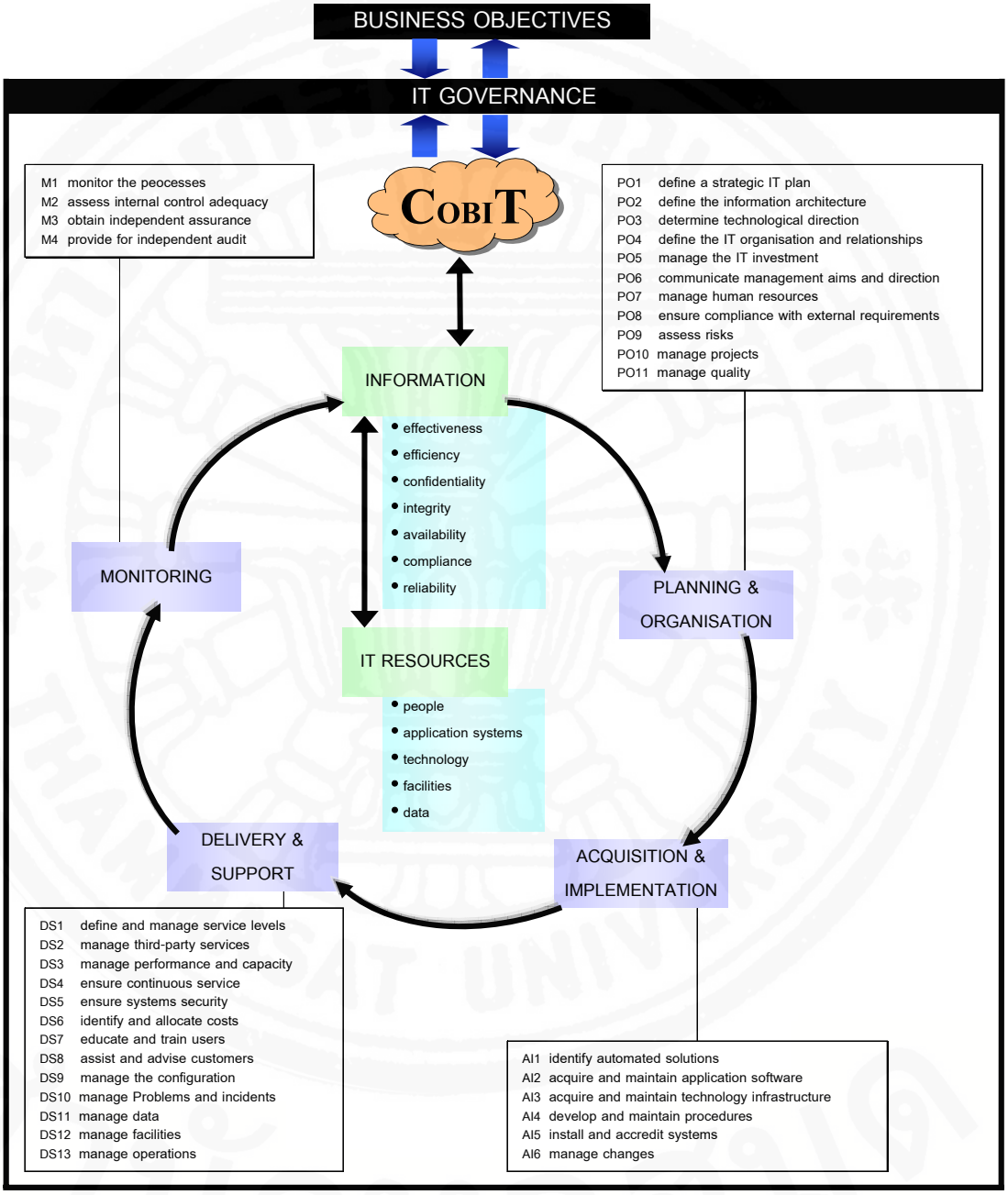
- การวางแผนและการจัดการองค์กร (PO : Planning and Organisation)
- การจัดหาและติดตั้ง (AI : Acquisition and Implementation)

- การส่งมอบและบำรุงรักษา (DS : Delivery and Support)
- การติดตามผล (M : Monitoring)

ในแต่ละกระบวนการหลักข้างต้น มาตรฐาน COBIT แสดงวัตถุประสงค์ของการควบคุมหลัก (High-level Control Objectives) รวมถึง 34 หัวข้อ และในแต่ละหัวข้อจะประกอบด้วยวัตถุประสงค์ของการควบคุมย่อยลงไปอีกขั้นหนึ่ง (Detailed Control Objectives) รวมถึง 318 หัวข้อย่อย พร้อมทั้งแนวทางการตรวจสอบ (Audit Guidelines) สำหรับแต่ละหัวข้ออีกด้วย

ภาพที่ 2.7

กรอบมาตรฐาน COBIT



ที่มา: www.isaca.org, www.itgi.org

วัตถุประสงค์ของการควบคุมหลัก (High-level Control Objectives) 34 หัวข้อ และวัตถุประสงค์ของการควบคุมย่อย (Detailed Control Objectives) 318 หัวข้อย่อยตามมาตรฐาน COBIT มีดังต่อไปนี้

1 <u>การวางแผนและการจัดการองค์กร</u> (PO : Planning and Organisation)

PO1 การจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ (Define a Strategic IT Plan) เพื่อให้องค์กรได้รับประโยชน์สูงสุดจากการใช้ IT

1.1 เทคโนโลยีสารสนเทศเป็นส่วนหนึ่งของแผนงานระยะสั้นและระยะยาวขององค์กร

1.2 แผนงานระยะยาวด้านเทคโนโลยีสารสนเทศ

1.3 วิธีการและโครงสร้างของการจัดทำแผนงานระยะยาวด้านเทคโนโลยีสารสนเทศ

1.4 การปรับเปลี่ยนแผนงานระยะยาวด้านเทคโนโลยีสารสนเทศ

1.5 แผนงานระยะสั้นสำหรับหน่วยงานด้านเทคโนโลยีสารสนเทศ

1.6 การสื่อสารแผนงานด้านเทคโนโลยีสารสนเทศ

1.7 การเฝ้าติดตามและประเมินผลการดำเนินงานตามแผนงานด้านเทคโนโลยีสารสนเทศ

1.8 การประเมินผลระบบงานที่มีอยู่

PO2 การกำหนดโครงสร้างด้านสารสนเทศ (Define the Information Architecture) เพื่อให้ได้รับประโยชน์สูงสุดจากการจัดรูปแบบระบบสารสนเทศ

2.1 ต้นแบบโครงสร้างด้านสารสนเทศ

2.2 พจนานุกรมและไวยากรณ์ข้อมูล

2.3 การจัดประเภทของข้อมูล

2.4 ระดับการรักษาความปลอดภัยของข้อมูล

PO3 การกำหนดทิศทางด้านเทคโนโลยี (Determine Technological Direction) เพื่อให้สามารถใช้เทคโนโลยีสมัยใหม่เป็นกลยุทธ์ในการบริหารธุรกิจ

- 3.1 การวางแผนโครงสร้างพื้นฐานด้านเทคโนโลยี
- 3.2 การติดตามทิศทางและกฎข้อบังคับทางด้านเทคโนโลยีในอนาคต
- 3.3 การจัดหา Contingency Plan ของโครงสร้างพื้นฐานด้านเทคโนโลยี
- 3.4 แผนการจัดซื้อฮาร์ดแวร์และซอฟต์แวร์
- 3.5 มาตรฐานด้านเทคโนโลยี

PO4 การจัดโครงสร้างองค์กรด้านเทคโนโลยีสารสนเทศและความสัมพันธ์กับหน่วยงานอื่น (Define the IT Organisation and Relationships) เพื่อให้สามารถให้บริการด้าน IT ได้อย่างเหมาะสมถูกต้อง

- 4.1 คณะกรรมการกำกับดูแลหรือวางแผนด้านเทคโนโลยีสารสนเทศ
- 4.2 การจัดองค์กรของหน่วยงานด้านเทคโนโลยีสารสนเทศ
- 4.3 การทบทวนความสำเร็จขององค์กร
- 4.4 หน้าที่และความรับผิดชอบ
- 4.5 ความรับผิดชอบด้านคุณภาพงาน
- 4.6 ความรับผิดชอบด้านการรักษาความปลอดภัยทั้งด้านระบบงานและข้อมูล
- 4.7 การกำหนดเจ้าของและผู้จัดเก็บข้อมูล
- 4.8 การกำหนดเจ้าของระบบงานและข้อมูล
- 4.9 การควบคุมดูแลงาน
- 4.10 การแบ่งแยกหน้าที่ความรับผิดชอบของแต่ละตำแหน่งงาน
- 4.11 การประเมินอัตราบุคลากรด้านเทคโนโลยีสารสนเทศ
- 4.12 การกำหนดหน้าที่ความรับผิดชอบของบุคลากรด้านเทคโนโลยีสารสนเทศ
- 4.13 บุคลากรหลักในหน่วยงานด้านเทคโนโลยีสารสนเทศ
- 4.14 นโยบายและขั้นตอนการว่าจ้างบุคลากรภายนอก
- 4.15 ความสัมพันธ์

PO5 การจัดการด้านการลงทุนในเทคโนโลยีสารสนเทศ (Manage the IT Investment) เพื่อให้มั่นใจในเงินลงทุนที่ต้องใช้ และมีการดูแลการใช้จ่ายเงินอย่างเหมาะสม

5.1 งบประมาณประจำปีของการดำเนินงานด้านเทคโนโลยีสารสนเทศ

5.2 การติดตามดูแลค่าใช้จ่ายและประโยชน์ที่ได้รับ

5.3 ความเหมาะสมของค่าใช้จ่ายและประโยชน์ที่ได้รับ

PO6 การสื่อสารเป้าหมายและทิศทางภายในองค์กร (Communicate Management Aims and Direction) เพื่อให้แน่ใจว่าคนในองค์กรรับรู้และเข้าใจในเป้าหมายและทิศทาง

6.1 สภาพแวดล้อมที่ดีด้านการควบคุมสารสนเทศ

6.2 ความรับผิดชอบด้านนโยบายของผู้บริหาร

6.3 การสื่อสารนโยบายขององค์กร

6.4 ทรัพยากรที่ใช้เพื่อให้บรรลุตามนโยบาย

6.5 การดูแลรักษานโยบาย

6.6 การปฏิบัติตามนโยบาย, ระเบียบขั้นตอนการปฏิบัติงาน และมาตรฐานต่างๆ

6.7 การยึดมั่นในคุณภาพ

6.8 แนวทางนโยบายในการรักษาความปลอดภัยและการควบคุมภายใน

6.9 สิทธิที่เกี่ยวกับทรัพย์สินทางปัญญา

6.10 การกำหนดนโยบายเฉพาะกิจ

6.11 การสื่อสารให้ตระหนักถึงการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

PO7 การจัดการทรัพยากรบุคคล (Manage Human Resources) เพื่อให้มีบุคลากรที่มีความสามารถ และทุ่มเทในการทำงาน

7.1 การจ้างงานและการเลื่อนตำแหน่งบุคลากร

7.2 คุณวุฒิหรือคุณสมบัติของบุคลากร

7.3 บทบาทหน้าที่และความรับผิดชอบ

7.4 การฝึกอบรมบุคลากร

7.5 การฝึกอบรมข้ามส่วนงาน หรือการมีพนักงานทดแทน

7.6 ระเบียบปฏิบัติการตรวจสอบบุคลากร

7.7 การประเมินผลงานพนักงาน

7.8 การเปลี่ยนแปลงตำแหน่งงานและการเลิกจ้างงาน

PO8 การปฏิบัติตามข้อกำหนดขององค์กรภายนอก (Ensure Compliance with External Requirements) เพื่อให้สอดคล้องถูกต้องตามกฎหมาย ระเบียบ และสัญญา

8.1 การสอบทานข้อกำหนดขององค์กรภายนอก

8.2 วิธีการและระเบียบปฏิบัติเพื่อให้เป็นไปตามข้อกำหนดขององค์กรภายนอก

8.3 การปฏิบัติตามมาตรฐานด้านความปลอดภัยและสุขลักษณะในการทำงาน

8.4 ความเป็นส่วนตัว ทรัพย์สินทางปัญญา และข้อมูล

8.5 พาณิชย์อิเล็กทรอนิกส์

8.6 การปฏิบัติตามสัญญาประกันภัย

PO9 การประเมินความเสี่ยง (Assess Risks) เพื่อให้ IT สามารถตอบสนองความต้องการของผู้บริหารในการตัดสินใจเพื่อลดความเสี่ยง โดยให้ข้อมูลที่เป็นรูปธรรม และชี้ให้เห็นประเด็นที่สำคัญ

9.1 การประเมินความเสี่ยงของธุรกิจ

9.2 วิธีการประเมินความเสี่ยง

9.3 การระบุความเสี่ยง

9.4 การประเมินความเสี่ยง

9.5 แผนปฏิบัติงานเพื่อจัดการความเสี่ยง

9.6 การยอมรับความเสี่ยง

9.7 การเลือกมาตรการควบคุม

9.8 การสนับสนุนของผู้บริหารในการประเมินความเสี่ยง

PO10 การจัดการโครงการ (Manage Projects) เพื่อกำหนดระดับความสำคัญ และดำเนินการให้แล้วเสร็จภายในเวลาและงบประมาณที่กำหนด

10.1 กรอบงานการจัดการโครงการ
10.2 การมีส่วนร่วมในการริเริ่มโครงการของหน่วยงานผู้ใช้ / ปฏิบัติงาน
10.3 ทีมงานโครงการและหน้าที่ความรับผิดชอบ
10.4 ข้อกำหนดของโครงการ
10.5 การอนุมัติโครงการ
10.6 การอนุมัติโครงการในแต่ละระยะ
10.7 แผนงานหลักของโครงการ
10.8 แผนงานรับรองคุณภาพระบบ
10.9 การกำหนดวิธีการรับรองคุณภาพ
10.10 การบริหารความเสี่ยงของโครงการอย่างเป็นทางการ
10.11 แผนการทดสอบ
10.12 แผนการฝึกอบรม
10.13 แผนการสอบทานระบบภายหลังการใช้งานจริง

PO11 การจัดการคุณภาพ (Manage Quality) เพื่อให้สามารถตอบสนองความต้องการของผู้ใช้ (ข้อมูล)

11.1 แผนคุณภาพทั่วไป
11.2 วิธีการรับรองคุณภาพ
11.3 แผนการรับรองคุณภาพ
11.4 การสอบทานการรับรองคุณภาพ โดยคำนึงถึงมาตรฐานระบบสารสนเทศและวิธีการทำงาน
11.5 กรรมวิธีวงจรการพัฒนาระบบงาน
11.6 กรรมวิธีวงจรการพัฒนาระบบงานสำหรับการเปลี่ยนแปลงที่สำคัญต่อเทคโนโลยีที่มีอยู่
11.7 การปรับปรุงกรรมวิธีวงจรการพัฒนาระบบงาน
11.8 การประสานงานและการสื่อสาร
11.9 กรอบงานการจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยี

11.10 สัมพันธภาพกับผู้ติดตั้งระบบงานจากภายนอก
11.11 มาตรฐานของเอกสารโปรแกรม
11.12 มาตรฐานการทดสอบโปรแกรม
11.13 มาตรฐานการทดสอบระบบงาน
11.14 การทดสอบคู่ขนานหรือการทดสอบนำร่อง
11.15 เอกสารการทดสอบระบบงาน
11.16 การประเมินเพื่อรับรองคุณภาพ โดยเทียบกับมาตรฐานการพัฒนา
11.17 การสอบทานเพื่อรับรองคุณภาพเกี่ยวกับการบรรลุวัตถุประสงค์ด้านเทคโนโลยีสารสนเทศ
11.18 ตารางเทียบวัดคุณภาพ
11.19 รายงานการสอบทานการรับรองคุณภาพ

2 <u>การจัดหาและการนำระบบออกใช้งานจริง</u> (AI : Acquisition and Implementation)

AI1 การเลือกเทคโนโลยีมาใช้ในการปฏิบัติงาน (Identify Automated Solutions) เพื่อให้มั่นใจว่าจะตอบสนองความต้องการข้อมูลของผู้ใช้ได้อย่างมีประสิทธิผลและประสิทธิภาพ

1.1 การกำหนดความต้องการสารสนเทศ
1.2 การกำหนดทางเลือกในการดำเนินการ
1.3 รูปแบบกลยุทธ์การจัดหา
1.4 การกำหนดระดับการบริการจากบุคคลภายนอก
1.5 การศึกษาความเป็นไปได้ของเทคโนโลยี
1.6 การศึกษาความคุ้มค่าในการลงทุน
1.7 โครงสร้างพื้นฐานสารสนเทศ
1.8 รายงานการวิเคราะห์ความเสี่ยง
1.9 การคุ้มทุนของการรักษาความปลอดภัย
1.10 การออกแบบหลักฐานเพื่อการตรวจสอบ
1.11 สุขลักษณะในการทำงาน
1.12 การคัดเลือกซอฟต์แวร์ระบบ

1.13 การควบคุมการจัดซื้อ

1.14 การจัดซื้อซอฟต์แวร์

1.15 การบำรุงรักษาซอฟต์แวร์ที่จัดซื้อจากบุคคลภายนอก

1.16 สัญญาการใช้โปรแกรมระบบงาน

1.17 การตรวจรับสิ่งอำนวยความสะดวกต่างๆ

1.18 การตรวจรับด้านเทคโนโลยี

AI2 การจัดหาและบำรุงรักษาโปรแกรมระบบงาน (Acquire and Maintain Application Software) เพื่อให้บริการประมวลผลที่สนับสนุนการดำเนินงาน และการปฏิบัติงานขององค์กรได้อย่างมีประสิทธิผล

2.1 วิธีการออกแบบระบบ

2.2 การเปลี่ยนแปลงที่สำคัญกับระบบงานปัจจุบัน

2.3 การอนุมัติการออกแบบ

2.4 การกำหนดความต้องการเกี่ยวกับแฟ้มข้อมูล และการจัดทำเอกสาร

2.5 ข้อกำหนดของโปรแกรม

2.6 การออกแบบวิธีการเก็บรวบรวมข้อมูลต้นทาง

2.7 การกำหนดความต้องการเกี่ยวกับข้อมูลนำเข้า และการจัดทำเอกสาร

2.8 การกำหนดเกี่ยวกับการเชื่อมต่อประสาน

2.9 การเชื่อมโยงระหว่างเครื่องกับผู้ใช้งาน

2.10 การกำหนดความต้องการเกี่ยวกับการประมวลผล และการจัดทำเอกสาร

2.11 การกำหนดความต้องการเกี่ยวกับผลลัพธ์ และการจัดทำเอกสาร

2.12 ความสามารถในการควบคุม

2.13 ความพร้อมใช้งานที่เป็นปัจจัยหลักในการออกแบบระบบ

2.14 ข้อกำหนดเกี่ยวกับความครบถ้วนถูกต้องของเทคโนโลยีสารสนเทศในโปรแกรมระบบงาน

2.15 การทดสอบโปรแกรมระบบงาน

2.16 คู่มือผู้ใช้ระบบและคู่มือสนับสนุนการปฏิบัติงาน

2.17 การประเมินผลซ้ำสำหรับด้านการออกแบบระบบ

AI3 การจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยี (Acquire and Maintain Technology Infrastructure) เพื่อให้องค์กรมี IT Platform ที่เหมาะสมกับระบบงาน

3.1 การประเมินความต้องการฮาร์ดแวร์และซอฟต์แวร์ใหม่
3.2 การบำรุงรักษาฮาร์ดแวร์แบบมีแผนกำหนดเวลาล่วงหน้า
3.3 การรักษาความปลอดภัยของโปรแกรมระบบ
3.4 การติดตั้งโปรแกรมระบบ
3.5 การดูแลและบำรุงรักษาโปรแกรมระบบ
3.6 การควบคุมการเปลี่ยนแปลงแก้ไขโปรแกรมระบบ
3.7 การใช้และการติดตามโปรแกรมอรรถประโยชน์

AI4 ระเบียบปฏิบัติในการพัฒนาและบำรุงรักษา (Develop and Maintain Procedures) เพื่อให้มีการใช้ระบบงานได้อย่างถูกต้องและเป็นระเบียบ

4.1 ความต้องการในการปฏิบัติงานและระดับการให้บริการ
4.2 คู่มือปฏิบัติงานของผู้ใช้
4.3 คู่มือปฏิบัติงานด้านปฏิบัติการคอมพิวเตอร์
4.4 เอกสารประกอบการฝึกอบรม

AI5 การติดตั้งและรับรองระบบ (Install and Accredit Systems) เพื่อสอบทานให้แน่ใจว่าระบบงานนั้นถูกต้องตรงตามวัตถุประสงค์ที่ต้องการ

5.1 การฝึกอบรม
5.2 ขีดความสามารถของโปรแกรมระบบ
5.3 แผนการนำระบบออกใช้งานจริง
5.4 การโอนย้ายระบบเดิมไปยังระบบงานใหม่
5.5 การโอนย้ายข้อมูลไปยังระบบงานใหม่
5.6 การกำหนดแผนและกลยุทธ์ในการทดสอบ
5.7 การทดสอบโปรแกรมที่เปลี่ยนแปลงหรือแก้ไข
5.8 ขั้นตอนและเกณฑ์การทดสอบแบบคู่ขนานหรือแบบนำร่อง
5.9 การทดสอบครั้งสุดท้ายเพื่อตรวจรับระบบ
5.10 การทดสอบด้านการรักษาความปลอดภัย และระดับความน่าเชื่อถือ

5.11 การทดสอบด้านการปฏิบัติงาน

5.12 การเริ่มใช้งานจริง

5.13 การประเมินความสอดคล้องกับความต้องการของผู้ใช้งาน

5.14 การประเมินผลหลังจากนำระบบออกใช้งานจริง

AI6 การจัดการการเปลี่ยนแปลง (Manage Changes) เพื่อลดโอกาสการหยุดชะงัก การแก้ไขโดยพลการ และความผิดพลาด

6.1 การควบคุมคำขอปรับปรุงแก้ไขระบบงาน

6.2 การประเมินผลกระทบ

6.3 การควบคุมการเปลี่ยนแปลงแก้ไข

6.4 การเปลี่ยนแปลงแก้ไขกรณีเร่งด่วน

6.5 การจัดทำเอกสารและระเบียบปฏิบัติ

6.6 การอนุมัติการบำรุงรักษา

6.7 นโยบายการอนุมัตินำโปรแกรมระบบงานออกใช้งาน

6.8 การกระจายติดตั้งโปรแกรม

3 <u>การส่งมอบและการสนับสนุน</u> (DS : Delivery and Support)

DS1 การกำหนดและการจัดการระดับการให้บริการ (Define and Manage Service Levels) เพื่อให้เกิดความเข้าใจที่ถูกต้องของระดับบริการที่เป็นที่ต้องการ

1.1 กรอบข้อตกลงเกี่ยวกับระดับการให้บริการ

1.2 หลักเกณฑ์ข้อตกลงของระดับการให้บริการ

1.3 วิธีปฏิบัติเพื่อให้เกิดประสิทธิภาพ

1.4 การติดตามและการรายงาน

1.5 การทบทวนข้อตกลงและสัญญาระดับการให้บริการ

1.6 รายการที่คิดค่าบริการ

1.7 แผนการปรับปรุงการให้บริการ

DS2 การจัดการการใช้บริการจากบุคคลภายนอก (Manage Third-Party Services) เพื่อให้มั่นใจว่าหน้าที่และความรับผิดชอบของ Third-Party มีกำหนดไว้ชัดเจน และมีการดำเนินการที่ถูกต้อง ต่อเนื่อง

- 2.1 การประสานงานกับผู้ให้บริการ
- 2.2 ความสัมพันธ์กับเจ้าของระบบ
- 2.3 สัญญากับผู้ให้บริการภายนอก
- 2.4 คุณสมบัติของผู้ให้บริการ
- 2.5 สัญญาการใช้บริการจากบุคคลภายนอก
- 2.6 ความต่อเนื่องของการให้บริการ
- 2.7 การตกลงร่วมมือด้านการรักษาความปลอดภัย
- 2.8 การติดตาม

DS3 การจัดการด้านประสิทธิภาพและความสามารถ (Manage Performance and Capacity) เพื่อให้มั่นใจว่ามี Capacity อย่างเหมาะสม ใช้ประโยชน์ได้สูงสุด ให้บริการได้ตามที่กำหนด

- 3.1 ความต้องการเกี่ยวกับความพร้อม และประสิทธิภาพในการใช้งาน
- 3.2 แผนงานความพร้อมสำหรับการใช้งาน
- 3.3 การติดตามผล และการรายงาน
- 3.4 เครื่องมือเสริมการทำงาน
- 3.5 การบริหารประสิทธิภาพแบบมีการคาดการณ์ล่วงหน้า
- 3.6 การคาดการณ์ปริมาณงาน
- 3.7 ความสามารถในการบริหารทรัพยากร
- 3.8 ความพร้อมใช้งานด้านทรัพยากร
- 3.9 แผนการจัดหาทรัพยากร

DS4 ความต่อเนื่องในการให้บริการ (Ensure Continuous Service) เพื่อให้มั่นใจว่าบริการด้าน IT มีให้ใช้ได้ตามที่ต้องการ และเกิดปัญหาต่อการดำเนินธุรกิจน้อยที่สุดหากมีเหตุการณ์สำคัญทำให้ต้องหยุดชะงัก

- 4.1 กรอบงานการดำเนินการอย่างต่อเนื่องด้านเทคโนโลยีสารสนเทศ
- 4.2 กลยุทธ์และปรัชญาในการจัดทำแผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศ
- 4.3 เนื้อหาของแผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศ
- 4.4 ความต้องการขั้นต่ำสำหรับดำเนินการอย่างต่อเนื่องด้านเทคโนโลยีสารสนเทศ
- 4.5 การบำรุงรักษาแผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศ
- 4.6 การทดสอบแผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศ
- 4.7 การฝึกอบรมเกี่ยวกับแผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศ
- 4.8 การเผยแพร่แผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศ
- 4.9 ระเบียบการปฏิบัติงานสำรองของผู้ใช้
- 4.10 ทรัพยากรที่มีความสำคัญด้านเทคโนโลยีสารสนเทศ
- 4.11 ศูนย์สำรอง และฮาร์ดแวร์
- 4.12 การจัดเก็บสื่อข้อมูลสำรองไว้นอกสถานที่
- 4.13 ระเบียบปฏิบัติในการสรุปผล

DS5 การรักษาความปลอดภัยระบบ (Ensure Systems Security) เพื่อปกป้องข้อมูลจากการถูกใช้ เปิดเผย แก้ไข ทำลาย โดยไม่ได้รับอนุมัติหรือการสูญหาย

- 5.1 การประเมินระบบรักษาความปลอดภัย
- 5.2 การให้อำนาจ / สิทธิ์และการควบคุมการเข้าสู่ระบบ
- 5.3 ความปลอดภัยในการเข้าถึงข้อมูลแบบออนไลน์
- 5.4 การจัดการบัญชีผู้ใช้งาน (User Account)
- 5.5 การสอบทานบัญชีผู้ใช้งาน
- 5.6 การควบคุมบัญชีผู้ใช้งานด้วยตนเอง
- 5.7 มาตรการติดตามรักษาความปลอดภัย
- 5.8 การจำแนกประเภทข้อมูล

5.9 การจัดการเกี่ยวกับการแสดงตน และสิทธิในการเข้าถึงข้อมูลแบบรวมศูนย์
5.10 รายงานการละเมิดและกิจกรรมที่เกี่ยวข้องกับความปลอดภัย
5.11 การจัดการกับเหตุการณ์ที่เกิดขึ้น
5.12 การทบทวนความน่าเชื่อถือของระบบรักษาความปลอดภัย
5.13 ความน่าเชื่อถือของคู่ค้า
5.14 การอนุมัติรายการ
5.15 การปฏิเสธรายการที่ผิดเงื่อนไข
5.16 ช่องทางการรับส่งข้อมูลที่เชื่อถือได้
5.17 การป้องกันการแก้ไขระบบควบคุมที่กำหนดไว้
5.18 การจัดการเกี่ยวกับรหัสลับ
5.19 การป้องกัน การตรวจหา และการแก้ไขเกี่ยวกับโปรแกรมที่เป็นอันตรายต่อองค์กร
5.20 โครงสร้างไฟร์วอลล์และการเชื่อมโยงกับเครือข่ายสาธารณะ
5.21 การป้องกันความเสียหายของข้อมูลอิเล็กทรอนิกส์

DS6 การกำหนดและจัดสรรต้นทุน (Identify and Allocate Costs) เพื่อให้เกิดการรับรู้อย่างถูกต้องในต้นทุนของบริการด้าน IT
6.1 รายการที่สามารถบันทึกค่าใช้จ่ายเป็นต้นทุนด้านเทคโนโลยีได้
6.2 ระเบียบปฏิบัติเรื่องต้นทุน
6.3 ระเบียบปฏิบัติในการเรียกเก็บค่าใช้จ่ายและการคืนค่าใช้จ่าย

DS7 การให้ความรู้และฝึกอบรมผู้ใช้งาน (Educate and Train Users) เพื่อให้มั่นใจว่าผู้ใช้สามารถใช้บริการได้อย่างมีประสิทธิภาพ และเข้าใจถึงความเสี่ยง ความรับผิดชอบที่เกี่ยวเนื่องในการใช้นั้นๆ
7.1 กำหนดแผนการฝึกอบรมที่จำเป็นให้แก่พนักงานในแต่ละระดับ
7.2 การกำหนดเป้าหมายของการอบรมในแต่ละระดับพนักงาน
7.3 การอบรมให้มีความตระหนักในเรื่องการรักษาความปลอดภัย

DS8 การให้ความช่วยเหลือและคำแนะนำแก่ผู้ใช้ระบบงานในองค์กร (Assist and Advise Customers) เพื่อให้มั่นใจว่าปัญหาที่ผู้ใช้ประสบได้รับการแก้ไขอย่างเหมาะสม

8.1 หน่วยงานช่วยเหลือผู้ใช้งาน
8.2 การบันทึกปัญหาต่างๆ ที่ถูกสอบถาม
8.3 ขั้นตอนการแก้ไขปัญหา
8.4 การติดตามการแก้ไขปัญหาที่เกิดขึ้น
8.5 การวิเคราะห์แนวโน้มและรายงาน

DS9 การจัดการรายละเอียดทรัพย์สิน (Manage the Configuration) เพื่อให้มีการดูแลรักษา จดบันทึกอย่างเหมาะสมในอุปกรณ์ IT ป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุมัติ มีการตรวจนับ และมีระบบการควบคุมการเปลี่ยนแปลง

9.1 การบันทึกรายการรายละเอียดทรัพย์สิน
9.2 ข้อมูลพื้นฐานของรายละเอียดทรัพย์สิน
9.3 การบันทึกสถานภาพของทรัพย์สิน
9.4 การควบคุมรายละเอียดทรัพย์สิน
9.5 โปรแกรมที่ไม่ได้รับอนุญาตให้นำมาใช้งาน
9.6 การจัดเก็บซอฟต์แวร์
9.7 ระเบียบปฏิบัติการจัดการเกี่ยวกับรายละเอียดทรัพย์สิน
9.8 การกำหนดความรับผิดชอบด้านซอฟต์แวร์

DS10 การจัดการปัญหาและเหตุการณ์ที่เกิดขึ้น (Manage Problems and Incidents) เพื่อให้มั่นใจว่าปัญหาและอุบัติเหตุที่เกิดขึ้นได้รับการแก้ไข มีการหาสาเหตุ และป้องกันไม่ให้เกิดขึ้นซ้ำอีก

10.1 ระบบการจัดการปัญหา
10.2 ขั้นตอนในการแก้ไขปัญหา
10.3 หลักฐานการตรวจสอบและการติดตามปัญหา
10.4 การอนุญาตให้เข้าถึงระบบในกรณีฉุกเฉินและชั่วคราว
10.5 การกำหนดลำดับการประมวลผลกรณีฉุกเฉิน

DS11 การจัดการข้อมูล (Manage Data) เพื่อให้มั่นใจว่าข้อมูลมีความสมบูรณ์ ถูกต้องและน่าเชื่อถือ ทั้งในช่วง input, update & storage

11.1 ระเบียบปฏิบัติในการจัดเตรียมข้อมูล

11.2 ระเบียบปฏิบัติในการอนุมัติให้นำข้อมูลเอกสารเข้าสู่ระบบ

11.3 การรวบรวมข้อมูลเข้าสู่ระบบ

11.4 การแก้ไขข้อผิดพลาดของข้อมูลเข้าสู่ระบบ

11.5 ระยะเวลาการจัดเก็บข้อมูลเอกสารประกอบรายการ

11.6 ระเบียบปฏิบัติว่าด้วยสิทธิในการนำข้อมูลเข้าประมวลผล

11.7 การตรวจสอบความสมบูรณ์ ถูกต้อง และการอนุมัติรายการ

11.8 การแก้ไขข้อมูลที่บันทึกผิดพลาด

11.9 ความครบถ้วนถูกต้องของการประมวลผลข้อมูล

11.10 การตรวจสอบความสมเหตุสมผลในการแก้ไขข้อผิดพลาดของการประมวลผลข้อมูล

11.11 การแก้ไขข้อผิดพลาดในการประมวลผลข้อมูล

11.12 การจัดการผลลัพธ์และการจัดเก็บ

11.13 การแจกจ่ายรายงาน

11.14 การสอบยันและกระทบยอดรวมของรายงาน

11.15 การสอบทานและการแก้ไขข้อผิดพลาดของรายงาน

11.16 ข้อกำหนดในการรักษาความปลอดภัยของรายงาน

11.17 การป้องกันข้อมูลที่มีความสำคัญในระหว่างการเคลื่อนย้ายหรือส่งผ่าน

11.18 การป้องกันข้อมูลสำคัญที่บันทึกอยู่บนสื่อบันทึกข้อมูลที่องค์กรได้จำหน่ายทิ้ง

11.19 การจัดการด้านการจัดเก็บข้อมูล

11.20 ระยะเวลาและเงื่อนไขการจัดเก็บข้อมูล

11.21 ระบบการจัดการคลังสื่อบันทึกข้อมูล

11.22 ความรับผิดชอบในการจัดการคลังสื่อบันทึกข้อมูล

11.23 การสำรองข้อมูล

11.24 งานด้านการสำรองข้อมูล

11.25 การจัดเก็บข้อมูลชุดสำรอง

11.26 การจัดเก็บข้อมูลถาวร

11.27 การป้องกันข้อความที่สำคัญ

11.28 การพิสูจน์ตนและความครบถ้วนถูกต้อง

11.29 ความครบถ้วนถูกต้องของรายการธุรกรรมอิเล็กทรอนิกส์

11.30 การคงความถูกต้องของข้อมูลที่จัดเก็บ

DS12 การจัดการด้านสิ่งอำนวยความสะดวก (Manage Facilities) เพื่อให้มีบรรยากาศแวดล้อมทางกายภาพที่เหมาะสมในการปกป้องอุปกรณ์ IT และบุคลากรจากภัยธรรมชาติและบุคคล

12.1 ความปลอดภัยทางกายภาพ

12.2 ความปลอดภัยของสถานที่ที่ตั้งศูนย์คอมพิวเตอร์

12.3 การควบคุมการเข้า – ออกศูนย์คอมพิวเตอร์

12.4 ความปลอดภัยและสุขอนามัยของบุคลากร

12.5 การป้องกันภัยจากปัจจัยรอบข้าง

12.6 เครื่องจ่ายกระแสไฟฟ้าสำรอง

DS13 การจัดการด้านการปฏิบัติการ (Manage Operations) เพื่อให้มั่นใจว่าการปฏิบัติการด้าน IT ที่สำคัญ มีการดำเนินงานอย่างสม่ำเสมอและเป็นลำดับอย่างถูกต้อง

13.1 ระเบียบปฏิบัติและคู่มือคำสั่งการประมวลผล

13.2 เอกสารขั้นตอนการเริ่มทำงานของระบบ และคู่มือการปฏิบัติงานอื่นๆ

13.3 ตารางการปฏิบัติงาน

13.4 การประมวลผลนอกเหนือจากตารางการปฏิบัติงาน

13.5 ความต่อเนื่องของการประมวลผล

13.6 การบันทึกเหตุการณ์การปฏิบัติงาน

13.7 การป้องกันเอกสารและอุปกรณ์ที่สำคัญ

13.8 การปฏิบัติงานระยะไกล

4 <u>การติดตามผล</u> (M : Monitoring)

M1 การติดตามกระบวนการทำงาน (Monitor the Processes) เพื่อให้มั่นใจว่ากิจกรรมด้าน IT สามารถบรรลุเป้าหมายการปฏิบัติงานตามที่กำหนด

1.1 การรวบรวมข้อมูล

1.2 การประเมินประสิทธิภาพการปฏิบัติงาน

1.3 การประเมินความพึงพอใจของผู้รับบริการ

1.4 การรายงานสำหรับผู้บริหาร

M2 การประเมินความเพียงพอของการควบคุมภายใน (Assess Internal Control Adequacy) เพื่อให้มั่นใจว่าเป้าหมายของการควบคุมภายในของกิจกรรมด้าน IT สามารถบรรลุได้ตามที่กำหนด

2.1 การติดตามการควบคุมภายใน

2.2 ระยะเวลาการปฏิบัติงานของการควบคุมภายใน

2.3 การจัดลำดับการรายงานการควบคุมภายใน

2.4 ความน่าเชื่อถือในความปลอดภัยของการทำงาน และการควบคุมภายใน

M3 การรับรองความเป็นอิสระ (Obtain Independent Assurance) เพื่อเพิ่มความมั่นใจและการไว้วางใจระหว่างองค์กร, ผู้ใช้ และ Third-Party

3.1 การเป็นอิสระในการรับรองความปลอดภัยและการควบคุมภายในของการให้บริการด้านเทคโนโลยีสารสนเทศ

3.2 การรับรองความปลอดภัย และการควบคุมภายในของการให้บริการที่รับรองจากบุคคลภายนอก

3.3 ความเป็นอิสระในการประเมินประสิทธิภาพ / ประสิทธิผลของการบริการด้านเทคโนโลยีสารสนเทศ

3.4 ความเป็นอิสระในการประเมินประสิทธิภาพ / ประสิทธิผลของการให้บริการจากบุคคลภายนอก

3.5 ความเป็นอิสระในการรับรองการปฏิบัติตามกฎหมาย ระเบียบข้อบังคับ และข้อตกลงที่กำหนดไว้

3.6 ความเป็นอิสระในการรับรองการปฏิบัติตามกฎหมาย ระเบียบข้อบังคับ และข้อตกลงที่กำหนดไว้กับผู้ให้บริการภายนอก

3.7 ความรู้ความสามารถในการทำหน้าที่รับรองอย่างเป็นอิสระ

3.8 การมีส่วนร่วมของการตรวจสอบ

M4 ความเป็นอิสระในการตรวจสอบ (Provide for Independent Audit) เพื่อเพิ่มระดับความมั่นใจและประโยชน์จากผู้เชี่ยวชาญในวิธีการปฏิบัติที่ดี

4.1 กฎบัตรการตรวจสอบ

4.2 ความเป็นอิสระ

4.3 จรรยาบรรณและมาตรฐานวิชาชีพ

4.4 ความรู้ความสามารถของผู้ตรวจสอบ

4.5 การวางแผน

4.6 การปฏิบัติงานตรวจสอบ

4.7 การรายงาน

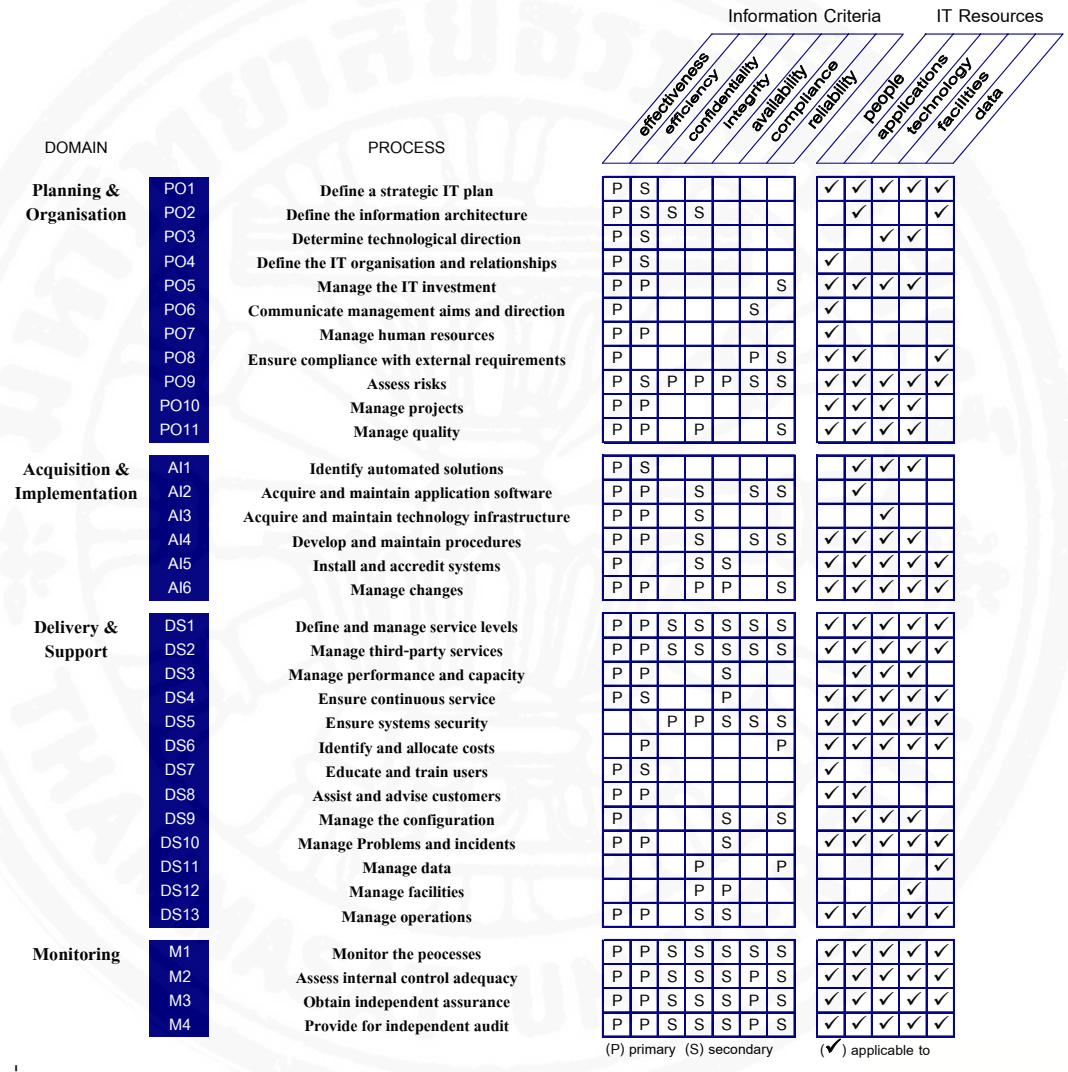
4.8 การติดตามผล

ในแต่ละหัวข้อของวัตถุประสงค์การควบคุม มาตรฐาน COBIT แสดงถึงความสัมพันธ์ต่อปัจจัย 2 ประการ ได้แก่

- คุณภาพของระบบข้อมูล (Information Criteria) 7 ประการ
- ทรัพยากรด้านเทคโนโลยี (IT Resources) 5 ประเภท

ภาพที่ 2.8

ความสัมพันธ์ระหว่างวัตถุประสงค์การควบคุมต่อปัจจัยด้านคุณภาพของระบบข้อมูล และปัจจัยทรัพยากรด้านเทคโนโลยี



ที่มา: www.isaca.org, www.itgi.org

2.5.1 <u>คุณภาพของระบบข้อมูล</u> (Information Criteria) 7 ประการ ประกอบด้วย

- ประสิทธิผล (Effectiveness) หมายถึง ข้อมูลที่ใช้มีความเกี่ยวข้องกับกระบวนการทางธุรกิจ รวมทั้งมีการส่งมอบข้อมูลแก่ผู้ใช้อย่างถูกต้อง ตรงเวลา สม่ำเสมอ (Consistent) และใช้ประโยชน์ได้ (Usable)
- ประสิทธิภาพ (Efficiency) หมายถึง มีการใช้ประโยชน์จากทรัพยากรอย่างเต็มที่เพื่อให้ได้มาซึ่งข้อมูลสารสนเทศ
- การรักษาความลับ (Confidentiality) หมายถึง การป้องกันการเปิดเผยข้อมูลที่สำคัญต่อบุคคล หรือหน่วยงานที่ไม่ได้รับอนุญาต
- ความสมบูรณ์ (Integrity) หมายถึง ความครบถ้วนถูกต้องของข้อมูล ตลอดจนเป็นข้อมูลใช้ได้ (Validity) ในแง่ของความคาดหมายและการให้ความสำคัญของธุรกิจ (Business Values and Expectations)
- การมีใช้เมื่อต้องการ (Availability) หมายถึง เป็นข้อมูลที่เรียกใช้ได้เมื่อต้องการและจำเป็น การมีใช้เมื่อต้องการหมายถึงทั้งในปัจจุบันและอนาคต และรวมทั้งการป้องกันภัยให้กับทรัพยากรต่างๆ ที่จำเป็น และการรักษาระดับความสามารถในการทำงานของทรัพยากรเหล่านั้น
- การปฏิบัติตามระเบียบ (Compliance) หมายถึง การที่ข้อมูลได้จัดทำขึ้นตามกฎระเบียบ ข้อบังคับ หลักเกณฑ์ ข้อตกลง หรือกฎหมายที่มีขึ้น เพื่อบังคับใช้ทั้งจากหน่วยงานภายในและภายนอกองค์กร เช่น ข้อบังคับของตลาดหลักทรัพย์แห่งประเทศไทย ประมวลกฎหมายภาษีอากร หลักการบัญชีที่ยอมรับโดยทั่วไป เป็นต้น
- ความน่าเชื่อถือของข้อมูล (Reliability of Information) หมายถึง ความสามารถในการจัดหาข้อมูลที่เหมาะสมให้แก่ผู้บริหารของกิจการ เพื่อสามารถดำเนินธุรกิจและเพื่อให้สามารถจัดทำรายงานทางการเงิน และรายงานที่จำเป็นอื่นๆ ภายใต้ความรับผิดชอบของผู้บริหาร

2.5.2 <u>ทรัพยากรด้านเทคโนโลยี</u> (IT Resources) 5 ประเภท ประกอบด้วย

- ข้อมูล (Data) รวมความถึง ข้อมูลในรูปแบบต่างๆ ทั้งที่มีโครงสร้าง และไม่มีโครงสร้าง ข้อมูลด้านกราฟฟิค และข้อมูลที่เป็นเสียง
- ระบบงาน (Application System) ได้แก่ ขั้นตอนและกระบวนการปฏิบัติงานทั้งที่ทำด้วยมือและโปรแกรมคอมพิวเตอร์
- เทคโนโลยี (Technology) ได้แก่ เครื่องคอมพิวเตอร์ (Hardware) โปรแกรมระบบ (Operating Systems) ระบบบริหารฐานข้อมูล (Database Management System) ระบบเครือข่าย (Networking) และระบบมัลติมีเดีย (Multimedia)
- สิ่งอำนวยความสะดวก (Facilities) ได้แก่ ทรัพยากรต่างๆ ที่ใช้เป็นสถานที่ติดตั้งหรือจัดวาง ตลอดจนสาธารณูปโภคที่จำเป็น เพื่อการปฏิบัติงานของระบบสารสนเทศ
- บุคลากร (People) ได้แก่ บุคลากรที่มีความรู้ ความชำนาญในการบริหารและปฏิบัติงาน สำหรับการดูแลและจัดทำระบบสารสนเทศ

นอกจากโครงสร้างของมาตรฐาน COBIT ดังกล่าวข้างต้นแล้ว มาตรฐาน COBIT ยังให้แนวทางสำหรับผู้บริหาร (Management Guidelines) เพื่อใช้ในการวัดผลการนำมาตรฐาน COBIT ไปใช้ในองค์กร โดยประกอบด้วย 4 ปัจจัยหลัก ได้แก่

- Generic Maturity Model

  เพื่อให้ผู้บริหารสามารถเปรียบเทียบระดับการควบคุมขององค์กรในปัจจุบันกับระดับที่เป็นเลิศของธุรกิจประเภทเดียวกัน และเป้าหมายที่องค์กรต้องการ โดยแบ่งระดับการควบคุมออกเป็น 6 ระดับ คือ
  - *0 ไม่มี (Non-Existent)* ไม่รับรู้ และไม่ให้ความสนใจใดๆ เลย
  - *1 มีบ้าง (Initial / Adhoc)* มีการรับรู้ และให้ความสนใจบ้าง แต่ไม่เป็นระบบ ไม่ต่อเนื่อง เป็นแต่ละครั้ง แต่ละกรณี
  - *2 มีทั่วไป (Repeatable)* มีความต่อเนื่อง แต่ยังไม่มีการอบรม การทำคู่มือยังขึ้นอยู่กับบุคคลที่ทำมากกว่า

- *3 มีอย่างเป็นระบบ (Defined)* มีการทำคู่มือ มีความเป็นระบบมากขึ้น แต่ยังเป็นไปอย่างง่ายๆ
- *4 มีอย่างเป็นระบบที่ดี (Managed)* มีมาตรการที่เข้มแข็งขึ้น มีมาตรการสำหรับเมื่อมีข้อผิดพลาดเกิดขึ้น
- *5 เป็นตัวอย่างได้ (Optimized)* มีการควบคุมที่เป็นอัตโนมัติ

- Critical Success Factors (CSF)

สิ่งสำคัญที่ต้องทำหรือเงื่อนไขที่จำเป็นที่จะช่วยเพิ่มโอกาสของความสำเร็จ หรือเพื่อให้บรรลุเป้าหมายได้อย่างเต็มที่ เป็นสิ่งที่มองเห็นได้ชัดเจนและส่วนมากสามารถวัดได้ อาจเป็นงานอะไร ระดับใดก็ได้

- Key Goal Indicators (KGI)

เป็นตัวชี้วัดที่ใช้วัดความสำเร็จของงานภายหลังการทำงานเสร็จสิ้นแล้ว สามารถวัดได้อย่างชัดเจน หรือค่อนข้างชัดเจน

- Key Performance Indicators (KPI)

ใช้วัดการทำงานที่มีผลสำคัญยิ่งต่อการที่จะบรรลุความสำเร็จ หรือเป้าหมายที่ต้องการ เพื่อให้ทราบว่าสิ่งที่จำเป็นต้องทำ ต้องมี ได้ดำเนินไปถึงไหนแล้ว สามารถใช้เป็นเครื่องทำนายโอกาสของความสำเร็จ หรือล้มเหลวในอนาคต